Defining the critical success factors that can allow for a public-private partnership in cyber intelligence in the Netherlands.

Master Thesis Crisis and security management – faculty of governance and global affairs.

Ko Voskuilen
S1215221
Thesis Master Crisis and security Management
10/06/2018
Wordcount excluding bibliography and appendices: 17.116
Wordcount including bibliography and appendices: 20.093
Thesis supervisor: Dr. Jaap Reijling.
Second Reader: Dr. Constant Hijzen.

I would like to thank all of those who helped me in writing my master thesis. Especially Dr. Jaap Reijling for his invaluable advice. A special thanks also goes out to the interview respondents without whom this thesis would not have been possible.

Contents

1 - Introduction.

Over the past three decades information and communication technology (ICT) has become an integrated part of our society. Both the public and the private sector have benefitted immensely from new technologies such as the internet, mobile phones and data collection methods. It comes as no surprise that the Dutch government is therefore actively encouraging ICT development in the digital domain[1]. Digitalisation can offer important stimuli for social-economic benefits and innovation in digitisation is therefore necessary (NCTV 2013, 19). However, innovation in the digital domain can only be achieved in a safe environment. Today it is no news that the development of ICT has come with its downsides too. Increasingly governments, companies and citizens are confronted with the negative sides of the developments in the cyber realm. Attacks on government networks by malicious state actors have been a 'hot topic' the past few years (Nationaal Cyber Security Centrum (NCSC) 2017, 13). Recently the Dutch minister for justice and safety, Ferd Grapperhaus, emphasised the need for increased cyber security in light of a growing cyberthreat against the government, but also against companies (Jonker and Witteman 2018). Furthermore, alleged meddling with elections and distribution of so called 'fake news' have held states all over the world busy (Ollongren 2018, 5). For companies who invest heavily in research and development, cyber espionage is an increasing threat (Tweede Kamer der Staten-Generaal 2015, 4). Citizens are increasingly aware of the information they share with companies and how that affects their privacy. For national security it is important to develop a sound cyber defence strategy to keep out those actors who are not welcome. This applies to government cyber networks, but also to networks surrounding critical infrastructure, such as telecommunications and electricity grids.

The Dutch government has therefore developed a National Cyber Security Strategy in 2013. The report highlights the increased threat posed by other states and professional criminals.

> "The threats from other states mostly concern the theft of confidential or competition sensitive information (cyber espionage), while professional criminals mainly focus on digital fraud and theft of information. Due to the increased complexity of, dependence

[1] The digital domain is the conglomerate of ICT tools and services and comprises all entities that can be or are digitally linked. The domain comprises both permanent, temporary or local connections, as well as information, such as data and programme codes, located in this domain where geographical limitations do not apply (NCTV 2013, 7).

on and vulnerability of ICT-based products and services, our digital resilience to these and other cyber threats is currently still insufficient" (NCTV 2013, 7).

The threat posed by cyberespionage has since developed. Cyber espionage can be defined as 'the intentional use of computers or digital communications activities in an effort to gain access to sensitive information about an adversary or competitor for the purpose of gaining an advantage or selling the sensitive information for monetary reward' (Weissbrodt 2013, 370–71). In the Cyber Security Assessment Netherlands of both 2016 and 2017 the threat posed by other states in terms of cyberespionage was considered a threat to national security. Intelligence agencies have observed a great deal of digital espionage in the form of cyber-attacks on the defence industry and 'on such leading sectors as high-tech, chemical, energy, life sciences & health and the water sector' (Nationaal Cyber Security Centrum (NCSC) 2016, 19). The government is also targeted repeatedly, in 2017 the ministry of foreign affairs and the ministry of defence were attacked by large-scale digital espionage (Nationaal Cyber Security Centrum (NCSC) 2017, 13). Foreign intelligence agencies are thus after state secrets relating to policy and strategy, but also after company secrets relating to research and development in high-end sectors for economic gain.

In light of the increased threat posed by other states in terms of espionage, the two Dutch intelligence agencies[2] joint efforts in Signals intelligence (SIGINT) and Cyber intelligence in the Joint Sigint Cyber Unit (JSCU) (NCTV 2013, 9). Core tasks of the JSCU include collection of data from technical sources, support in data-analysis, and investigations into cyber threats. The unit is managed by the head of the AIVD, the director of the MIVD and the head of the JSCU. The board of the JSCU comprises the Secretary-General of General Affairs, Internal Affairs and Kingdom Relations, and Defence. The board is concerned with political and governance aspects relating to the JSCU which supersede the managerial board (Hennis-Plasschaert and Plasterk 2014, 2–3).

In addition, the private sector is also targeted by other states through cyber espionage. Private companies with large research and development (R&D) departments often invest large amounts of money to remain ahead of the market. This information is interesting to other states, since it can provide their companies with the same R&D, without the cost. Giving them a crucial economic edge over the competition. In that sense, cyber espionage becomes cyber

[2] General Intelligence and Security Service (with the Dutch acronym AIVD) and Military Intelligence and Security Service (with the Dutch acronym MIVD).

industrial espionage. The latter can be defined as ‘a form of commercial intelligence gathering, usually, but not exclusively, on the part of industry competitors’ (Crane 2005, 23). While traditionally this has been intelligence between companies, recently foreign actors have been active in industrial intelligence gathering as well. A well-known example of state intelligence services using cyber industrial espionage is China. In 2010 McAfee published a report with the results of an investigation dubbed ‘operation shady rat’. Multiple cyber intrusions over a period of five years targeted the networks of governments, private companies, and international organisations (Inkster 2015, 68). In the Netherlands it also proves to be a concern. From 2012 to 2015 a Chinese hacker group targeted over 24 companies internationally, amongst which a ‘German-Dutch cooperation in the defence industry’ (Modderkolk 2016).

In light of the growing threat posed by cyber espionage the private sector has launched several cyber security initiatives. One such initiative is the Cyber Security Chain (CSC). The CSC consists of six Dutch private cyber security companies that offer an end-to-end cyber security service for companies. CSC focusses on prevention, detection and response. Prevention and detection focus on awareness, governance, compliance, ethical hacking, and monitoring data leaks, attacks, and deviations (Cyber Security Keten n.d. 2018).

Cyber security is tangible in all layers of society. It is no black and white manner, it cannot be divided into public sector security and private sector cyber security. National cyber security has to take into account the numerous (semi) private companies that control and manage critical networks that could form a threat to national security. Critical infrastructure networks include telecommunications, electricity, healthcare and water structures. These sectors often have private companies behind them. Therefore it is vital that the private sector and the government partner up to ensure cyber security throughout society. To this end, the Dutch National Cyber Security Centre facilitates Information Sharing and Analysis Centres (ISACs). ISACs have been developed, in which participants can ‘exchange information and experiences about cyber security’ (NCSS 2018b). The ISAC structure is a way for vital sectors of the Dutch economy to share information and best-practices in cyber security. The information that is shared between participating organisations is often focused on vulnerabilities and public knowledge (NCSS 2018a).

The public and private sector are aware of the need for more cyber security and have established several public-private partnerships (PPPs) to develop better responses to cyber-attacks. However, the focus in cyber security is shifting. As of now, companies as well as the government are focussing on policies of compliance and there is an excessive focus on

vulnerabilities. This means security control frameworks are periodically controlling ICT systems on security leaks and correcting known vulnerabilities. However, security controls do not always address actual threats and correcting known vulnerabilities leaves many unknown vulnerabilities exposed (Muckin and Fitch 2014, 3). A reactive approach, then, focusses on quick responses to cyber-attacks, minimizing downtime and continuing usage with minimal interruption (Mattern et al. 2014, 704). A proactive approach, however, 'track[s] the capabilities, intentions, and activities of potential adversaries and competitors, as they evolve, in the cyber realm' (Mattern et al. 2014, 704). The proactive approach is not only important to governments, but also to the private sector. Companies are facing continuous threats from competition, both domestic and international. Having intelligence regarding who is preparing an attack, why they are preparing an attack and what might by next (Mattern et al. 2014, 704) creates an advantage on which a better cyber security strategy can be built.

However, for a large part of the private sector it is difficult to collect and analyse intelligence. Especially when cyber intelligence is related to state actors who are actively trying to hack into company networks to steal information. In traditional intelligence, the national intelligence agencies are responsible for counterintelligence. The National Cyber Security strategy highlights that, in a constant open dialogue between all stakeholders, 'the underlying fundamental principle is that the responsibilities that apply in the physical domain should also be taken in the digital domain' (NCTV 2013, 7). In terms of cyber intelligence, this relates to countering the espionage efforts of foreign services and private actors. 'The necessity for counterespionage stems from the fact that defence measures, although essential, are often not enough to track down vulnerabilities in a security system or to trace people that work for the opposition' (de Jong and Keller 2010, 278). The necessity for traditional counterespionage, carried out by the AIVD and MIVD, can be applied to cyber security as well. Defence measures such as security systems and control frameworks are not enough to guarantee a high security level. An active approach is necessary to find threats and to adapt cyber security systems to them. This applies to the private sector as well as to the public sector. In terms of cyber intelligence, however, there is little to no partnership with the private sector, despite the fact that a large part of the spectrum on which intelligence must be gathered belongs to private companies.

Effective cyber security, therefore, relies on threat intelligence. It is thus the responsibility of the Dutch government to provide all sectors with cyber threat intelligence, in order for private companies to comply with cyber security regulation. At this moment the JSCU

is carrying out cyber intelligence alone. This thesis aims to find out whether a public-private partnership in cyber intelligence is achievable. As a central question this thesis asks

'what are critical success factors that would allow for a public-private partnership in cyber intelligence in the Netherlands?'

Increasing reliance on digital systems will mean that in the coming years much more data will be produced. So much that it will be difficult for the Dutch government to keep up intelligence wise. Traditionally, the market has always come through in innovating systems and services which can allow for such growth. In that sense, private companies can prove to be a valuable asset for Dutch intelligence agencies in terms of cyber intelligence. What kind of governance does it take to make such a public private partnership successful?

Besides governance, in a PPP the commercial side of outsourcing is important. In each PPP the part taken by the private party can be fulfilled by many different companies. Numerous legislations have been written, both on a European (European Parliament and Council of the European Union, 2004) as well as on a National level (Aanbestedingswet, 2012), regarding rules and regulation on public procurement. The extent of this legislation and its impact on a PPP in cyber intelligence in the Netherlands goes beyond the scope of this thesis project and deserves a research project on its own. Therefore, this thesis will limit its focus to the governmental aspect of a cyber intelligence PPP.

Part of the governance of such a PPP surrounds the question of public accountability. The outcomes of such a partnership have to be communicated back to parliament and the public. Those communications cannot be outsourced to the private side of the partnership. In terms of governance, this becomes quite a puzzle. Especially regarding such sensitive matters as cyber intelligence.

This thesis will use performance management theory to establish critical success factors in which a public private partnership in cyber intelligence would be possible. It will find out what performance management in the cyber security field constitutes and how a public private partnership in cyber intelligence can be characterised against a background of performance management. The thesis will look at public accountability and how it can fit in such a partnership. Ultimately, the aim of this research project will be to find out what discrepancies there are, how they can be explained, and how they can be addressed.

Chapter two will set out on theories surrounding public private partnerships, accountability and performance management. Next, chapter three will delve into critical

success factors and their theory. It will outline critical success factors this research project will use. Chapter four will provide a methodological overview of how the research will be conducted. Chapter five provides an analysis of the data. Finally, chapter six will provide recommendations on policy and further research.

2 - Theory.

2.1 - Public Private Partnerships.

Before delving into Performance Management as a theory to govern a public-private partnership in cyber intelligence, it is worthwhile to describe what a PPP actually is. In recent years, the term PPP has been used in many different settings. Ranging from urban renewal projects, to the interaction between civil society actors and 'third sector' organisations, to public policy networks. Most of the time, a PPP refers to what Greve defines as 'long-term infrastructure contracts which combine the efforts of public sector actors and private sector actors' (Greve 2010, 3). A more technical definition is provided by Bovaird, who defines PPPs as 'working arrangements based on a mutual commitment (over and above that implied in any contract) between a public sector organization with any organization outside of the public sector' (2004, 200). However, for purposes of this thesis the definition proposed by Skelcher is more suitable: 'Public-private partnerships […] combine the resources of government with those of private agents (businesses or not-for-profit bodies) in order to deliver societal goals' (2009, 347). It broadens the scope of what a PPP can entail and allows a partnership in cyber intelligence. In relation to cyber security, Skelcher's definition can be complemented by Carr's contribution on PPPs in Cyber security. She views PPPs as a 'relationship between the government and the owners/operators of critical infrastructure' keeping in mind that other aspects of cyber security are 'linked to the national interest, [while] critical infrastructure protection is unequivocally and intrinsically linked to national security' (Carr 2016, 45). Overarching in all definitions of PPPs 'is the added value of synergy, i.e. being able to develop a product with characteristics that would not have been available without a PPP' (E.-H. Klijn and Teisman 2003, 137). In this research, the product that is being developed is an increased cyber intelligence capacity for Dutch intelligence agencies through a PPP.

Therefore, these type of PPPs are concerned with the make-or-buy decisions that a government faces. 'Governments can choose to realize societal goals directly, through public employees and collectively controlled facilities (the make decision), or indirectly by means of business and not-forprofit organizations (the buy decision)' (Skelcher 2009, 348). Choosing the buy option can result in five different forms of partnership: 'public leverage, contracting-out, franchising, joint ventures, and strategic partnering' (Skelcher 2009, 348). The relation that results from such a partnership gives rise to the phenomenon of hybridity, which refers to a dual orientation of an organisation; that is, both public and private (Skelcher 2009, 348).

Hybridity, however, can only benefit both sides of the partnership when clear rules and regulatory principles are agreed upon beforehand. A public-private partnership has to be beneficial for both the public party as well as the private party. 'The core of a PPP is that the supplier becomes co-responsible for both losses as well as profits' (Elias et al. 2014, 173). Inherent to a successful PPP is thus the process of preparing, structuring and managing a PPP. The World Bank Group (2016) specifies a PPP process cycle in their Public-Private Partnership Certification Guide which contains six steps (see figure 1).

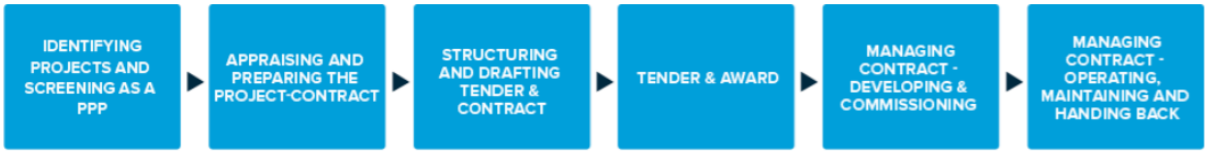

Figure 1 (The World Bank Group (WBG), 2016; 145)

It starts with identifying certain projects which are susceptible to a public private partnership. A scope must be defined and the financial side of the project is mapped. The second step is about refinement, both the scope and the pre-design are developed in more detail and due diligence and feasibility are investigated. Thirdly, the preparatory stage is finalised by defining the final structure of the contract, including contract management strategies and tools. In the fourth stage, a tender is launched, bidders are chosen and the contract is awarded. In the fifth step, a contract management team is set up and approved. The sixth and final step is about monitoring performance, managing changes, claims, and disputes (The World Bank Group (WBG) 2016, 145).

Important to note is that a PPP is different from contracting out. In contracting out, the government dictates the terms and conditions for service production and delivery. Once those terms and conditions are set, the private company starts producing the service or good. There is no interaction between public and private, except from resolving disputes. In a PPP, the 'government defines the problem and, sometimes, specific performance indicators (outcomes), there remains extensive interaction between the agency and potential private partners during pre- and post-award negotiations to determine how the good or service might be provided' (Forrer et al. 2010, 476–77).

A PPP, then, is also about achieving goals that would not have been possible without the partnership. However, this requires partners that are 'willing to look for new solutions for joint ambitions, which requires exchange of information and ideas' (E. Klijn and Teisman 2000, 92). In other words, in order to achieve synergy, the two partners need to have a certain minimal level of trust. Successful partnerships need interactive learning, and creative solutions.

Without trust, partners stick to their own interests and refuse to search for new solutions out of fear of being exploited by the other actors (E. Klijn and Teisman 2000, 92).

The last two steps in the PPP process cycle, and to some extent the third, relate to problem definition, performance indicators and interaction. Leading ultimately to another important factor in PPPs besides trust: accountability.

2.2 - Accountability in PPPs.

In any public private partnership accountability plays an important role (Forrer et al. 2010; Shaoul et al. 2012; Bovens et al. 2014; Fombad 2015; Alfan and Zakaria 2012). Accountability has been widely studied, on both public as well as individual levels (Bovens et al. 2010). Over the years, accountability has gained a more prominent role in society. This has to do with the changing landscape as a result of globalisation. Theisens uses Bauman's concept of solid and fluid modernity to point out that the power of institutions is diminishing. Political parties, unions and religious institutions have less and less followers and have lost their once great level of authority. Instead, individual freedom has resulted in unpredictable behaviour of individuals and groups. These shifts in society are examples of 'a trend in which institutions crumble, borders fade, and individual freedom of choice increases' (Theisens 2012, 16–17).

This also means that such a society is increasingly difficult to govern by means of one centralised government. Decentralisation is, then, a way to cope with these changes. This includes putting local governments at work (Theisens 2012, 17) and increased networked cooperation (Petersen and Tjalve 2017, 10). The changing landscape in governance has also changed the way citizens perceive the government. Trust is an important aspect of that. Whereas before citizens had 'blind' trust in what the government did, now the government continuously has to regain the trust of its citizens. Consequently, accountability plays an important role.

Accountability is a widely studied phenomenon and many different academic traditions have different meanings for it. In social psychology, accountability is studied on an individual level. There, it is an enforcement mechanism, 'the social psychological link between individual decision-makers on the one hand and social systems on the other' (Bovens et al., 2014; 4). In accountancy, accountability is 'about the "exchange of reasons for conduct" and aims to "verbally bridge the gap between action and expectation"' (Bovens et al. quoting Messner 2014, 4). More relevant to this thesis, however, is the definition provided by public administration, which 'adamantly focuses on the public character of formal accountability. Its

focus is on systemic, structural forms of accountability for public service provision or governments' (Bovens et al. 2014, 4–5).

The public part of public accountability is especially important in a PPP. 'Public accountability mainly regards matters of public concern, such as the spending of public funds, the exercise of public powers, or the conduct of public institutions' (Bovens et al. 2014, 7). In a Public Private Partnership these matters are outsourced to a private party. The private party, then, needs to be held accountable by the public party, who in turn needs to be held accountable by the government. To that extent, accountability mechanisms come into play. 'In this usage, accountability is conceptualized as an institutional relation or arrangement in which an agent can be held to account by another agent or institution' (Bovens et al. 2014, 8). In a public institutions this accountability mechanism is focused on governing the behaviour of public agents in order to hold them accountable *ex post facto* (Bovens et al. 2014, 8–9). However, in a Public Private Partnership it is about governing the partnership in order to be able provide accountability on the partnership itself to the public at large. 'Accountability in PPPs requires the creation of proper safeguards to ensure that public services are not compromised for the sake of private profits' (Forrer et al. 2010, 477).

In an intelligence setting PPPs, as well as accountability within them, are more difficult to effectuate. Petersen and Tjalve have looked at democratic control and accountability in regard to public-private intelligence collection in the United States. They take as a premise that civil society is already involved in the process of intelligence gathering and that such an enlisting is a fact, beyond 'rolling back' (Petersen and Tjalve 2017, 2). They conclude that it is no longer viable for the Intelligence Community to address the problems of control and accountability "from 'within the framework of legal compliance' only" (Petersen and Tjalve 2017, 10). The field of intelligence studies 'must unpack what the governance implications of uncertainty really mean (Petersen and Tjalve 2017, 10). To address the problems of uncertainty regarding private parties in intelligence collection, the intelligence community must move beyond legal frameworks of compliance and toward a mode of governance and accountability. Petersen and Tjalve put forward two points of crucial importance. The first concerns political responsibility. It is the responsibility of the public party to clearly define national threats or interests. 'Without clear political leadership, the judgment that public and private actors are asked to exercise in the emerging intelligence networks will ultimately refer back to nothing' (Petersen and Tjalve 2017, 11). The second involves the issue of political opposition or dissent. It is important to create room for opposing views in order to avoid ending up in ineffective

groupthink. Established practice does not longer suffice for correct assessment in an evolving threat environment (Petersen and Tjalve 2017, 11).

PPPs have also been critiqued by many scholars (Bovaird 2004; Brinkerhoff and Brinkerhoff 2011; E.-H. Klijn and Teisman 2003; Roehrich, Lewis, and George 2014). Roehrich points out that 'it is intriguing to note […] that despite [PPPs] global prevalence, empirical evidence of benefits is mixed' (2014, 110). Pitfalls of PPPs include complexity, political exposure, rising prises (i.e. rise in charges), high costs of surveillance for governments, and lack of competition after a contract is procured (during renegotiations) (The World Bank Group (WBG) 2016, 69–70). Problems with regulation have also been a concern in PPPs (Pongsiri, 2002). It thus seems that many critiques surrounding PPPs are concerned with management. Issues such as complexity, political exposure, and regulation can be prevented through proper management and are inherent to a successful PPP.

2.3 - Performance Management.

With classic forms of governance relying on rules and legal frameworks becoming irrelevant, new forms of management arise. 'The classic rule-based bureaucratic form of governance has been challenged by the doctrine of performance management, which advocates that the managers of public service provision should be relieved of their rule-based constraints and instead held accountable based on their results' (Jakobsen and Mortensen 2016, 302). Salminem defines performance management as 'a process of establishing goals and regularly checking the progress made toward achieving those goals' (Salminen 2011, 1854). It is described profoundly by many other scholars (Jacobson and Ok Choi 2008; Latham, Sulsky, and MacDonald 2009; Mackie 2008; Roberts and Siemiatycki 2015; Salminen 2011; Sonnentag and Frese 2005). Performance management thus aims to reduce rule based governance and move towards output based governance. Performance management is concerned largely with accountability and is based on the new public management (NPM) doctrine. NPM was coined by Christopher Hood and it refers to 'a popularised mixture of management theories, business motivation psychology and neo-liberal economy' (Lynn quoting König 2009, 43).

NPM 'called for government to show its efficiency in expending public resources as well as prove that substantive results—or outcomes related to a program's effectiveness—had been generated by its activities' (Ewoh 2011, 105). Whereas before the public sector was the primary driver of reform initiatives, now privatisation and commercialisation were part of that

driving force (Glor 2001, 122). New public management has commonly been associated with performance management as new public management system. NPM has been characterised by 'a move towards performance management with the difficult task of defining performance specifications and creating the appropriate incentives which are essential for the system to function correctly' (Löffler 1999, 1).

Performance management is thus moving away from traditional bureaucracy and is a multidimensional tool that can be applied to a wide range of actors. Ranging from individuals, to government organisations, to companies in a PPP. Performance management is a mechanism to ensure a 'desire for continuous improvement' (Latham, Sulsky, and MacDonald 2009, 364) by people in the workplace. It allows management to set goals and provide feedback on them in order to 'increase self and collective efficacy so that even higher goals can and should be attained' (Latham, Sulsky, and MacDonald 2009, 365).

Relevant to a PPP in cyber intelligence is organisational performance management. Public private partnerships are the organisational manifestation of the attempt to 'combine the added value of governmental interference with the qualities of market-oriented parties' (E. Klijn and Teisman 2000, 84). Mackie proposes two distinct functions for performance management. First, intra-organisational performance management ensures 'appropriate internal controls to monitor the extent to which the organisation (and its sub-units) is achieving what it is supposed to achieve' (2008, 2). Periodic reviews by the organisation's management keep track of performance standards and trajectories, allowing for corrective action where deviations from desired standards are detected. Second, extra-organisational performance management facilitates communication of performance for the purpose of governance and accountability. Recipients are organisational stakeholders such as the government, funding bodies, audit agencies and the wider public (Mackie 2008, 2).

Furthermore, a common approach to performance management is described by Mackie (2008). It involves five steps. The first is to define and communicate a future state of affairs which serves as the rationale for objectives and targets which stretch organisational capability' (Mackie 2008, 2). Second, those aspirations need to be translated into long and short-term objectives, output and outcome performance indicators and targets against which performance and progress can be measured. The third step involves cascading ownership through different levels of the organisational structure, with each level 'having responsibility for specific objectives and targets which, if realised, contribute to the attainment of key performance indicators and outcomes which the organisation is charged with achieving' (Mackie 2008, 2). Fourth, management and organisational members need to recognise their collective and

individual accountability for performances attained. Without such accountability, systemic and comprehensive performance monitoring is next to impossible. Fifth, and last, reinforcement mechanism must be put in place. An appropriate set of both positive and negative incentives can promote positive consequences for success and negative consequences for under-performance against plan (Mackie 2008, 2). In order to implement these five steps, data need to be collected on the progress of performance.

2.4 - Performance Measurement.

'Performance measurement is a process of quantifying and reporting the effectiveness and efficiency of the action performed towards influencing organizational objectives' (Liu et al. 2013, 2). Many scholars have written on different performance measurement systems (PMS) (Koontz and Thomas 2012; Liu et al. 2013, 2014; Moynihan and Pandey 2010). A PMS is 'a structure in which strategic, tactical and operational actions are linked to process to provide the information required to improve the program or service on a systematic basis' (Liu et al. quoting del-Rey-Chamorro et al. 2014, 501). Components of a successful performance measurement of a PPP are input, process, output and outcome (Liu et al. 2014, 504). Outputs are defined as products and services delivered, while outcomes are defined as events or conditions that occur outside the partnership. Outcomes therefore follow outputs (Koontz and Thomas 2012, 771). Keeping track of those components allows for clarity throughout the process and fosters an accountability environment which is key in any PPP (Forrer et al. 2010).

Performance measurement, however, is only one part of performance management. The second part of the concept, management, is equally critical. Performance management is concerned with stakeholder management, regulation, and accountability (El-Gohary, Osman, and El-Diraby 2006; Forrer et al. 2010; Pongsiri 2002). Stakeholder management is important in any PPP, since stakeholder opposition can easily lead to project failure (El-Gohary, Osman, and El-Diraby 2006, 595). Regulation is important for both the public and the private side of a PPP. 'Regulations should be designed and administered to protect collective welfare, ensuring open competition and promoting the advantages of market discipline without strangling the market with unnecessary or unrealistic controls' (Pongsiri 2002, 488).

2.5 - Performance management critiques.

The study of performance management has not been without critique. Van Dooren et al. highlight the bipolarity of performance information. They argue that a bipolar view of

performance management ‘assumes a direct 1:1 relation between performance information and managerial or policy decisions’ (van Dooren, Bouckaert, and Halligan 2010, 96). It is thus fed by a certain technocratic hope that performance information will answer everything, from accountability problems to reward schemes. However, performance management systems almost never can do that (van Dooren, Bouckaert, and Halligan 2010, 96). Others point towards challenges surrounding tunnel vision (Soss, Fording, and Schram 2011), goal multiplicity (Behn 2003), monitoring complex program objectives (Amirkhanyan 2009) and opportunism in performance management (Negoita 2018, 3).

3 - Making a PPP in cyber intelligence work: critical success factors based on performance management.

Scholars (Bruin 2007; Ebrahim 2005; Forrer et al. 2010; Heinrich and Marschke 2010) have extensively studied the design of performance management in such a way to address the challenges posed above. In order to overcome those challenges and create a successful Public Private Partnership, critical success factors (CSF) for such a partnership need to be established. This section will look into what CSFs are, what common CSFs in PPPs are and which CSFs can be defined for a PPP in cyber intelligence.

3.1 - Critical Success Factors.

In 1988 York P. Freund identified CSFs as 'the hottest management buzzwords' (1988, 20). Freund defined CSFs for companies through the words of John Rockard as 'those things that must be done if a company is to be successful' (Freund 1988, 20). Rockards definition is rooted in the private sector and was later developed by Brotherton and Shaw who define CSFs 'as the essential things that must be achieved by the company or which areas will produce the greatest "competitive leverage"' (Fryer, Antony, and Douglas referencing Brotheron and Shaw 2007, 502). CSFs are then defined not as objectives but as managerial tools to achieve the organisation's goals. However, the public sector is not set to gain a competitive edge. In the public sector CSFs can be defined as those 'areas that must be given special and continual attention to bring about high performance' (Boynton and Zmud 1986, 17).

For a Public Private Partnership in cyber intelligence, critical success factors are defined differently than a PPP in, for example, infrastructure or public works projects. Those PPPs often involve CSFs surrounding risk allocation, private consortium and transparent procurement (Osei-Kyei and Chan 2015, 1342). The sensitive nature of a PPP in cyber intelligence demands critical success factors in other areas. Important to a PPP in cyber intelligence are factors surrounding governance and proper management of the partnership process in order to guarantee accountability and democratic control.

A PPP in cyber intelligence cannot be put into a framework of legal compliance alone (Petersen and Tjalve 2017, 10). This section will set out on three CSFs based on the work by Forrer et al.: (1) synergy and trust; (2) goal-definition; and (3) public added value. Forrer et al. describe public-private partnerships in relation to the public accountability question. In their article *'Public–Private Partnerships and the Public Accountability Question'* they provide a

framework to assist public managers in effectively exercising accountability with PPPs (Forrer et al. 2010, 475). Six dimensions 'that shape the relationships forged in public–private partnerships' are offered (Forrer et al. 2010, 475). For the three CSFs described in this research project, especially the final two dimensions are important: partnership collaboration and performance measurement. The first CSF, synergy and trust, is derived from the dimension partnership collaboration. The second and third CSFs, goal-definition and public added value, are derived from the dimension performance measurement. Furthermore, the third CSF is complimented by an article written by Alnoor Ebrahim, who has written on the importance of organisational learning in organisations.

All three CSFs are related to each other. Each CSF needs 'special and continuous attention' (Boynton and Zmud 1986, 17) in order for the PPP to succeed. On its own, each CSF is important, but rather than maximizing each CSF as a stand-alone entity the ultimate goal is to maximize all three CSFs as one coherent unit. The underlying coherence between the three CSFs is based on shared values between each PPP stakeholder. Both the private and the public sector know the need to increase cyber security against all forms of threats (Nationaal Cyber Security Centrum (NCSC) 2017, 11–15). In designing a PPP in cyber intelligence both the public side and the private side value trust, goal-definition and added value.

3.1.1 - CSF 1: creating synergy through trust.

Creating synergy is about establishing trust. An important underlying reason to create a PPP in cyber intelligence is generating solutions that would have otherwise not been possible (i.e. synergy). 'Achieving synergy demands a true partnership in which the partners are willing to discuss their perceptions and goals in a search for new solutions' (E. Klijn and Teisman 2000, 92). However, this creates a problem of trust. Both parties need assurance that outcomes of the partnership will not hurt them (E. Klijn and Teisman 2000, 92). Trust is therefore necessary to create an environment in which those innovative ideas can be put on the table, with guarantees that the interests of partners will not be hurt.

However, opportunism is always luring, even with guarantees. Ideally there needs to be a certain level of intrinsic motivation next to the profit motivations of a company. However, this is a panacea. For the private side return on investment is most important and trust needs to be built based on results. Building trust is therefore closely linked to a well thought out performance measurement system. Being able to prove that what is promised is also delivered builds trust (Grossman 2012, 598). 'Trust implies an integration of ideas, communication, and action, and performance is well identified by the success of this integration. Public-private

partnerships (PPPs) challenge our understanding of how multisectoral relationships occur and function to achieve new avenues for policy management and how we view performance' (Grossman 2012, 298).

On the public side trust is equally, if not more, important in a cyber intelligence PPP. Given the sensitive nature of the PPP, the government needs assurance that the private party will not take advantage of the information that is being collected. To that extend, the nature of the partnership is important. 'Moving toward a long-term relationship based on trust and commitment shifts the contractual basis of the PPP from a traditional contract to a relational one' (Brinkerhoff and Brinkerhoff 2011, 6). However, ultimately a PPP 'is "not a marriage, but a business relationship"' (Forrer et al. quoting Kee et al. 2010, 481). In that sense '"trust but verify" might be a more appropriate goal' (Forrer et al. 2010, 481). A network relation, however, does create 'a stream of future benefits which increases the chances that partners will remain working together' (E. Klijn and Teisman 2000, 92). In that regard, it is beneficial for the private party to give assurance, keeping long-term income in mind.

Trust is thus developed through performance measurement. For the agent, trust is developed through establishing, and agreeing upon, functions of performance measurement and the intended forums for dealing with performance measurement results (de Bruijn 2007, 58). This creates an environment of trust in which both principal and agent are comfortable to engage in a dialogue on the figures of performance measurement. This type of interaction between principal and agent avoids gaming of numbers and suspicion (de Bruijn 2007, 59). Once agreed upon, the functions and forums remain unchanged to create predictability and enhance trust in the system as well as between the principal and agent (de Bruijn 2007, 61).

Trust is also important to avoid groupthink. As mentioned before, in an ever evolving threat environment, established practice does not suffice as a guarantee for successful assessment (Petersen and Tjalve 2017, 11). Especially in cyber intelligence, the threat environment is changing rapidly. In such an environment, sticking to established practice can result in groupthink. To avoid such a scenario, the PPP needs to be open to contradiction. To steer away from blind consensus, a continuous discussion needs to be able to take place to question the process and improve it according to the threat environment (Petersen and Tjalve 2017, 11). In that sense, performance measurement information is critical. Meaning making related to performance measurement results can contribute to groupthink. The first meaning, if left unquestioned, institutionalises. It often survives longest, which can be catastrophic if it misrepresents reality (de Bruijn 2007, 77–78). Therefore it needs to be challenged in a trusted environment.

3.1.2 - CSF 2: clear goal definition.

The second critical success factor concerns goal definition. Goal definition is critical to creating a performance management system (Ferreira and Otley 2009, 266–67). Especially in a public private partnership in cyber intelligence it is important to establish what the government expects from the private party and what a national cyber security threat constitutes (Petersen and Tjalve 2017, 10–11).

When establishing goals it is important to distinguish between output and outcome. A public private partnership in cyber intelligence needs to establish goals that go beyond organisational limits (output) and contribute results that would not have been possible without the partnership (outcomes). However, these outcome measures are difficult to define since a PPP is a multiple-value activity in which criteria can be contradicting and can demand ever-changing trade-offs. 'Unambiguity does not work in an ambiguous world' (Bruin 2007, 80). This multiplicity implies that goals may be defined in many ways, and can therefore be measured and assessed in many ways. The goals that need to be established thus have to be embedded in a variety of criteria relating to product definitions, performance indicators, methods of measurement and ways of forming a judgment (de Bruijn 2007, 56).

The goals that are defined need to be developed into a performance management system in order to track the process of reaching those goals. 'The quality—or validity—of output and outcome measures is a fundamental component of any performance management system' (Koontz and Thomas 2012, 770). The performance measurement system is specific to the PPP. 'The development of performance measures can be understood as an interactive dialogue between principals and agents that provides a valuable learning forum' (Koontz and Thomas 2012, 770). In this regard, the public sector forms the principal and the private side takes up the role of the agent.

Developing performance measures is also important in establish accountability within the PPP. Performance measures are then 'helping managers on both sides engage, assess, and continuously improve organizational results; and strengthening accountability in the partnership' (Forrer et al. 2010, 481).

Important in the PPP is the periodic revision of performance measurements. It is only when the measurements are 'tried, evaluated, modified, and/or discarded that agents' responses become known' (Heinrich and Marschke 2010, 203). Feedback by both the principal and the agent is important to create a dynamic performance measurement system. It is up to the

principal to '[learn] faster than the agent, [so that] the usefulness of a performance measure is more likely to increase' (Heinrich and Marschke 2010, 203).

Ultimately Velotti describes partnership performance in an apt way: 'partnership performance is defined as a set of innovative ways of working that reinforce the process and sustainability of the relationship' (2012, 342).

3.1.3 - CSF 3: public added value.

The third critical success factor concerns public value added. This CSF ensures that the PPP in cyber intelligence actually adds to the value of the public. A PPP can unfold in two different ways. The first relates to efficiency: 'securing the same outcomes for lower costs'; the second concerns added value: 'greater outcomes for the same cost' (Steijn, Klijn, and Edelenbos 2011, 1237). This CSF focusses on the second, added value, because the aim here is about adding value through a PPP (see also CSF 1). Steijn et al. define added value in more detail: 'Public and private actors can add value to each other's performance because their efforts enhance the value of the product or service that is being delivered' (2011, 1237).

In a PPP, then, added value begins with organisational learning. Learning in this sense means 'improving actions through better knowledge and understanding' (Ebrahim 2005, 67). It is a process of feeding performance information back into the organisation and changing processes for the better. It thus goes beyond establishing shortcomings. 'Simply identifying shortfalls in organizational performance and assuming that the information will be used by the organization to improve performance is insufficient for ensuring actual change' (Ebrahim 2005, 67). The continuous process of feedback on performance measurements will ultimately lead to a better, more dynamic performance management system (de Bruijn 2007, 58). Furthermore, evaluation of the performance management system will help in establishing accountability. 'Performance measures increase accountability to the public, and they encourage and codify shared commitments and responsibilities' (Forrer et al. 2010, 478).

Continuous performance management feedback, then, results in more dynamic performance management and ultimately higher performance (Heinrich 2002, 716). In that sense, it contributes to a more efficient process, resulting in more outcome at the same cost.

> 'The challenge of managing public-private partnerships is thus to create extra value by using the knowledge and resources of the partners while at the same time fostering a minimum level of trust in the relationship and achieving concrete outcomes, which are the actual realization of the extra value' (E. Klijn and Teisman 2000, 93–94).

4 - Methodology.

4.1 - Design.

This study involves a qualitative holistic single case study. It takes a single case with one unit of analysis in order to test the validity of the three CSFs mentioned above as the basis for answering the research question. The case is a PPP in cyber intelligence in the Netherlands. However, at the moment of writing this research, the Netherlands knows no PPP in cyber intelligence. Therefore, there is no known case that can be studied. This, however, does not mean that the CSFs cannot be tested. This study will focus on a hypothetical case involving the Dutch government and private sector cyber intelligence companies. It will use interviews with experts from both the public and the private sector to see whether these CSFs would be as important as the literature suggests. It is a revelatory case, because it reveals a phenomenon that has hitherto been unexplored in this context. It is a holistic case study, because the case is also the unit of analysis. The case, thus, hypothesises a PPP in cyber intelligence in the Netherlands.

Case study research has been a critical part of social science for many years now. This has also contributed to a vast amount of differing definitions. Gerring defines case study as 'the intensive study of a single case for the purpose of understanding a larger class of cases (a population)' (Gerring 2009, 95). Yin defines the case study as:

> 'an empirical inquiry about a contemporary phenomenon (e.g., a "case"), set within its real-world context—especially when the boundaries between phenomenon and context are not clearly evident' (Yin 2009, 18)

For a PPP in cyber intelligence this is true. The boundaries between the phenomenon and context are indeed vague. Case study research 'assumes that examining the context and other complex conditions related to the case(s) being studied are integral to understanding the case(s)' (Yin 2012, 4). As a concept, a PPP can be applied to various different situation and purposes. Context and other conditions are therefore important to understand how a PPP would work in cyber intelligence. A PPP in cyber intelligence, then, deserves a closer look in the form of a case study, in order to find out what critical success factors can effectuate it. Furthermore, the CSFs that are studied are also valuable to other types of PPPs. Since subjects such as

accountability, performance measurement, partnership collaboration, and social and political impact can be found in other PPP frameworks as well (Forrer et al. 2010, 479).

4.2 - Defining the case.

One of the benefits of case study research is that a phenomenon is studied within its real world context and data is collected in a natural setting (Yin 2012, 5). The context in this case is cyber intelligence collection. The case is holistic, because it focusses on one unit of analysis (i.e. the PPP in cyber intelligence) and is set in the cyber intelligence collection context.

The case draws on the three CSFs outlined earlier. In order to be able to answer the research question, the three CSFs derived from the literature on PPPs have to be tested in a real-world context. To collect data to test these CSFs interviews will be held with experts from both the public and the private sector. The data collected from the interviews will be complemented by document study.

4.3 - Data collection.

The critical success factors will be tested in two ways. The first is semi-structured interviews. Three interviews will be held with public experts in the field of cyber security and intelligence. On the private side, three interviews will be held with experts in the private sector of the same field.

The reason a semi-structured approach is preferred is because the critical success factors are not set in stone.

> 'The flexible format permits open-ended interviews, if properly done, to reveal how case study participants construct reality and think about situations, not just to provide the answers to a researcher's specific questions and own implicit construction of reality' (Yin 2012, 12).

The second way of testing the CSFs is document analysis. Document analysis is a systematic procedure for reviewing or evaluating documents—both printed and electronic material (Bowen 2009, 27). Documents include both organisational and institutional documents. Examples are government publications, newspaper articles, websites, and company reports. Documents contain text and, in some cases, images that have been recorded without the researcher's intervention (Bowen 2009, 27).

It is important to operationalise the three CSFs according to the case (see also table 1). The goal is to reveal how respondents construct reality surrounding the three CSFs in relation to the PPP in cyber intelligence. The interview consists of sixteen questions surrounding the three CSFs (see also appendix A). The first CSF, Synergy and trust, is defined as trust building and open collaboration amongst stakeholders. Trust building and the role performance management plays in trust building can be viewed differently between participants and especially between sectors (public vs. private). Open collaboration amongst stakeholders is then important to establish trust (Forrer et al. 2010, 481). The second CSF, goal-definition, is defined in context of the case through definition, process and accountability. That is, definition through output or outcome, tracking the process of reaching goals defined and accountability measurement. Lastly, added value is defined through organisational learning and expertise. The role of organisational learning in a PPP and how it can contribute to adding value. Expertise concerns added value of the expertise of the private sector.

CSF	**Operationalisation**
Synergy and trust.	Building trust and creating an open collaboration amongst stakeholders to reach innovative solutions.
Goal-definition.	The end-to-end process of establishing goals: defining goals, reaching goals and accounting for goals.
Added value.	Adding value through organisational learning and private expertise.

Table 1: operationalisation of the three CSF.

The semi-structured interviews are held with experts in the public and private field on cyber security. The case hypothesises a PPP between the Dutch government and private sector cyber intelligence companies. Therefore, three experts from private cyber security companies are interviewed. In the private sector experts from leading governmental bodies on cyber security are interviewed. Through interviewing experts in both the public and private field a clear image is generated which sheds light on how both sides would construct a PPP in cyber security.

The interviews have been recorded for purposes of transcription, but also for increased transparency and control. Furthermore, recordings will increase the quality of the data and can provide additional insight to answering the research question (Boeije 2005, 60–61). The respondents have been anonymised and are identified through an initial (PU = public, PR = private) and a number (1, 2 or 3). After the raw data are processed into transcripts, the data is

organized and coded. A code ‘is most often a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data’ (Saldana 2009, 3). The transcripts are divided into portions which can be coded, those portions are given a code. Ultimately, these codes will form a pattern which can be analysed vis-à-vis the three CSFs identified in the literature (Saldana 2009, 3–4) (for the codebook see appendix B).

4.4 - Validity and Reliability.

In any research project it is important to establish validity and reliability. Many scholars have written about the importance of reliability and validity (Golofshani 2003; Morse et al. 2002; Noble and Smith 2015; Riege 2003; Rolfe 2006; Whittemore, Chase, and Mandle 2001). In qualitative research, reliability can be defined through dependability and consistency. ‘The consistency of data will be achieved when the steps of the research are verified through examination of such items as raw data, data reduction products, and process notes’ (Golofshani quoting Campbell 2003, 601). Validity, then, is not a fixed or universal concept, rather it is ‘a contingent construct, inescapably grounded in the processes and intentions of particular research methodologies and projects’ (Golofshani 2003, 602). Validity is thus dependant on the type of research that is being conducted.

However, qualitative research needs some sort of qualifying check or measure, whether validity and reliability are clearly definable or not. To test reliability and validity in qualitative research a much used technique is triangulation of data.

> ‘Triangulation has risen an important methodological issue in naturalistic and qualitative approaches to evaluation [in order to] control bias and establishing valid propositions because traditional scientific techniques are incompatible with this alternate epistemology’ (Golofshani 2003, 603)

Triangulation combines several methods or forms of data in order to come to the same conclusions with different sources of information and is used to provide ‘a confluence of evidence that breeds credibility’ (Bowen 2009, 28). This research project also uses triangulation to establish reliability and validity. Three sources of data are used: academic literature, document analysis and interviews. However, triangulation of data will only result in reliable and valid research when the data is collected in the right way. Only than can reliable and valid research lead to generalisation (Golofshani 2003, 603).

In this research interviews and document analysis are combined to verify the three CSFs that have been deducted from academic literature. Interviews are a valuable source of information but can also be prone to researcher bias. 'The interaction between the researcher and participant has the potential to yield disjunctures in meaning and intent' (Galletta and Cross 2013, 103). In order to address researcher bias, reflexivity is engaged with.

> 'Through reflexivity, the researcher looks within the research activities, as well as within the relationship between the researcher and her or his participant, in order to locate potential interference' (Galletta and Cross 2013, 104).

This is also done for the interviews held for the purposes of this research. 'Interference of some kind is predictable in both quantitative and qualitative research' (Galletta and Cross 2013, 104). Any interference that is found is therefore documented. In this sense, it becomes part of the overall analysis of the data. To that extent it helps to identify the limitations of research, but also to establish hitherto unexplored dimensions important to the research question. Any interference relevant to the study will be reviewed in the next chapter.

In addition to reflexivity, document analysis will be used to validate the data. In document analysis the documents that are being analysed are written truth. These documents have been recorded without any interference by the researcher. Combining these three sources of data, findings can be corroborated 'across data sets and thus reduce the impact of potential biases that can exist in a single study' (Bowen 2009, 28).

5 - Analysing the Data.

Having established three CSFs in chapter three and a clear methodology to test those CSFs in chapter four, chapter five will analyse the data that has been collected. This process will be twofold, since data have been collected through document analysis and semi-structured interviews. Each critical success factor will be scrutinized by the data. Both document analyses, coding data and interview citations will be used to analyse the CSFs.

The case under scrutiny describes a partnership in which private companies collect intelligence in collaboration with the Dutch government. The case, however, is a hypothetical one, since in the Netherlands there is no such partnership at the time of writing. Respondents therefore

answered the interview question by relying on experiences in PPPs in intelligence sharing. Although intelligence sharing and intelligence collection are two different practices, experiences in cyber intelligence sharing initiatives does provide valuable insight in how a PPP should be governed and managed. Furthermore, respondents pointed out that private companies, in securing their own digital infrastructures, collect cyber threat intelligence.

> '[I think private company expertise can be of added value] because companies see a lot in the protection of their own infrastructure and gather a lot of information. And that infrastructure and that information is not readily available to the intelligence services. So that will definitely have an added value. I think they have information that is not available to the intelligence services at any given time' (PR 3).

The following section analyses the data acquired through the interviews and analyses whether the critical success factors could allow for a PPP in cyber intelligence.

5.1 - Analysing synergy and trust.

All respondents, both public and private, found trust to be an important, if not the most important, factor in the PPP. One respondent in the private sector identified confidence building measures as the most important underlying factor of building trust in a cyber intelligence PPP. Confidence building measures included contractual agreements enforceable in Dutch court, expertise to check products delivered and, to some extent, trust on a personal level.

> 'So you are talking about trust, trust is fun, but control is better' (PR 1).

Other respondents identified trust on a personal level as most important.

> 'What is especially important for trust is that you know each other personally. It is all about, personal contacts, occasionally drinking a drink together. Really working on informal trust' (PU 3).

Trust on a personal level is thus an important factor in a cyber intelligence PPP. This is furthermore demonstrated by a PPP set up in 2016, when a Dutch company was extorted for a period of six weeks. In order to prevent the criminal from executing the extortion, a PPP

between the Dutch police, the Team High Tech Crime, external experts from a consultancy firm and the company under attack, was initiated (Kop 2016, 12). This PPP was established quickly as a reaction to the case at hand which brought with it several dilemmas. One of the dilemmas involved sharing information amongst partners.

> 'One dilemma in the PPP is which information can or may be shared. This was not immediately clear at the start of the cooperation, but later, when permission was granted to share all relevant information to the case, the parties involved found sharing that information rather uncomfortable at first' (Kop 2016, 13).

The lack of trust amongst partners created the uncomfortable atmosphere. The PPP, in this case, was established in a rapid pace and there had not been established a relationship of trust. Building trust is important when establishing the PPP for sake of sharing sensitive intelligence between stakeholders. Trust is needed not only on an organisational level, but also on a personal level.

Furthermore, respondents identified continuity as an important factor in establishing trust. Continuity in the PPP, then, revolves around sending the same person time and time again, as one respondent pointed out:

> 'What I have noticed, what works, is that if you have a form of cooperation, you always send one and the same person. Because you get confidence at an individual level and not at company level. Trust you build up by seeing each other often and getting to know each other and then it is a question of one person taking a leap, so that the rest can follow' (PR. 2).

Continuity also comes forward in a report written by TNO[3], in which cyber security information sharing in top-sectors is explored. Part of the exploration is a closer look at the ISACs, that already share cyber security information and is set up as a PPP. The report identifies two success factors, namely trust and value.

> 'After all, information is only shared with parties or persons who are trusted. Parties only participate in an information exchange initiative if they themselves gain added

[3] Dutch organisation for applied scientific research.

> value. Otherwise enthusiasm decreases quickly. Commitment and continuity of the participants contributes to building trust' (Huistra and Krabbendam-Hersman 2017, 15).

This information sharing initiative is twofold, the government shares cyber security intelligence with private parties and vice versa. That way the partnership creates an outcome that would not have been possible without the partnership. Neither the government or the private party has the capacity to provide all the information the partnership ultimately offers. One respondent put it as follows:

> 'No one is able to know everything he needs to know in order to secure himself or to secure our society. So I think that information sharing is really the key to, together, keep our society digitally safe. It is too large and too wide to have an isolated approach. You have to do that in collaboration' (PR 3).

For the private side, the CSF identified opportunism as a possible hurdle in the PPP. Both for the private and the public side. The interviews reveal that the majority of respondents does not find opportunism to be a hurdle in the cyber intelligence PPP. One respondent stated that opportunism would not be a problem because the intelligence PPPs in the Netherlands are formed bottom-up instead of top-down.

> 'No, I do not see [opportunism] as a problem. Everyone is there with their own interests, to make your own company safer, but there is also a group interest, to make the entire sector safer. This comes partly from the chain responsibilities, because you depend on each other and all have systems that are connected to each other. In addition, it is also the believe in the cyber world that you cannot do it alone, you can invest in cyber security yourself as much as you want, but you have to work on it together eventually' (PU 3).

What is interesting about this particular quote is that the private sector too has an intrinsic motivation to collect and share intelligence. For them, the return on investment consist of increased cyber security of the company, but also of the sector. It is therefore different from the traditional motivation based on financial gain, one of the underlying reasons the CSF identified opportunism as a possible problem.

On the public side, the CSF identified, a long-term relation would be important to prevent opportunism. One respondent linked opportunism to the duration of the partnership:

> 'If a private party steps in to acquire knowledge and then bring a product to the market, it is something different than trying to make the Netherlands safer over the next ten years. So I think that there is already a big difference there. How you can prevent that? I think that requires contracts. Is it completely preventable? I do not know that, but people should especially have the idea that it is a long-term cooperation to achieve a certain goal' (PU 2).

A long term relationship is thus desirable in a cyber intelligence PPP. However, it becomes less of a problem when the public side of the partnership has an intrinsic motivation at the base of their partnership participation. Nevertheless, a long-term cooperation contributes to building trust.

Another important factor in the cyber intelligence PPP is confidentiality. Almost all respondents referred to confidentiality as an important factor in establishing a trustworthy environment in which intelligence can be shared. This is important not only for building trust, but also for creating a platform in which public and private parties can contradict each other. Interesting to see is that it is equally important for public and private that information is shared confidentially.

> 'For private companies it is very difficult to share something that you think is good for the Netherlands to know, intelligence that is vital, and then a WOB[4] request can come and it can be revealed that it was your company that had the vulnerability the information came from, many companies find that difficult' (PR 2).

Assuring that the intelligence that is shared will remain confidential is thus an important part of the cyber intelligence PPP. The traffic light protocol (TLP)[5] is one example used in the ISACs that provides such confidentiality.

[4] WOB stands for 'Wet Openbaarheid Bestuur' which can be translated into English as the Freedom of Information Act.

[5] The TLP consists of four classifications of information sharing, ranging from red (only for those participating in the meeting. TLP red also mean no minutes) to white (public information that can be spread freely).

> ‘[Trust] is really about meeting the same membership requirements, for example using traffic light protocol (TLP). You should actually be able to guarantee that the other party deals with information the same as you do yourself’ (PU 3).

The CSF synergy and trust describes the importance of performance measurement in building trust. The interview data shows that half of the respondents finds a performance management system valuable to establish trust, while the other half does not. One respondent even remarked that a performance management system would be counterproductive in establishing trust:

> ‘My experience is that [a performance management system] does not help per se and that it is just counterproductive. Involved parties often have a flawless feeling whether they still trust each other or not. People have that too’ (PR 3).

Other respondents did find performance management to be valuable when it comes to establishing trust. However, they did not think a traditional performance management system as described by the literature would contribute to trust. Rather, an implicit form of performance evaluation, in an informal way, would. This operationalises as informal updates on how different stakeholders have progressed since the previous meeting.

> ‘After each meeting you ask the question: how did it go? But nothing is recorded or something’ (PR 2).

Concrete performance management systems, as described by new public management, are thus less important in building trust. More important, respondents suggested, are membership criteria.

> ‘If a new member is added, it will be discussed and if the case is 'well they only want to join to get something’ then we do not agree with that. With all those meetings I have now, there is an interview with new members: what will you get from us, but also what will you bring to the table? Then that is submitted to the group, but if the group says no, it will not happen’ (PR 2).

Lastly, a sustainable open collaboration can contribute to establishing trust within a cyber intelligence PPP. Respondents identified equality and transparency as important factors in creating a sustainable open collaboration. Equality is important in the starting phase of the PPP.

> 'I think that you have to start a process together from the beginning. So there does not have to be a party that has more interest or a more important share, you have to keep that equal as much as possible' (PU 2).

Furthermore, transparency is important in establishing a sustainable open collaboration which can establish trust. One respondent highlighted the importance of dialogue in that regard:

> '[…] especially the conversation is important. You see that it works well and that everyone is always open and transparent about what he can and cannot deliver' (PU 3).

One respondent suggested a co-operative[6] as a strategy to ensure a sustainable open collaboration between PPP stakeholders.

> 'There [the co-operative] they can go to for consultancy and best practices . The large companies will use it more, so they pay more, they have a platinum contract so to speak and then you have silver and the small companies have a bronze contract. Everyone takes what they need, but they help each other' (PR 2).

In conclusion the CSF synergy and trust proves to be invaluable to a PPP in cyber security. Personal level trust is important in establishing trust on a higher level, between organisations. In establishing trust between persons, continuity is important. To that extent, a long-term PPP is desirable, since that can prevent opportunism. Although most respondents did not think opportunism would form a problem, because the private sector feels equally responsible for a safe cyber security environment in the Netherlands and finds its return on investment in increased cyber security. For the private sector, however, it is important that the cyber intelligence that is shared remains confidential, an important factor in establishing and maintaining trust, but also for creating an environment in which parties can contradict each

[6] A co-operative can be defined as 'A co-operative is an autonomous association of persons united voluntarily to meet their common economic, social, and cultural needs and aspirations through a jointly-owned and democratically-controlled enterprise' (International Co-operative alliance n.d.).

other. Performance management, in that regard, has divided opinions when it comes to contributing to trust building. It can be used to build trust, but it has to remain informal. Lastly, a sustainable open collaboration can be created through equality and transparency.

5.2 - Analysing goal-definition.

The data show that goal-definition is an important part of a cyber intelligence PPP. All interview participants found goal-definition to be important. Almost all respondents mentioned equality and outcome as key factors in the goal-setting process. Equality, then, refers to creating goals together.

> 'You [define goals] together, you put the dot on the horizon together. This often happens through discussions about an annual plan. But you also know that parties will no longer participate if the partnership cannot offer them anything. In order for that PPP to work, each party must get something out of it, otherwise you will see that they do not show up any more' (PU 3).

Although goal-setting is best done together, the government can play an important role in creating a fertile environment in which a PPP can grow. On 24 April 2018 minister Grapperhaus of Justice and Security presented the Dutch National Cyber Security Agenda (NCSA) (NCSC 2018). The Dutch cyber security agenda was part of the new coalition agreement, made in 2017. One clause in that agreement pertained the cyber security agenda, stating that:

> 'An ambitious cyber security agenda will be drawn up, including standards for Internet-of-things devices, encouraging companies to make safer software through software liability, strengthening the National Cyber Security Centre (CCSC) as contact point for Computer emergency response teams (CERT) of all sectors, encouraging cybersecurity research and improving information campaigns in the field of cyber hygiene' (Kabinet Rutte III 2017, 3).

The cyber security agenda that followed consists of seven strategic starting points. The NCSA is accompanied by a new Dutch cyber security alliance, which uses the NCSA as its foundation.

> ‘We have laid the foundation for this cooperation in recent months with all involved public, private and other social actors, in the form of our Dutch Cyber Security Agenda: An ambitious, cabinet-wide agenda, with which we take a crucial step towards a safer digital Dutch society. That is a top priority for this government’ (Grapperhaus 2018).

The NCSA is thus a document with goals-defined through a cooperation between public and private parties. The cyber security alliance is a public private partnership which aims to enforce the seven strategic starting points of the NCSA. To that end, the NCSA suggests not only goals, but also measures which should be taken to achieve those goals. Although no specific operationalisation of how those goals and measures will be achieved or implemented is provided in the NCSA, it does pronounce the need for development and evaluation in a PPP approach to increased cyber security. ‘The approach can only be successful if it is designed, further developed and evaluated in close public-private partnerships’ (NCTV 2018, 43).

To that extent, one respondent suggested that the government has an important role in establishing the foundational layers of a cyber intelligence PPP.

> ‘[…] I think that the government must initially play an exemplary role in sharing the information that they have with private parties, without affecting national security. And then hopefully the business community sees that they have an ally in the government and that it is a reciprocal partnership’ (PU 1).

The goals defined in the NCSA are a good example of how difficult it is in PPPs on cyber security, and in line with cyber security, to set measurable goals. One goal that is set, as part of the strategic starting point ‘adequate strength’, concerns insight and detection. ‘Organizations that are vital to national security have a better understanding of digital threats and attacks, and are capable of detecting attacks that threaten them and thus national security’ (NCTV 2018, 19). Measuring such a goal is difficult, to say the least, because criteria to reach those goals can be contradicting for different parties. Furthermore, it is hard to establish when such a goal is reached.

However, outcome was still preferred over output by the majority of respondents. The interview data thus reveals that goals should be set broadly, because the cyber domain is changing rapidly and therefore it is difficult to create a concrete product.

> ‘It's more about learning from each other, so that's the outcome, that you're all better off, than that you have a beautiful document as output’ (PR 2).

One respondent highlighted the importance of maturity. It depends in which phase the PPP is when deciding to focus on output or on outcome.

> ‘I think that in the beginning you have to focus on output, ensure that the intelligence exchange really gets going . In a later phase you have to start focussing on outcome, but directly going for outcome is difficult and can lead to opportunism, scoring urgency’ (PR 3).

One respondent preferred output over outcome. In this case, the goals have to be set by the government and the public party has to provide a product. That can be information or an application.

> ‘[Goals should be set] by the customer, by the government. I want something from you, the public company, this is what I want from you, and this is what it should be able to do’ (PR 1).

What is supposed to be delivered should then be set in a contract, with a fixed price and a fixed date of completion, according to the respondent. Furthermore, there needs to be a problem owner, a project leader, provided by the government who can oversee the project.

> ‘The client, the government, must set up a project manager who will remain project leader until the project is completely finished’ (PR 1).

The second CSF is also concerned with tracking the process of reaching the goals that are defined. The PPP established to prevent extortion put forward transparency as an important factor of that process:

> ‘Transparency ultimately provided understanding for each other's position and interests, which positively influenced the cooperation between the police, the Public Prosecution Service and the company’ (Kop 2016, 14).

However, one respondent pointed out that transparency and openness is the result of a bureaucracy. The advantage of a bureaucracy is that when a certain goal is reached, it can be traced back through certain steps that have been defined.

> ‘That is something the government always does and why we have a bureaucratic environment. But we do that to be open and transparent to the people of the Netherlands’ (PU 2).

This is different from the private sector approach, in which bureaucracy is viewed as time consuming and costly. In the private sector it is important to act and react quickly. However, the downside is that it is not always possible to justify why certain steps were taken.

> ‘I think the power of such PPP is that you get a mix. Always asking everything to six people and being bureaucratic, that is not a quick way and certainly not in this domain’ (PU 2).

Being able to justify steps taken, however, is a way to ensure accountability in the cyber intelligence PPP. The CSF identifies performance measures as an important instrument to establish accountability in a PPP. Interview data, however, show that in practice accountability is thought to be established differently. One respondent provided a different approach to performance measurement and highlighted the importance of using a contract.

> ‘I have set goals myself and in my opinion the government only should do business with private IT companies with which you conclude a contract where they deliver on a fixed date, discuss well in advance what we want from each other, and then there is a fixed price and a fixed time’ (PR 1).

Other respondents had differing opinions. One did not believe in accountability and was convinced the cyber intelligence PPP needs to be on a voluntary basis.

> ‘[The Netherlands] is pretty unique in that. In America, for example, those ISACs are much more institutionalized. There they are based on many legal documents, with us it is really done on trust’ (PU 3).

One interviewee did think accountability was important. However, not in the traditional sense that the government needs to hold the public party responsible. Rather, accountability was established internally.

> ‘So then you are constantly busy with accountability. But that is something participating members arrange internally, so the private and public parties that participate will do that internally for themselves. I do not see anyone doing accountability together, but that is not necessary anyway, because everyone has to be accountable for themselves because everyone invests in it’ (PR 2).

However, establishing accountability in a cyber intelligence PPP through performance measures also forms a dilemma. Important then is to decide together to what extent information is written down. A performance management system can be valuable for measuring the effectiveness of intelligence sharing. However, writing down what is being shared and tracking to see if it is valuable can also lead to a decrease in trust. The result being that less information is shared.

> ‘If you are going to focus a lot on hard KPIs, for example, then it will come under a magnifying glass and that can sometimes be scary for people’ (PR 3).

In conclusion, the second CSF proves to be valuable to a cyber intelligence PPP. Data from the interviews and document study have revealed that important factors in goal-definition are equality and outcome. However, focussing on outcome is not without its dilemmas. Outcome goals are often broad and hard to define in a way that is easy to measure. Therefore, as one respondent pointed out, it is easier to focus on output goals when measuring goals is preferred, but not desired by other respondents. In terms of tracking the process to reach goals defined it is important to record steps to establish best practices. However, this too is difficult, since a bureaucratic process can slow down the process and create friction between public and private sides. Therefore, a mix between both processes was preferred by one respondent. Finally, accountability remains a difficult subject in a PPP. The literature suggests performance measures as an important factor in establishing accountability in a PPP. Although the interview respondents did think accountability was as important, it was not necessarily established through performance measures, rather it is established implicitly through internal accountability and intrinsic motivation.

5.3 - Analysing Public Added Value.

All respondents thought public added value was important in the cyber intelligence PPP and could be achieved through a cyber intelligence PPP. Furthermore, almost all respondents found public expertise to be of added value to the cyber intelligence PPP. All respondents identified organisational learning as a measure to achieve added value in the PPP. A majority of the respondents found that a Performance Management System could help in improving the learning organisation and therefore add value to the PPP overall.

One of the main reasons respondents thought the cyber intelligence PPP could add value was because both public and private cannot increase national cyber security alone.

> 'From a public point of view, it is of course the government's job to protect us and to protect companies. If you need information for your intelligence and security services, it helps if you have all the pieces of the puzzle, so if private can help with that, that's nice. From a private point of view, I think that if companies alone have to carry out that cyber battle it will cost a lot and they cannot do everything. I have noticed in all those years that working together really helps' (PR 2).

One respondent did find that the PPP in cyber intelligence could add value, but that it would be difficult in the Netherlands.

> 'I have not yet thought about it in terms of intelligence services. I think it is possible, but very quickly you will run into problems with legislation in the Netherlands' (PU 2).

Another respondent found public added value would be achieved through generating output by the private sector in partnership with the government.

> '[…] cooperation is fine, if that leads quickly to results in a great partnership, then that is fantastic' (PR 1).

This view moves away from other respondents because it is focussed on output. It revolves around the idea that the private sector delivers a product in exchange for a financial reward by the government. It therefore moves towards contracting out, in which the government buys a

product ‘of the shelf’. In this case, the product would be open source content for intelligence analyses, not the analyses itself.

> ‘I do not think we have private companies that can handle cyber intelligence. We do have private companies that offer applications, but you also have private companies that deliver content’ (PR 1).

The value that can be added by the private sector, respondents found, entailed knowledge and expertise. In that sense, private companies can provide intelligence that can help in creating analyses on a larger scale.

> ‘For us as a government it is important that we have that good relationship with private parties so that they inform us when something is going on and that we can use all the information we get to make larger analyses. So we can help others on how they can mitigate certain attacks, because we have the general oversight on [current cyber security issues]’ (PU 3).

Furthermore, the public sector can add value because it can provide information to the Dutch Intelligence and Security Agencies.

> ‘[…] it is very valuable for [the AIVD]. Because private companies have a lot of information that the intelligence services can use. We do not always know that, but I do think that it is true. Otherwise they would not invest, they are not in it for the fun’ (PR 2).

One respondent remarked that the area in which the private sector could add value was adoption. The cyber security domain is changing rapidly, therefore a PPP in cyber intelligence needs to be able to adapt to new situations quickly. Private companies are better able to do that than public organisations, so the respondent argued.

> ‘They are much faster at adapting certain technologies or linking different technologies together. I think that that is very much the added value of private companies’ (PU 2).

In creating added value the respondents found organisation learning to be important. The main way learning in the PPP could be established, according to the majority of respondents, was by sharing information and best practices. Perfecting the PPP in cyber intelligence is a process of trial and error and requires a hands on approach.

> ‘In terms of the learning organization, it is just doing things and after that you can find out that it does not work and you stop in order to go a different direction’ (PU 1).

The TNO report on cyber security information sharing described a trial and error approach used by the ISACs in their starting phase:

> ‘At the start of the ISACs the 'learning by doing' approach was followed. Learning came from experimenting and following a hands on approach, both successes and failures were useful in that regard. Those learning points were then applied’ (Huistra and Krabbendam-Hersman 2017, 15).

This is a clear example of organisational learning, in which it is important to continuously look for successes identified, but also failures identified, and to build on that. Through that kind of knowledge actions can be improved and value can be added.

To that extent, respondents also highlighted the importance of following up on best practices that are revealed in the PPP. One respondent added that a project leader can contribute to solving that dilemma:

> ‘[…] you are only learning if you have a project leader and your lessons learned, or now lessons identified, the things you have identified; you have to do something with that. The latter often is insufficient. Then there are beautiful reports with recommendations that are not used. So the learning organization with the government is a problem, because people always change. So you need an independent survey, such as the audit office or the CPB, which analyses every so often or checks to see that what is concluded is also processed. A learning organization is therefore certainly important, because that saves money’ (PR 1).

In this example, the project leader oversees the process of identifying lessons learned and an independent office checks whether the project leader implements lessons learned into the PPP.

Another example of organisational learning in a PPP can be found in the plan-do-check-act cycle proposed by the centre for crime prevention and security. In this cycle, a PPP is designed through four steps. Design, execution, evaluation and adjustment (Centrum Criminaliteitspreventie Veiligheid 2013, 4). The latter two steps are important for organisational learning, since the results of an evaluation are valuable knowledge which can be used to adjust the PPP for the better. The NCSA also touches on the point of evaluation. 'The progress of the cybersecurity approach will be monitored under the coordination of the NCTV and in collaboration with all parties involved and, where necessary, recalibrated on the basis of technological and social developments' (NCTV 2018, 44).

Organisational learning is not only important for improving the PPP as a whole, but also in improving operational aspects of a PPP. Such as communication, processes and working methods. The council of head-commissioners[7] issued a report on their vision of PPPs, stating that: '[PPPs] need added value not only in terms of effectively preventing crime, but also for regular organisation of work' (Raad van Hoofdcommissarissen 2005, 20).

The third CSF also identified a Performance Management System (PMS) as a way to contribute to organisational learning. Respondents found a PMS to be an important part of organisational learning too. By regularly checking progress in the PPP, it is possible to improve the intelligence sharing process, increase transparency and measure the effectiveness of information that is shared.

> '[With a PMS] you can check whether the learning has an effect. That depends on the KPIs that you name in such a PMS, but that will give an indication of whether we have made better use of that information, whether we have shared more or less information, or whether information had more or less effect' (PR 3).

However, this can also have a negative effect. Recording how information is shared and measuring if that information had any effect on increasing national cyber security also creates a tension within the PPP. It then comes down to outweighing values, putting performance measurement and trust on the scale.

[7] Council of the 26 head-commissioners of the Dutch police force.

> ‘Then [private companies] are hesitant to share things, because it ends up under a magnifying glass. [That is a consideration you have to make] and you can name that. That there is tension’ (PR 3).

Furthermore, it will always remain difficult to measure the outcome of a PPP concerning cyber security, as one respondent said:

> ‘It is always difficult to really measure cybersecurity, the same goes for the information exchange that takes place in ISACs, which is very difficult to prove. How much you actually earn in euros. That remains one of the larger issues in cyber security, which is actually the case for all security issues. If you put in a euro, how much security will come out’ (PU 3).

In conclusion the third CSF, public added value, also proves to be important for a PPP in cyber intelligence. In adding value, the data shows the public and private sector separately cannot achieve the same levels of value as together. The value that can be added by the private sector mainly consists of expertise and information. Through additional information and expertise from the private sector it becomes possible to create large scale analyses, create a more complete picture of the current cyber threat environment and adopt quicker to the changing cyber security domain.

Organisational learning can foster added value in the PPP. The learning organisation is mainly established through a trial and error approach, or learning by doing. Important to check in that process is whether best practices and lessons identified are also used to improve the PPP. Furthermore, data shows that a performance management system can contribute to the learning organisation. However, a balance needs to be found between recording processes and maintaining trust.

5.4 - Answering the research question.

The analysis of the data that has been gathered can now be summarised in order to answer the research question. In the beginning of this article, the question ‘what are critical success factors that would allow for a public private partnership in cyber intelligence in the Netherlands?’ was posed. The theoretical framework closely looked at the concept of Public Private Partnerships in order to conceptualise how a PPP in cyber intelligence should be designed. Public accountability, the literature suggested, is an important factor in a cyber intelligence PPP. To

that extent, performance management theory was set out and performance measurement theory was closer looked at. Ultimately, the theoretical framework led to the development of three Critical Success Factors that were tested.

The first CSF constituted synergy and trust. Creating outcomes that would not have been possible without the PPP can only be done when trust is established (Forrer et al. 2010, 481). To establish trust between the different stakeholders in the PPP, the CSF outlined performance measures and continuity as trust building factors. Furthermore, it established trust as the foundation of a vibrant PPP in which parties were able to contradict each other to avoid groupthink. The data collected to test the CSFs showed that at least two of these factors are important in practice, namely: continuity and contradiction. Performance measures as a way to establish trust divided opinion amongst respondents. This was due to the importance of confidentiality within the PPP. The data also revealed that personal level trust is vital to designing a sustainable PPP in cyber intelligence.

The second CSF that was identified surrounded goal-definition. The CSF suggested a focus on outcome when establishing goals, in order to create something beyond organisational limits. Furthermore, performance measures needed to be established in order to track the process of reaching the goals that are defined and to establish accountability in the PPP. The data show that the second CSF too is important in establishing a sustainable PPP. Respondents thought goal definition should focus on outcome and should be developed as equal partners. In terms of performance measures as a way to check the process of reaching the goals defined, respondents preferred trust over recording measurements. Performance evaluation, the data show, is done implicitly through internal accountability and intrinsic motivation. Explicitly recording performances, according to the data, would mean the private companies are placed under a magnifying glass and, consequently, diminish trust.

The third CSF entailed public added value. Ultimately, the PPP is designed to improve national cyber security, a task attributed to the government. Creating greater outcomes for the same cost is then an important factor in creating a successful PPP. The CSF identified organisational learning as a means to create added value and emphasised the importance of processing the performance information in the organisation to improve overall organisational performance. The data showed that organisational learning is an important part in a cyber intelligence PPP. Respondents found that best practices and lessons identified were important to improve the overall partnership. However, those best practices and lessons identified were, again, established implicitly rather than explicitly. Data showed the importance of finding a balance between recording processes and maintaining trust in the PPP. Overall, according to

the data, the public and private sector could achieve the most value together. The private sector could contribute to the PPP through their knowledge and expertise on cyber security, which, in turn, helps the public side in large scale analyses, a more complete picture of, and higher adaptability in, the cyber domain.

In conclusion, then, the data has shown that the three CSFs can establish a PPP in cyber intelligence. However they cannot be implemented one on one in practice. The data show that the way in which the theoretical framework depicts the three CSFs must be improved. The three CSFs themselves were valuable to the PPP in cyber intelligence. However, in maximising the value each CSF can add to the PPP, the data show measures are different from what the literature study shows. Most interesting is the fact that respondents placed trust above performance measures. The reason being that private companies have valuable cyber intelligence on threats and vulnerabilities and are only willing to share that information if it remains confidential. In that regard, performance measures are not ideal, since those record information officially which can then be revealed to the public through a Freedom of Information request.

Confidentiality, then, is important in creating an environment in which parties are willing to share information. However, personal level trust is equally important, since information that is shared in person will only be shared with someone that is trusted. As one respondent put it:

> 'You are not going to exchange this kind of information with someone you don't know, because then that trust is not there yet. You should at least know the organization and preferably a person within the organization you share with' (PR 3).

The data shows that performance is preferably evaluated implicitly. This means that stakeholders in the PPP informally update each other on their progress in reaching the defined goals. Part of that progress, is sharing best practices and lessons identified. This shows that organisational learning is an important factor in the PPP, be it that it is done informally. Accountability, then, is based on trust too. Data show accountability is ensured through the investments stakeholders make. Consequently, stakeholders have to account for their investments internally. Furthermore, accountability is generated through a continuous demand for intelligence by other stakeholders. When a stakeholder is unable to provide sufficient intelligence, and is only receiving intelligence, the partnership will reconsider the stakeholders membership.

6 - Recommendations.

This study has revealed interesting subjects in the establishment of a PPP in cyber intelligence. The study set out to research critical success factors that could allow for a public private partnership in cyber intelligence in the Netherlands. It found three CSFs that could do just that. However, the study also yielded some surprising results. In this final chapter, these surprising results will be scrutinised and recommendation will be provided for policies and further research.

6.1 - Intrinsic motivation as a driver, trust as a vehicle.

One of the most interesting results of the study was the intrinsic motivation found with the private sector to increase national cyber security in a public private partnership. The public private partnership envisioned at the beginning of this study proposed a traditional public private partnership in which the private sector received a financial reward for their added value in the partnership. The motivation for the private party, then, comes from the financial gain they are set to make from the partnership. Interestingly enough, this is not the case for a public private partnership in cyber intelligence in the Netherlands. The reason being that private companies are intrinsically motivated to increase national cyber security, the cyber security of the sector, and therefore their own cyber security. The financial gain is thus replaced by increased cyber security, which is more valuable to the private sector.

Furthermore, the PPP envisioned in the beginning of this research project saw a partnership in intelligence collection. This meant that the added value of the private sector was their ability to collect cyber security intelligence to benefit the Dutch intelligence agencies. This has proven to be true, however a cyber intelligence PPP was not necessary to collect that intelligence because the private sector already possesses valuable cyber intelligence which can be used by Dutch intelligence agencies. Both public and private respondents thought the private sector could be of added value in that way.

> ‘[Private expertise] is very valuable, private parties have a lot of knowledge and expertise. We can make much use of that as a government. It is not that we have all that knowledge in-house ourselves, so that's why you really need them’ (PU 3).

> ‘The AIVD knows a great deal, which we do not know. They get bits and pieces of information from such a partnership and that can be just that missing piece of the puzzle’ (PR 2).

This intelligence is gathered by the private sector through in-house experiences with cyber attacks and vulnerabilities. Sharing this information with the government and other private companies can be valuable to increase national cyber security. Through providing additional information to security services and in that way validating intelligence reports or revealing new information which can be used in writing up intelligence reports. Furthermore, it can strengthen the private sector in their fight against cyber criminals, both private and state actors.

The sharing of this information, however, needs to be done based on trust, another interesting result of this study. Trust proves to be more important in a cyber intelligence PPP in the Netherlands than explicit performance management results. The study revealed that trust unfolds itself in two ways, namely: confidentiality and personal level trust. The former is necessary to ensure the intelligence that is shared is not leaked to the public. For a private company, sharing cyber security vulnerabilities and detailed information on cyber attacks can be threatening when leaked to the public. It is therefore important that stakeholders in the PPP can trust each other and that sensitive intelligence is not spread.

That is trust is mostly established on a personal level. Trust, then, is about knowing who you share intelligence with. If, for some reason, a stakeholder does not trust someone in the partnership, the intelligence sharing will stop. It is therefore important that there is continuity in the partnership members. Both on an organisational level, and especially on a personal level.

> ‘There are fixed faces at the table and there should not be too much change. So often you have a direct point, a person who is always there’ (PU 3).

6.2 - Limitations.

This study has focused on the Netherlands to research critical success factors in a cyber intelligence PPP. It is therefore limited in generalisability, since the Dutch setting cannot easily be compared to, for example, a German setting. However, the results of the study can be tested in different countries. It will be interesting to see whether the three CSFs, adjusted according to the results of this study, will prove to be valuable in different countries, or not.

6.3 - Recommendations for policy and further research.

Ultimately, the results of the study are useful in providing policy recommendations and proposals for further research. The private sector possesses valuable cyber intelligence which can benefit the government, but also the private sector as a whole. To that extent, it is recommended to create a public private partnership in cyber intelligence sharing. It is important to note that a PPP in cyber intelligence sharing is different from the Information Sharing and Analysis Centres. Whereas the latter is focused on sharing information about vulnerabilities and cyber attacks with the government and the public sector, the former actively collaborates with the government to look for the missing piece in the intelligence puzzle. It therefore specifies the sharing of intelligence on the most pressing issues, rather than sharing all intelligence of which a large part may not be useful. This requires close collaboration between public parties and the Dutch intelligence agencies. The PPP has to be based on the three CSFs identified in this study, with special attention to the establishment of confidentiality and personal level trust. In return, the Dutch government must provide valuable information to the private sector. Not necessarily to offer private companies something in return for the intelligence they share, but more importantly to give insight into the most pressing issues intelligence is required for.

However, before such a PPP can be established further research is necessary in how these trust mechanisms can be operationalised. Research should focus on different trust mechanisms that can establish personal level trust in a cyber intelligence sharing PPP and that can constitute a confidential environment in which all stakeholders are comfortable sharing sensitive intelligence. Furthermore, research needs to be conducted in how trust can establish accountability in a cyber intelligence sharing PPP. This research has shown that hard KPIs and explicit performance management systems decrease trust rather than increase trust. Therefore, future research should focus on how the balance between recording information and building trust can be found and what mechanisms are needed to implement that balance. One mechanism that can be extended is the Traffic Light Protocol used in the ISACs. However, for a cyber intelligence sharing PPP, in which the intelligence agencies will play a large role, a protocol based on a gentleman's agreement will not suffice. Therefore, research is needed in how, for example, official classifications can improve the TLP so that confidentiality is increased.

A cyber intelligence sharing public private partnership can improve intelligence collection by the Dutch intelligence agencies and in the process improve private sector cyber

security. It is therefore invaluable to increasing national cyber security through prevention. No one party has all the intelligence needed to digitally secure the Netherlands, nor does it have the capacity to collect that intelligence. Truly increasing national cyber security can only be done through a public private partnership.

Bibliography.

Alfan, Ervina, and Zarina Zakaria. 2012. "Accountability in Public-Private Partnership Projects: A Financial Analysis of Malaysian Highway Authority." *World Applied Sciences Journal* 20(2): 221–27.

Amirkhanyan, A. A. 2009. "Collaborative Performance Measurement: Examining and Explaining the Prevalence of Collaboration in State and Local Government Contracts." *Journal of Public Administration Research and Theory* 19(3): 523–54. https://academic.oup.com/jpart/article-lookup/doi/10.1093/jopart/mun022.

Behn, Robert D. 2003. "Why Measure Performance? Different Purposes Require Different Measures." *Public Administration Review* 63(5): 586–606. http://doi.wiley.com/10.1111/1540-6210.00322.

Bovaird, Tony. 2004. "Public-Private Partnerships: From Contested Concepts to Prevalent Practice." *International Review of Administrative Sciences* 70(2): 199–215.

Bovens, Mark et al. 2014. "Public Accountability." *The Oxford Handbook of Public Accountability* (April 2018): 1–23. http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199641253.001.0001/oxfordhb-9780199641253-e-012.

Bowen, Glenn A. 2009. 9 Qualitative Research Journal Document Analysis as a Qualitative Research Method *Document Analysis as a Qualitative Research Method*. http://dx.doi.org/10.3316/QRJ0902027%5Cnhttp://%5Cnhttp://dx.doi.org/10.1108/11766091111162070.

Boynton, Andrew C, and Robert W Zmud. 1986. "An Assessment of Critical Success Factors." *Sloan Management Review* 25: 17–27.

Brinkerhoff, Derick W., and Jennifer M. Brinkerhoff. 2011. "Public-Private Partnerships: Perspectives on Purposes, Publicness, and Good Governance." *Public Administration and Development* 31(1): 2–14. http://doi.wiley.com/10.1002/pad.584.

de Bruijn, Hans. 2007. *Managing Performance in the Public Sector*.

Bruin, J.A. 2007. *Managing Performance in the Public Sector*. 2nd ed. Routledge.

Carr, Madeline. 2016. "Public – Private Partnerships in National Cyber-Security Strategies." *International Affairs* 1(February): 43–62.

Centrum Criminaliteitspreventie Veiligheid. 2013. *Samenwerken Werkt: Norm Voor de Werkwijze van Een Publiek-Privaat Samenwerkingsverband*.

Crane, Andrew. 2005. "In the Company of Spies: When Competitive Intelligence Gathering Becomes Industrial Espionage." *Business Horizons* 48(3): 233–40. http://linkinghub.elsevier.com/retrieve/pii/S0007681304001302.

"Cyber Security Keten." 2018. www.cybersecurityketen.nl.

Decuir-gunby, Jessica T, Patricia L Marshall, and Allison W Mcculloch. 2011. "Developing and Using a Codebook for the Analysis of Interview Data: An Example from a Professional Development Research Project." *Field Methods* 23: 136–55.

van Dooren, Wouter, Geert Bouckaert, and John Halligan. 2010. "The Use of Performance Information." In *Performance Managment in the Public Sector*, , 96–116.

Ebrahim, Alnoor. 2005. 34 Nonprofit and Voluntary Sector Quarterly *Accountability Myopia: Losing Sight of Organizational Learning*.

El-Gohary, Nora M., Hesham Osman, and Tamer E. El-Diraby. 2006. "Stakeholder Management for Public Private Partnerships." *International Journal of Project Management* 24(7): 595–604.

Elias, Ton et al. 2014. "Parlementair Onderzoek Naar ICT-Projecten Bij de Overheid." *Tweede Kamer der Staten-Generaal* (5): 1–219.

European Parliament, and Council of the European Union. 2004. "Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 Coordinating the Procurement Procedures of Entities Operating in the Water, Energy, Transport and Postal Services Sectors." *Official Journal of the European Union* L 134(1): 1–113.

Ewoh, Andrew I.E. 2011. "Performance Measurement in an Era of New Public Management." *Journal of Emerging Knowledge on Emerging Markets* 3(1): 1–14. http://digitalcommons.kennesaw.edu/jekem/vol3/iss1/8.

Ferreira, Aldónio, and David Otley. 2009. "The Design and Use of Performance Management Systems: An Extended Framework for Analysis." *Management Accounting Research* 20(4): 263–82.

Fombad, M. C. 2015. "Enhancing Accountability in Public–private Partnerships in South

Africa." *Southern African Business Review* 18(3): 66–92. http://www.ajol.info/index.php/sabr/article/view/111365.

Forrer, John, James Edwin Kee, Kathryn E. Newcomer, and Eric Boyer. 2010. "Public-Private Partnerships and the Public Accountability Question." *Public Administration Review* 70(3): 475–84.

Freund, York P. 1988. "Critical Success Factors." *Planning Review* 16(4): 20–23. http://dx.doi.org/10.1108/eb054458%5Cnhttp://dx.doi.org/10.1108/eb054457.

Fryer, Karen J., Jiju Antony, and Alex Douglas. 2007. "Critical Success Factors of Continuous Improvement in the Public Sector." *The TQM Magazine* 19(5): 497–517. http://www.emeraldinsight.com/doi/10.1108/09544780710817900.

Galletta, Anne, and William E Cross. 2013. "Section II: The Semi-Structured Interview: Collecting and Analyzing Qualitative Data." *Mastering the Semi-Structured Interview and Beyond : From Research Design to Analysis and Publication*: 73–112. http://0-search.ebscohost.com.brum.beds.ac.uk/login.aspx?direct=true&db=edspmu&AN=edspmu.MUSE9780814732953.10&site=eds-live&scope=site.

Gerring, John. 2009. The Oxford Handbook of Comparative Politics *The Case Study: What It Is and What It Does*.

Glor, Eleanor D. 2001. "Has Canada Adopted the New Public Management?" *Public Management Review* 3(1): 121–30.

Golofshani, Nahid. 2003. "Understanding Reliability and Validity in Qualitative Research." *The Qualitative Report* 8(4): 597–607.

Grapperhaus, Ferdinand. 2018. "Slottoespraak Minister Grapperhaus Tbv Kickstart Nationale Cyber Security Agenda 2018. Den Haag, Babylon, 24 Mei 2018." https://www.rijksoverheid.nl/documenten/toespraken/2018/05/24/slottoespraak-minister-grapperhaus-tbv-kickstart-nationale-cyber-security-agenda-2018.-den-haag-babylon-24-mei-2018.

Greve, Carsten. 2010. The Oxford Handbook of Business and Government *Public-Private Partnerships in Business and Government*.

Grossman, Seth A. 2012. "The Management and Measurement of Public-Private Partnerships." *Public Performance & Management Review* 35(4): 595–616.

http://www.tandfonline.com/doi/full/10.2753/PMR1530-9576350402.

Heinrich, Carolyn J. 2002. “Outcome-Based Performance Management in the Public Sector : Implications for Government Accountability and Efectiveness.” *Public Administration Review* 62(6): 712–25.

Heinrich, Carolyn J., and Gerald Marschke. 2010. “Incentives and Their Dynamics in Public Sector Performance Management Systems.” *Journal of Policy Analysis and Management* 29(1): 183–208. http://doi.wiley.com/10.1002/pam.20484.

Hennis-Plasschaert, J.A., and R.H.A. Plasterk. 2014. *Convenant AIVD – MIVD Inzake de Joint Sigint Cyber Unit*.

Huistra, A.W., and T.H.E.E.A. Krabbendam-Hersman. 2017. *Verkenning Cybersecurity Informatiedeling Binnen de Topsectoren*.

Inkster, Nigel. 2015. “Cyber Espionage.” *Adelphi Series* 55(456): 51–82. https://www.tandfonline.com/doi/full/10.1080/19445571.2015.1181443.

International Co-operative alliance. “Statement on the Co-Operative Identity (Archived).” https://web.archive.org/web/20120204081503/http://www.ica.coop/coop/principles.html .

Jacobson, Carol, and Sang Ok Choi. 2008. “Success Factors: Public Works and Public-private Partnerships.” *International Journal of Public Sector Management* 21(6): 637–57. http://www.emeraldinsight.com/doi/10.1108/09513550810896514.

Jakobsen, Mads L.F., and Peter B. Mortensen. 2016. “Rules and the Doctrine of Performance Management.” *Public Administration Review* 76(2): 302–12.

de Jong, B, and P Keller. 2010. “Contra-Inlichtingen En Contraspionage.” In eds. B.A. de Graaf, E.R. Muller, and J.A. van Reijn. , 275–94.

Jonker, Jorn, and Lise Witteman. 2018. “Grapperhaus: ’Ik Zou Er van Wakker Liggen’.” https://www.telegraaf.nl/nieuws/1944740/grapperhaus-ik-zou-er-van-wakker-liggen.

Kabinet Rutte III. 2017. *Regeerakkoord: Vertrouwen in de Toekomst*.

Klijn, Eh, and Gr Teisman. 2000. “Governing Public-Private Partnerships: Analysing and Managing the Processes and Institutional Characteristics of Public-Private Partnerships.” *Routledge Advances in Management and …*: 84–102.

http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Governing+Public-Private+Partnerships:+Analysing+and+managing+the+processes+and+institutional+characteristics+of+public-private+partnerships#0.

Klijn, Erik-Hans, and Geert. R. Teisman. 2003. "Institutional and Strategic Barriers to Public-Private Partnerships: An Analysis of the Dutch Case." *Public Money & Management* 23(3): 137–46.

Koontz, Tomas M., and Craig W. Thomas. 2012. "Measuring the Performance of Public-Private Partnerships." *Public Performance & Management Review* 35(4): 769–86. http://www.tandfonline.com/doi/full/10.2753/PMR1530-9576350410.

Kop, Nicolien. 2016. "Leren van Publiek-Private Samenwerking in Een Afpersingszaak." *Tijdschrift voor de Politie* 79(7): 12–15.

Latham, Gary P., Lorne M. Sulsky, and Heather MacDonald. 2009. "Performance Management." *The Oxford Handbook of Human Resource Management* (March 2018): 1–21.

Liu, Junxiao et al. 2013. "Conceptual Framework for the Performance Measurement of Public-Private Partnerships." *Journal of Infrastructure Systems* 21(December): 395–408. http://ascelibrary.org/doi/abs/10.1061/(ASCE)IS.1943-555X.0000138.

———. 2014. "Public-Private Partnerships: A Review of Theory and Practice of Performance Measurement." *International Journal of Productivity and Performance Management* 63(4): 499–512. http://www.emeraldinsight.com/doi/10.1108/IJPPM-09-2013-0154.

Löffler, Elke. 1999. *The Modernization of the Public Sector in an International Comparative Perspective*.

Lynn, Laurence E. 2009. *Public Management: A Concise History of the Field.* Oxford University Press. http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780199226443.001.0001/oxfordhb-9780199226443-e-3.

Mackie, Bobby. 2008. "Organisational Performance Management in a Government Context: A Literature Review." : 42. http://scrutinyreview.org/Publications/2008/08/25142353/9.

Mattern, Troy, John Felker, Randy Borum, and George Bamford. 2014. "Operational Levels

of Cyber Intelligence." *International Journal of Intelligence and CounterIntelligence* 27(4): 702–19.

Modderkolk, Huib. 2016. "Nederlands-Duits Defensiebedrijf Gehackt Door Chinezen." *Volkskrant*. https://www.volkskrant.nl/tech/nederlands-duits-defensiebedrijf-gehackt-door-chinezen~a4320398/.

Morse, Janice M. et al. 2002. "Verification Strategies for Establishing Reliability and Validity in Qualitative Research." *International Journal of Qualitative Methods* 1(2): 13–22. http://journals.sagepub.com/doi/10.1177/160940690200100202.

Moynihan, Donald P., and Sanjay K. Pandey. 2010. "The Big Question for Performance Management: Why Do Managers Use Performance Information?" *Journal of Public Administration Research and Theory* 20(4): 849–66.

Muckin, Michael, and Scott C Fitch. 2014. "A Threat-Driven Approach to Cyber Security." *Lockheed Martin*: 1–45. http://www.lockheed.fi/content/dam/lockheed/data/isgs/documents/Threat-Driven Approach whitepaper.pdf.

Nationaal Cyber Security Centrum (NCSC). 2016. *Cyber Security Assessment Netherlands 2016*. https://english.nctv.nl/.../25760-csan-5-v3.2-web-uk_tcm92-611157.pdf.

———. 2017. *Cyber Security Assessment Netherlands 2017*. https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cybersecuritybeeld-nederland-2016/1/CSBN2016.pdf.

NCSC. 2018. "Nederlandse Cybersecurity Agenda Gepresenteerd." *News Article*. https://www.ncsc.nl/actueel/nieuwsberichten/nederlandse-cybersecurity-agenda-gepresenteerd.html (June 3, 2018).

NCSS. 2018a. "Deelname Aan ISAC." https://www.ncsc.nl/samenwerking/deelname-aan-een-isac.html.

———. 2018b. "ISAC." https://www.ncsc.nl/english/Cooperation/isacs.html.

NCTV. 2013. *National Cyber Security Strategy 2*. http://english.nctv.nl/Images/ national-cyber-security-strategy-2_tcm92-520278.pdf.

———. 2018. Rijksoverheid.nl *Nederlandse Cybersecurity Agenda: Nederland Digitaal*

Veilig. https://www.rijksoverheid.nl/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig.

Negoita, Marian. 2018. "Beyond Performance Management: A Networked Production Model of Public Service Delivery." *Public Performance & Management Review* 41(2): 253–76. https://www.tandfonline.com/doi/full/10.1080/15309576.2017.1408473.

Nielsen, Poul A. 2014. "Performance Management, Managerial Authority, and Public Service Performance." *Journal of Public Administration Research and Theory* 24(2): 431–58.

Noble, Helen, and Joanna Smith. 2015. "7) Issues of Validity and Reliability in Qualitative Research." *Evidence-Based Nursing* 18(2): 34–35. http://ebn.bmj.com/cgi/doi/10.1136/eb-2015-102054.

Ollongren, K.H. 2018. "Heimelijke Beïnvloeding van de Publieke Opinie Door Statelijke Actoren." (508): 1–7.

Osei-Kyei, Robert, and Albert P.C. Chan. 2015. "Review of Studies on the Critical Success Factors for Public-Private Partnership (PPP) Projects from 1990 to 2013." *International Journal of Project Management* 33(6): 1335–46. http://dx.doi.org/10.1016/j.ijproman.2015.02.008.

Petersen, Karen Lund, and Vibeke Schou Tjalve. 2017. "Intelligence Expertise in the Age of Information Sharing: Public–private 'Collection' and Its Challenges to Democratic Control and Accountability." *Intelligence and National Security* 33(1): 21–35. http://doi.org/10.1080/02684527.2017.1316956.

Pongsiri, Nutavoot. 2002. "Regulation and Public-private Partnerships." *International Journal of Public Sector Management* 15(6): 487–95. http://www.emeraldinsight.com/doi/10.1108/09513550210439634.

Raad van Hoofdcommissarissen. 2005. *Visie Op Publiek-Private-Samenwerking*.

Riege, Andreas M. 2003. "Validity and Reliability Tests in Case Study Research: A Literature Review with 'Hands-on' Applications for Each Research Phase." *Qualitative Market Research: An International Journal* 6(2): 75–86. http://www.emeraldinsight.com/doi/10.1108/13522750310470055.

Roberts, David J., and Matti Siemiatycki. 2015. "Fostering Meaningful Partnerships in Public–private Partnerships: Innovations in Partnership Design and Process

Management to Create Value." *Environment and Planning C: Government and Policy* 33(4): 780–93.

Roehrich, Jens K., Michael A. Lewis, and Gerard George. 2014. "Are Public-Private Partnerships a Healthy Option? A Systematic Literature Review." *Social Science and Medicine* 113: 110–19. http://dx.doi.org/10.1016/j.socscimed.2014.03.037.

Rolfe, Gary. 2006. "Validity, Trustworthiness and Rigour: Quality and the Idea of Qualitative Research." *Journal of Advanced Nursing* 53(3): 304–10.

Saldana, Johnny. 2009. "An Introduction to Codes and Coding." In *The Coding Manual for Qualitative Researchers.,* London: Sage Publications, 1–31.

Salminen, Ari. 2011. "Performance Management." In *International Encyclopedia of Political Science*, eds. Bertrand Badie, Dirk Berg-Schlosser, and Morlino Leonardo. , 1854–57.

Shaoul, Jean, Anne Stafford, and Pamela Stapleton. 2012. "Accountability and Corporate Governance of Public Private Partnerships." *Critical Perspectives on Accounting* 23(3): 213–29. http://linkinghub.elsevier.com/retrieve/pii/S1045235411001729.

Skelcher, Chris. 2009. *Oxford Handbooks Online Public – Private Partnerships and Hybridity*.

Sonnentag, Sabine, and Michael Frese. 2005. "Performance Concepts and Performance Theory." *Psychological Management of Individual Performance*: 1–25. http://doi.wiley.com/10.1002/0470013419.ch1.

Soss, J., R. Fording, and S. F. Schram. 2011. "The Organization of Discipline: From Performance Management to Perversity and Punishment." *Journal of Public Administration Research and Theory* 21(Supplement 2): i203–32. https://academic.oup.com/jpart/article-lookup/doi/10.1093/jopart/muq095.

Steijn, Bram, Erik-hans Klijn, and Jurian Edelenbos. 2011. "PUBLIC-PRIVATE PARTNERSHIPS : ADDED VALUE BY ORGANIZATIONAL FORM OR MANAGEMENT ?" *Public Administration* 89(4): 1235–52.

The World Bank Group (WBG). 2016. "The APMG Public-Private Partnership (PPP) Certification Guide." : 1–180. https://ppp-certification.com/sites/default/files/documents/Chapter-1-PPP-Introduction-and-Overview.pdf.

Theisens, Henno. 2012. “Governance in Interessante Tijden: Een Essay.” *De Haagse Hogeschool Lectoraten*: 1–35.

Tweede Kamer der Staten-Generaal. 2015. “Toezichtsverslagen AIVD En MIVD.” (315): 1–58.

Velotti, Lucia, Antonio Botti, and Massimiliano Vesci. 2012. “Public-Private Partnerships and Network Governance.” *Public Performance & Management Review* 36(2): 340–65. http://www.tandfonline.com/doi/full/10.2753/PMR1530-9576360209.

Verhagen, M.J.M. 2012. *Aanbestedingswet 2012*. ’s-Gravenhage: Ministerie van Economische Zaken. http://wetten.overheid.nl/BWBR0032203/2016-07-01.

Weissbrodt, David. 2013. “Cyber-Conflict, Cyber-Crime, and Cyber- Espionage.” : 347–87.

Whittemore, Robin, Susan K. Chase, and Carol Lynn Mandle. 2001. “Validity in Qualitative Research.” *Qualitative Health Research* 11(4): 522–37.

Yin, Robert K. 2009. *Case Study Research: Design and Methods*. Sage.

———. 2012. “A (VERY) BRIEF REFRESHER ON THE CASE STUDY METHOD.” *Applications of Case Study Research*: 3–20.

Appendix A – the interview questions.

Synergy and trust.

1. What do you think is necessary for establishing trust in Public Private Partnership (PPP)?
2. What role can a performance management system play in building trust?
3. To what extent do you opportunism is a problem for a cyber intelligence PPP?
4. What could be a strategy for developing a sustainable open collaboration between the PPP stakeholders?
5. To what extent do you think it is important to have the opportunity to contradict each other?

Goal definition.

1. How do you think goals should be established in a PPP in cyber intelligence?
2. Do you think it is important to focus on output (product) or on outcome (results)?
3. What do you find important when it comes to tracking goals?
4. Do you think that performance management can guarantee accountability in a cyber intelligence PPP?

Added value.

Organizational Learning means improving actions through better knowledge and understanding.

1. What role does the organisational learning play in a cyber intelligence PPP, do you think?
2. How do you think a performance management system can add to the 'learning organization'?
3. Do you think that the expertise of the private sector can be of added value in the cyber intelligence process?
4. How do you think a PPP in cyber intelligence can be of value?

Appendix B – codebook.

The codebook was developed based on an article by DeCuir-Gunby et al., *Developing and Using a Codebook for the Analysis of Interview Data: An Example from a Professional Development Research Project* (2011).

Table 2. Theory-Driven Codes, definitions, and examples

Code	Description	Example
Value Added	Respondent refers to an outcome of achieving more in a PPP at the same cost.	So I think that information sharing is really the key to keep our society digitally safe with each other. It is too large and too wide to have an isolated approach. You have to do that in collaboration.
Trust	Respondent refers to the role trust plays in a PPP.	The interesting thing is that you immediately start with the most difficult. Trust is what is most difficult to realize and breaks down the easiest.
Goal-Definition	Respondent makes direct/indirect reference to defining goals in a PPP.	You do it together, you put the dot on the horizon together. This often happens through discussions about an annual plan
Accountability	Respondant remarks or provides examples of accountability in a PPP.	That really depends on what the parties at the table want. If they want to record this in a procedural way, then the performance management system, that justification, can help.
Performance Management System	Respondent refers to a performance management system in the PPP.	You can set your goals specifically for activities. That's why I also mentioned KPIs. The disadvantage is then what exactly you are going to measure. How do you measure whether you have achieved goals?

Organisational Learning	Respondant directly or indirectly refers to organisational learning and a type of learning by doing approach.	I think that such a partnership is in itself a learning organization.
Output	Respondent refers to the importance of output.	I do not believe in intelligence companies, but I do believe in companies that provide information or applications that can help the intelligence services to arrive at the highest possible certainty in their analyses.
Outcome	Respondent refers to the importance of outcome.	Yes, because the goal is not to write reports, the goal is to increase Dutch cyber resilience. So the time you need to write and review reports, you can also use to discover and combat new attacks.
Contradiction	Respondent refers to the importance of contradiction. Also applies to situations of validation, i.e. extra confirmation by third parties.	It is always good to organize contradiction.
Opportunism	Respondent refers to or provides an example of the degree opportunism might pose a problem in a PPP.	Opportunism can also have a positive side . It can also be 'we do not know if it will work, but let's just try it'.

Table 3. Data-Driven Codes, Definitions, and Examples

Code	Definition	Example
Continuity	Respondent references to continuity as an important factor in a PPP.	What must also be included in my personal opinion is a problem owner. The client, the government, must set up a project manager who will remain project leader until the project is completely finished.

Personal Level Trust	Respondent decribes the importance of trust relationships between people in the PPP.	What is especially important for trust is that you know each other personally. That is all about, personal contacts, occasionally drinking a drink together. Really work on the informal trust.
Implicit performance evaluation	Respondent refers to or provides an example of evaluating performance in a PPP in an unofficial manner.	We have that implicitly. I think that should be a part of it, how can you learn if you do not check your progress?
Contract	Respondent refers to contracts to legally bind the PPP or to contracting out.	I have set goals myself and in my opinion the government only should do business with private IT companies with which you conclude a contract where they deliver on a fixed date, discuss well in advance what we want from each other, and then there is a fixed price and a fixed time.
Transparency	Respondent refors to transparancy in the PPP, between Public and Private.	Openness and transparancy is then very important'.
Public Private Dynamics	Respondent refers to the differences between Public and Private worlds.	If there are differences in that, for example a commercial party that wants to market a product and the government that sees a long-term project, then there is already friction there.
Intelligence Sharing	Respondent remarks that intelligence sharing is important in a cyber intelligence PPP (rather than Public Private collection).	What can also help is a kind of vetting system, which you often see with intelligence sharing.
Equality	Respondent refers to equality between partners in the PPP.	Together, that is that cooperative model, and perhaps also an Eindhoven model, we do everything together.

Confidentiality	Respondent refers to the importance of confidentiality in the PPP.	The question is actually whether you want to record information in your collaboration.
Value Added Private	Respondent refers to value added by private parties.	Because companies see a lot in the protection of their own infrastructure and gather a lot of information. And that infrastructure and information is not just available to the intelligence services.

Table 4. Coding Themes

Theme	Codes
Trust	Trust Contradiction Opportunism Continuity Personal Level Trust Tranparancy Equality Confidentiality Performance Management System
Goal Definition	Goal-Definition Output Outcome Contract Performance Management System Accountability Intelligence Sharing
Value Added	Value Added Value Added Private Performance Management System Organisational Learning Best Practices Implicit Performance Evaluation Public Private Dynamics