Cybersecurity Cooperation in the Port of Rotterdam

Universiteit Leiden

Author: Douwe Bartstra

Student number: s2567245

Supervisor: Dr. Tatiana Tropina

Second reader: Dr. Tommy van Steen

Master Thesis

MSc Crisis and Security Management

Faculty of Governance and Global Affairs

Leiden University

02/07/2020

Abstract

Ensuring the proper functioning of critical infrastructure is important for a nation's national security. Due to digitalization and growing interdependencies across sectors, any disruption can have disastrous consequences. Cybersecurity therefore is a public-private effort requiring governments and business to cooperate.

As the Port of Rotterdam is part of Dutch critical infrastructure, a cybersecurity incident can have negative consequences for the Netherlands as a whole. Thus, it is in the interest of the general public that public and private actors active in the port work together in managing cybersecurity risks. However, issues such as a lack of trust, misplaced expectations and conflicts of interest often hamper public-private cooperation in cybersecurity.

This thesis therefore aims to analyze to what extent public and private actors in the Port of Rotterdam cooperate in managing cybersecurity risks. In order to provide insight into public-private cybersecurity cooperation, the NIST Cybersecurity Framework is used.

The analysis shows that cybersecurity cooperation between public and private actors in the Port of Rotterdam is lacking. While Dutch government and port policy reports promote public-private cybersecurity cooperation, the analysis indicates otherwise. Conflict of interest, lack of trust, financial shortcomings, governmental law as well as responsibility disputes hinder public-private cooperation. In order to overcome these issues, trust has to be built and knowledge sharing has to be stimulated.

Acknowledgements

I would like to express great appreciation to my thesis supervisor Dr. Tatiana Tropina for her support and supervision throughout the entire process of writing this thesis. I would also like to thank the professionals that took their time for the interviews and for providing me with valuable insight into this area of research.

Rotterdam, July 2020

Douwe Bartstra

Table of Contents

Abbreviations

DTC	Digital Trust Center
ENISA	European Union Agency for Cybersecurity
FERM	No acronym, but the Dutch translation of resilience
ICT	Information and Communications Technologies
ISAC	Information Sharing and Analysis Centers
ISPS	International Ship and Port Facility Security Code
IT	Information Technology
NCSC	National Cyber Security Centre
NCTV	National Coordinator for Security and Counterterrorism
NDN	National Detection Network
NIST	National Institute of Standards and Technology
port-ISAC	port-Information Sharing and Analysis Center
SOC	Security Operations Center
Wbni	Wet Beveiliging Netwerk- en Informatiesystemen

1. Introduction

On the afternoon of June 27, 2017, chaos erupted in the Port of Rotterdam. A cyberattack of unprecedented scale had erupted, infecting and shutting down computers one by one. APM Terminals, part of Maersk, had fallen victim to a piece of malware named Notpetya that was racing beyond its initial location in Ukraine and out to countless machines around the world. As a result, other organizations in the port also became infected, leading to a shutdown of operations. The Rotterdam Port Authority together with the National Cyber Security Centre (NCSC) had to do everything in its power to minimize the impact of this cyber-attack, which would eventually result in hundreds of millions of euro's in damages (IFV, 2018, pg.119).

As can be seen, cyber-attacks can have devasting effects on companies around the world, which is especially true for those operating critical infrastructure. Already since the early 1990's, the importance of protecting critical infrastructure has been stressed by countries around the world. This type of infrastructure is prioritized according to national importance, as they are so vital that their destruction can have disastrous societal effects (Moteff & Parfomak, 2014, pg.4). Critical infrastructure not only encompasses technical assets, but also functional sectors and essential services. Therefore, it has been considered of utmost importance to prepare, invest in, and manage all categories of critical infrastructure. These include lifeline networks such as energy, water and transportation, as well as lifeline support networks consisting of emergency and medical services (Petit, pg.4).

However, protecting such infrastructure is becoming more challenging due to the increase in interdependencies within infrastructure systems. Growing dependencies and interdependencies across critical infrastructure systems have increased vulnerabilities to different kind of threats. In particular, reliance on information and communications technologies (ICT) has increased the potential for physical and cyber threats (Petit et al., 2015, pg.5). As many of the ICT's are developed in the private sector, computer and network vulnerabilities are to be expected. This is because the private sector is driven by competition, leading to designs that are not security driven with critical points of failure. Furthermore, as systems blend into one another due to the increasing use of ICT's, it becomes merely impossible to adequately maintain a separation of systems. As a

result, attacking critical infrastructure can have a force multiplier effect, in which a small attack can have a large impact (Cavelty, 2007, pg.16).

Because of this, countries around the world have taken initiatives in an attempt to better secure critical infrastructure. One of the key protection challenges however, arises from the privatization and deregulation of many parts of the public sector. On one hand, private market forces are not capable of providing protection. On the other hand, if the state provides the public good of security on its own, competitiveness and prosperity of a nation may diminish (Dunn-Cavelty & Suter, 2009, pg.1). Thus, strengthening the security and resilience of critical infrastructure is a shared responsibility between all relevant stakeholders. These include infrastructure owners and operators as well as numerous governmental and non-governmental organizations. By incorporating these public and private stakeholders, mutual understanding and trust is enhanced while information sharing and practical exchanges are promoted (CISA, 2019, pg.9). This is especially true for cybersecurity, as several incidents have shown that strong working relationships between the public and private sector can minimize the impact of cyber-attacks. Therefore, effective cybersecurity requires a cultural shift towards continuous public-private cooperation in which both agencies and businesses view collaborative cybersecurity as an essential part of their daily operations (Givens & Busch, 2013, pg.45).

However, attempts to increase cybersecurity cooperation between the public and private sectors have often been unsuccessful. Lack of trust, misplaced expectations, conflicts of interest as well as government laws requiring a certain level of secrecy or openness have all hampered cooperation efforts (Shore, Du, & Zeadally 2011, pg.4). Furthermore, the appearance often differs from the reality. This is because, even though governments and business may appear to use relatively uniform cybersecurity standards, this is not always the case. Both the public and private sector share cybersecurity best practices, however, compliance with recommendations is often minimal. Thus, even though public-private partnerships are publicized to stress the importance of these cybersecurity initiatives, cooperation and adopting shared measures is limited (Givens & Busch, 2013, pg.45).

In the Netherlands, ICT is increasingly intertwined in Dutch society. Both the government and private organizations make extensive use of data-driven applications and processes. As a result, stakeholders are dependent on one another. When digital processes are disrupted, especially in critical infrastructure, significant societal disruption in the Netherlands can occur (NCSC, 2018, pg.31). One of the main ambitions of the Dutch government when it comes to cybersecurity is therefore to stimulate public-private cooperation. This is especially important in the Netherlands, as over 80 percent of the Dutch critical infrastructure is in private hands. It is therefore not only the government's responsibility to provide cybersecurity, but also the responsibility of businesses and citizens. As a matter of fact, public-private cooperation forms the basis of Dutch cybersecurity measures. Only when the private sector is incorporated in cybersecurity measures, such as the sharing of knowledge and the exchange of information, will threats be minimized (NCSC, 2018, pg.7-13).

When looking at major ports in particular, it can be seen that a large portion of the development consists of private investments. Global terminal operators, shipping lines, logistic providers and energy companies are just a few of the many private organizations that invest in major ports. However, port authorities are mostly public organizations that manage all facets of the port (Dooms, van der Lugt & De Langen, 2013, pg.148). The Port of Rotterdam is no different, as it consists of a large number of private national and international organizations and is managed by a semi-publicly held Port Authority with two shareholders, namely: the city of Rotterdam (70%) and the Dutch government (30%). The Port Authority is responsible for the continuous functioning of the port as well as ensuring physical and digital safety. When it comes to cybersecurity, it aims to work together with private actors in tackling digital disruptions that can jeopardize the safety of the entire port (Havenbedrijf Rotterdam, 2018, pg.4). It is therefore important to research how the public and private sector in the Port of Rotterdam work together in ensuring cybersecurity. Do they collectively manage cybersecurity risks, or do they prefer to do this individually? The central research question will therefore be as follows: *To what extent do public and private actors in the Port of Rotterdam cooperate in managing cybersecurity risks?*

The added benefits to society regarding this research are evident. A strong Dutch cybersecurity sector results in digital autonomy. This means that both the government and business can count on

their own cybersecurity measures and by doing so, promote digital security in general (NCSC, 2018, pg.10). Thus, Dutch values such as an open, free and safe internet are promoted. Furthermore, as Dutch society has become completely dependent on digital processes, the continuous functioning of these processes is of utmost importance. This is not only true for government and business operations, but also for the daily lives of citizens (NCSC, 2018, pg.11). Properly functioning public-private cybersecurity initiatives in the Port of Rotterdam is therefore essential.

Furthermore, the Port of Rotterdam is the largest port of Europe and is responsible for 6.2 percent of the Dutch gross domestic product. The port not only promotes economic activity all around the Netherlands, but also directly and indirectly provides employment for over 385,000 people (Havenbedrijf Rotterdam, 2019, pg.17). It is therefore of no surprise that the Dutch government has labeled the Port of Rotterdam as critical infrastructure. As a result, adequate cybersecurity measures in the Port of Rotterdam are important to Dutch society. Any disruptions can have far reaching negative consequences. Cooperation between the public and private sector in managing cyber risks is therefore in the interest of the general public. Furthermore, this research has considerable academic relevance. Protection of critical infrastructure has been linked to cybersecurity for the past 25 years, and public-private cooperation is not unique in this domain (Carr, 2016, pg.48-52). However, very limited academic research has been conducted regarding cooperation in major ports. This is especially true for the Port of Rotterdam. This research can therefore result in new insights regarding this area of study.

This thesis is structured as follows. Chapter two includes key concepts, background information on cybersecurity and public-private cooperation as well as the NIST Cybersecurity Framework. Chapter three discusses information regarding the methodology and research design, in which it stipulates how data analysis is conducted. It also operationalizes the NIST Framework and presents the methods of data collection. Chapter four includes a systematic analysis of the collected data followed by a discussion of the results and answer to the research question. Lastly, chapter five contains a reflection and discusses limitations of the research complemented by recommendations and areas for future research.

2. Body of Knowledge

This chapter discusses concepts that are of importance in this research. First, it discusses the notion of cyber threats in order to stress the importance of cybersecurity. After this, it provides a review of existing academic literature regarding public-private cooperation. Finally, it introduces the cybersecurity framework used in answering the research question.

2.1. Cybersecurity Risks

There is very limited literature regarding the conceptualization of cybersecurity risks. Thus, in order to gain an understanding of this concept, it is divided into two. First, this section briefly discusses cyber risks. Afterwards, it conceptualizes cybersecurity. By doing so, it will become clear what it is that public and private actors aim to manage.

2.1.1. Cyber Risks

Following the end of the Cold War, a variety of new non-military threats moved onto the security political agenda of nations around the world. These new threats had greater uncertainty surrounding them, as they often came from non-state actors using non-military means. One of these new threats entailed threats from cyberspace. Cyber threats therefore came to be considered serious, forcing governments to implement measures to counter them (Cavelty, 2007, pg.5).

However, conceptualizing cyber threats seems to be an ongoing debate, as existing definitions and related terms vary widely. Even though concepts such as ‘cyber incident’, cyber-attack’ and ‘cybercrime’ are popular in existing literature and used interchangeably, there are no universally adopted definitions (Johnson, 2015, pg.569). For example, a definition of the term ‘cybercrime’ differs depending on the perception of both the observer and victim. On top of this, the broad spectrum across which cybercrime can occur makes conceptualization even more difficult (Gordon & Ford, 2006, pg.14). Some definitions are narrow, pinpointing the type of attack and size of impact. Others define the concept more broadly, defining it as a risk resulting in failure of information systems (Biener, Eling &Wirfs, 2015, pg.4). Generally, as Ciolan (2014) puts it,

cyber-attacks vary from illegal low-level individual crime (such as hacking) to actions of non-state actors or groups (criminals and terrorists) to well organized attacks by nation states (Ciolan, 2014, pg.124).

In order to understand cyber threats and risks, it helps to grasp the nature of threats and how they exploit technological systems. Cybercrime comes in many forms and the tools are varied. The attack surface, or the size of the vulnerability presented by hardware and software, is enormous. Thus, depending on the organization, the attack surface can run into the thousands or even more (ACS, 2016, pg.14). The type of cyber threats are also numerous, and vary in sophistication and impact. For the past seven years ENISA has published a yearly threat landscape, stipulating the 15 biggest cyber threats in the European Union. These threats range from ransomware to cyber espionage, continuously changing in frequency and sophistication (ENISA, 2018, pg.24). They may arise from external or internal entities, and may be a product of intentional or unintentional action. Furthermore, cyber risks can arise from non-human factors as well (Siegel, Sagalow & Serritella, 2002, pg.12-13). On top of this, the complex nature of ICT drastically increases potential vectors of vulnerability and expands their scope to many different actors, ranging from private actors to governmental institutions. Cyber risks can therefore come from anywhere, characterizing cybersecurity by a fundamental uncertainty (Christensen & Petersen, 2017, pg.1436).

2.1.2. Cybersecurity

Naturally, the rise of cyber threats calls for cybersecurity. However, just like the term ‘cyber threats’, conceptualizing cybersecurity has been a difficult process. Ill-defined concepts and inconsistent terminology further complicates an already complex issue. As a result, it becomes difficult for policy makers to develop strategies in addressing such risks (Dewar, 2014, pg.7-8). As former director of the CIA Michael Hayden mentioned, “rarely has something been so important and so talked about with less clarity and less apparent understanding than cyber security” (Nye, 2011, pg.18). To make matters more complex, the inconsistent use of syntax for cybersecurity has been an issue. Both terms ‘cyber security’ and ‘cybersecurity’ are used in existing literature, which complicates research (Schatz, Bashroush & Wall, 2017, pg.55). Even so, the popularity in the use of the term cybersecurity has significantly increased in the past decade.

This was especially evident after former U.S. President Barack Obama used the term in a press release in 2009 (Schatz, Bashroush & Wall, 2017, pg.54). Nevertheless, as can be seen, it is important to clearly define cybersecurity in order for this analysis to be coherent and consistent.

Many definitions of cybersecurity emphasize the protection of some sort of network system. Security in its broad sense, involves a process of identifying and remedying vulnerabilities of a system against a specified set of threats posed by an adversary. Cybersecurity applies these activities to networked computer systems (Burstein, 2008, pg.173). Ciolan (2014) proposes a similar definition, emphasizing that cybersecurity refers to protection of systems and protection of data from alteration (Coilan, 2014, pg.122). However, in this research, taking an organizational strategic management approach is more suitable in defining cybersecurity as the focus is on public and private organizations. Regular strategic management is a process that determines the sequence of actions of an organization for developing and implementing a certain strategy. Choosing a cybersecurity strategy is also a process. Cybersecurity is therefore defined as "the process of developing methods, security policies and implementing measures to protect information systems, networks, and cyberspace applications of the organization from digital (computer) attacks" (Mandritsa et al., 2018, pg.2).

What is clear from existing literature is that cybersecurity is one of the most important national security policies of the moment. Since great interdependency and interconnectivity exists between sectors, resilience of communication and electronic systems has become crucial for critical services. As a result, critical infrastructure protection has become intertwined with cybersecurity (Ciolan, 2014, pg.123). It has therefore become a top priority for organizations, both in the public and private sector. Cybersecurity is a shared responsibility and requires close partnership between the government, private sector, international partners and citizens in ensuring vital systems (Mandritsa et al., 2018, pg.2). Thus, it is of no surprise that public-private cooperation is often advocated in the cybersecurity domain, as it is seen as the answer to many of the challenges related to cybersecurity governance (Christensen & Petersen, 2017, pg.1436).

2.2. Public-Private Cooperation

In this research, public-private cooperation encompasses various types of partnership efforts between the public and private sector. In order to get an understanding of this concept, a literature review regarding public-private partnerships is conducted. However, conceptualizing the term public-private partnership is difficult to do as it is a contested concept with no single authoritative definition (Weihe et al., 2011, pg.13). A common definition does not exist, which is why the term is still often used without precision (Bossong & Wagner, 2017, pg.268). Nevertheless, understanding the concept of public-private partnerships helps in addressing cybersecurity cooperation.

2.2.1. Public-private Partnerships

Historically, public-private partnerships have been studied in terms of economic or financial synergies in the development of some sort of product or service, such as infrastructure projects. Linder (1999) stresses this point by arguing that the hallmark of partnerships has been cooperation that spreads financial risks between public and private sectors. These arrangements work to mitigate competitive pressures and contests the division of responsibility between both parties (Linder, 1999, pg.36). For example, Van Ham and Koppenjan (2001) define public-private partnerships as "co-operation of some durability between public and private actors in which they jointly develop products and services and share risks, costs and resources which are connected with these products or services" (Van Ham & Koppenjan, 2001, pg.598). According to Hodge and Greve (2007) this definition has several benefits. It not only underlines cooperation of some durability, but also emphasizes risk sharing as a vital component. Furthermore, it includes the production of something, a product or service, while both parties stand to gain from this (Hodge & Greve, 2007, pg.546). An important aspect here is the product or service, as most literature focused on public-private partnerships take infrastructure projects into consideration. Even critical success factors of public-private partnerships mostly focus on this. For example, Osei-Kyei and Chan (2013) have done extensive research regarding critical success factors when it comes to infrastructure projects around the world. It can therefore be seen that mainstream public-private partnerships are typically based on a formalized agreement that tasks the private sector with the

provision of a public service, new construction project, or maintenance of infrastructure. Thus, the main drivers for the formation of these mainstream public-private partnerships are cost and efficiency (Bossong & Wagner, 2017, pg.268).

However, when reviewing the current literature it becomes clear that there are many other reasons for public-private partnerships to occur. Linder (1999) proposes six distinct uses of the term, in which each use conveys an understanding of the intended purpose and significance. In a 'partnership as management reform', partnerships are promoted as an innovative tool in which government officials become more like their private counterparts. They learn from private managers and as a result become more entrepreneurial and flexible. In 'partnership as problem conversion', public actors commercialize certain problems in attracting profit-seeking collaborators. 'Partnership as moral regeneration' emphasizes that partnerships have a beneficial moral effect on all involved participants, strengthening their characters and stimulating creative problem solving skills. 'Partnership as risk shifting' are financially beneficial, as it spreads the financial costs and risks of projects among both sectors. In 'partnership as restructuring public service', private agencies take a more prominent role in public services initially taken up by the government. Lastly, in 'partnership as power sharing' control is spread horizontally, especially in regulatory matters where control has been in the hands of the government. This is based on mutually beneficial sharing of responsibility, knowledge or risk. Thus, as can be seen, these uses of partnerships stress that the government functions are shifted towards the private sector (Linder, 1999, pg.49).

There are not only many different reasons for taking part in public-private cooperation efforts, but these partnerships also take on many different forms. What form works best depends on the nature, scope and risks of the project (Schaeffer & Loveridge, 2002, pg.175). Schaeffer and Loveridge (2002) propose four ideal forms of public-private partnerships. Firstly, a leader-follower relationships may emerge when participants are very unequal in power or resources. It is one of the most widely used forms based on an understanding reached through experience. Secondly, exchange relationships are voluntary based, in which decisions are coordinated between both sectors. Thirdly, joint ventures allows public and private parties to retain their independence while working closely together on issues or projects. This type of partnership is not open ended as they

are dedicated to a specific purpose. Lastly, an ideal typical partnership is one that is open ended in nature, allowing new developments and opportunities to arise (Schaeffer & Loveridge, 2002, pg.175-180). Many distinctions like this one make clear that cooperation between the public and private sector can take different forms depending on the intention and desired outcome of both sectors. It is therefore of no surprise that most of the existing literature revolves around identifying and classifying partnership arrangements (Carr, 2016, pg.54).

2.2.2. Public-private Cooperation and Partnerships in Cybersecurity

For the purpose of this research it is interesting to look specifically at public-private cooperation and partnerships in the cybersecurity realm. Cybersecurity, especially in the context of critical infrastructure protection, is often viewed as a collaborative project between the public and private sector. Since the state is responsible for national security, and most of the critical infrastructure is privately owned, cooperation is inevitable (Carr, 2016, pg.54). Promotion of collaboration between the public and private sector has therefore been central to efforts to manage the challenge of cybersecurity. Knowledge sharing between both sectors is highlighted as a way to mitigate these risks. This is because it provides all relevant parties with a more comprehensive view of the threat landscape, making it easier to govern the uncertainty of cybersecurity risks (Christensen & Petersen, 2017, pg.1440). These views are also evident in the European Union Cybersecurity Strategy. This strategy recognizes the need for a shared responsibility between public and private actors. It therefore encourages voluntary cooperation and information sharing between both sectors (Hiller & Russell, 2013, pg.243).

Just like mainstream public-private partnerships, cybersecurity partnerships can take many different forms. For example, Shore, Du and Zeadally (2011) identify 10 different cybersecurity partnerships with corresponding pros and cons. These arrangements differ according to the strength of influence from either market forces or the government (Shore, Du & Zeadally, 2011, pg.9-11). However, solely focusing on public-private partnerships in the cybersecurity realm is not feasible. Since the Internet is a dominantly private construct, mainstream partnerships are rare. Instead, a wide range of policy initiatives, forums and consultation platforms have been labelled as public-private partnerships (Bossong & Wagner, 2017, pg.269). Eichensehr (2016) therefore

speaks of a public-private cybersecurity system, rather than a public-private partnership. He argues that the private sector and the government do not always act as partners. Instead, the relationship between both sectors can vary from declared partnership to antagonistic (Eichensehr, 2016, pg.478). Thus, this research will take any form of cybersecurity cooperation into consideration instead of focusing on pure partnership forms.

However, issues such as a lack of trust, misplaced expectations and conflicts of interest often hamper public-private cooperation in cybersecurity (Shore, Du & Zeadally, 2011, pg.4). The private sector builds the hardware and software that drives cyberspace and operates much of a nation's critical infrastructure. However, they are hesitant in sharing information about vulnerabilities with the government. This is because they worry that product or service flaws are leaked as well as public revelations of corporate intellectual property (Stavridis & Farkas, 2012, pg.15). Carr (2016) takes Linder's (1999) distinctive uses of the term 'public-private partnership' in explaining the disjuncture of perceptions between the public and private sector in cybersecurity efforts. The 'partnership as management reform' argues that the government takes a bigger role in cybersecurity. Yet, there is widespread belief that governments do not have the authority and capability to deal with cybersecurity in private networks. On the other hand, private actors are profit-maximizing driven and invest less in cybersecurity than what is socially optimal. This disjuncture is at the heart of the tension in public-private cybersecurity partnerships (Carr, 2016, pg.57). Furthermore, Linder's (1999) 'partnership as power sharing' entails cooperation and the mutual beneficial sharing of responsibility. However, partnerships are often characterized by disputed responsibility instead of shared responsibility (Carr, 2016, pg.58). There is also often disagreement between both sectors over the knowledge to be shared. Even though both may agree that cybersecurity risks are there to be shared, they have different notions of what counts as cybersecurity knowledge that will help minimize these risks (Christensen & Petersen, 2017, pg.1440). Furthermore, many actors fear the reputational costs of breaches of their cybersecurity rather than the benefits of shared threat awareness. Mandatory public regulation for a 'duty to notify' in cases of large ICT incidents has therefore become more common (Bossong & Wagner, 2017, pg.273). These points of concern have to be taken into account. This is because this disjuncture may also be evident in this research, resulting in unsuccessful cooperation efforts between the public and private sector.

In order for public-private partnerships in cybersecurity to be effective, knowledge sharing has to be stimulated. Building trust and collaboration is not only a dominant theme in national security strategy documents, but also in responses from the private sector (Carr, 2016, pg.58). This is also the case when looking at Manley's (2015) four essential elements of successful partnerships in cybersecurity. The first step to any successful partnership is building a high level of trust. Without trust, there will be no flow of voluntary information. The second step is to create clear legal guidance in order to nurture a trusted relationship between both sectors. The third step is to implement a bottom-up organization structure to encourage participation from the private sector. Lastly, it is important to involve the community within and surrounding the public and private entities (Manley, 2015, pg.90-96). If this research identifies shortcomings in public-private cooperation in managing cybersecurity risks, these elements can be used in building successful relationships in the future.

2.3. NIST Framework

A theoretical framework is used in order to measure these concepts and answer the research question. By doing so, cybersecurity risk management can be measured and be applied to cooperative efforts between public and private actors in the Port of Rotterdam.

The framework that is used, namely *The National Institute of Standards and Technology (NIST) Cybersecurity Framework*, was enacted in 2014 after the United States Cybersecurity Enhancement Act called for the strengthening of resilience of critical infrastructure. This framework provides guidance for understanding, managing and expressing cybersecurity risks for all relevant stakeholders. It helps in identifying and prioritizing actions for reducing cybersecurity risks and can be used across entire organizations (NIST, 2018, pg.6). The framework can be found in Appendix B.

For the purpose of this research, the Framework Core is used as this provides guidance for the managing of cybersecurity risks as well as a set of activities to achieve specific cybersecurity outcomes (Shackelford, Proia, Martell & Craig, 2015, pg.330). These cybersecurity outcomes

identified by stakeholders are helpful in managing cybersecurity risks. The Core consists of five functions with corresponding categories, subcategories and informative references (NIST, 2018, pg.6). This can be seen in figure 1.

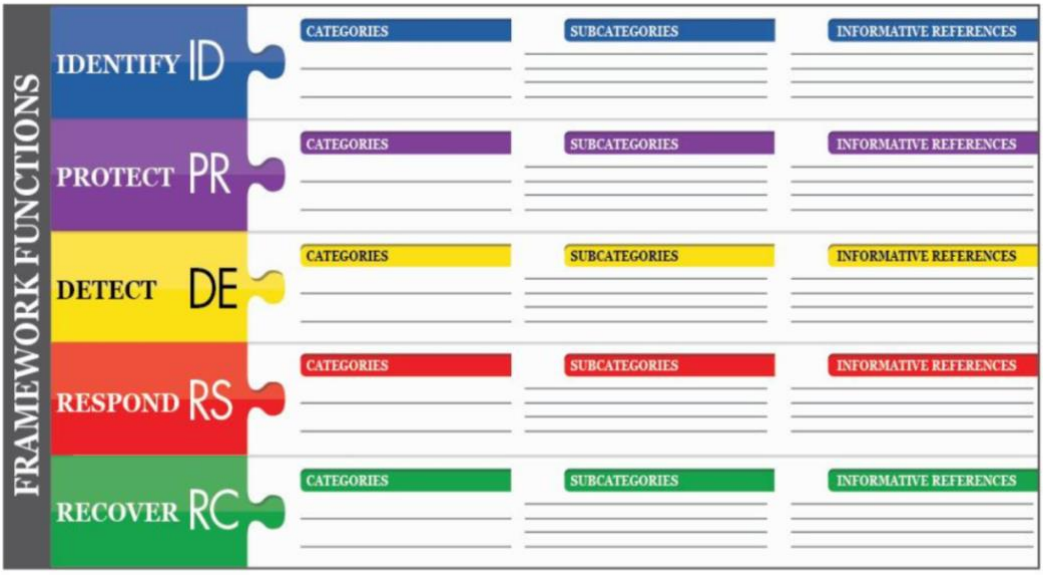

Figure 1: NIST Framework core functions (NIST, 2018, pg.6).

The five functions are Identify, Protect, Detect, Respond and Recover. These functions form the basis of the framework and provide industry standards, guidelines, and practices for communication of cybersecurity activities and outcomes. Each function entails a different step in the cybersecurity risk management process. The Identify, Protect and Detect functions encompass measures to be taken prior to a cybersecurity incident. The Respond function concerns measures that are to be taken during a cybersecurity incident whilst the Recover function provides resiliency measures (NIST, 2018, pg.6). The five functions include categories and subcategories that provide cybersecurity outcomes. The functions with corresponding categories can be seen in figure 2. Furthermore, the informative references provide the organization technical starting points for implementing desired practices (NIST, 2018, pg.6). Each function will be defined as they are of particular importance to this research. This is because they form the main themes along which cooperation efforts between public and private actors can be measured:

1. *Identify*: "Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities" (NIST, 2018, pg.7).
2. *Protect*: "Develop and implement appropriate safeguards to ensure delivery of critical services" (NIST, 2018, pg.7).
3. *Detect*: "Develop and implement appropriate activities to identify the occurrence of a cybersecurity event" (NIST, 2018, pg.7).
4. *Respond*: "Develop and implement appropriate activities to take action regarding a detected cybersecurity incident" (NIST, 2018, pg.8).
5. *Recover*: "Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident" (NIST, 2018, pg.8).

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 2: Functions with corresponding categories (NIST, 2018, pg.23)

The aim of this research is to analyze the extent to which cooperative efforts take place between public and private actors in managing cybersecurity risks. Therefore, the cybersecurity outcomes as specified by the categories and subcategories will be adjusted to cooperation between relevant stakeholders. In order to do so, a selection of categories belonging to each function will be made. Not all categories will be taken up in this research as some are less feasible to use in studying the main research question. This feasibility depends on whether or not the categories can be tailored to cooperative efforts between public and private actors.

3. Methodology

3.1. Research Design

This research sets out to analyze how public and private actors in the Port of Rotterdam cooperate in managing cybersecurity risks. To answer this research question, an inductive qualitative method is used. It is qualitative in nature, in that it is explorative with the aim to get an understanding of a complex phenomenon by means of observation and description (Burkholder, Cox, Crawford & Hitchcock, 2019, pg.83). A grounded theory approach is used in order to enhance theory development. By doing so, research can be done effectively and efficiently because it helps in structuring and organizing data gathering and analysis (Charmaz & Belgrave, 2007, pg.28). Instead of using ordinal values, this research focusses on the interpretation and circumstances of organizations in the Port of Rotterdam. By seeking to explain 'to what extent' cooperation between public and private actors takes place in managing cybersecurity risks, a qualitative approach is best fitting.

3.2. Operationalization

As mentioned previously, not all categories of the NIST Framework are used in this research. This is because the extent to which certain categories are tailored to cybersecurity in individual organizations is significant, making it difficult to apply these to cooperative efforts between public and private actors. Furthermore, there are a total of 108 subcategories. It is beyond the scope of this research to use every single subcategory, especially because not all are relevant to this research. Thus, managing cybersecurity risks is operationalized according to a specific set of categories with corresponding subcategories fit for this research. The categories per function that are taken up in this research are listed in table 1. The indicators are based on the corresponding subcategories and specify what can be understood under each category. It has to be noted that the format of categories and indicators does not imply a degree of importance, but instead represents a common set of activities to manage cybersecurity risks.

Function	Category	Indicators
Identify	Asset Management	- Cooperation efforts regarding the establishment of cybersecurity roles and responsibilities
	Business Environment	- Role of organization in supply chain and criticality of business affecting cybersecurity roles and responsibilities?
	Governance	- How are organizational cybersecurity policies established? - Legal and regulatory requirements that all stakeholders have to comply with
	Risk Assessment	- Cyber threat information received from information sharing forums and sources? - Cooperation efforts to identify internal and external cyber threats
	Risk Management Strategy	- Mutual risk management strategy amongst organizations - How is risk tolerance established?
Protect	Awareness and Training	- The organization's personnel and partners are provided cybersecurity awareness education - Mutual training amongst organizations?

	Information Protection Processes and Procedures	- Sharing of protection technology effectiveness with other stakeholders - How are business continuity plans established? - How are incident recovery plans established?
	Maintenance	- Cooperation regarding maintenance and repairs of information systems
Detect	Anomalies and Events	- Cooperation to detect anomalous events
	Security Continuous Monitoring	- How is the physical environment and network monitored? Information exchange?
Respond	Communications	- Established criteria to respond to incidents? - Information is shared with external stakeholders - Voluntary information sharing amongst stakeholders takes place
	Analysis	- Analysis of incidents is conducted with other stakeholders
	Improvements	- Learning takes place amongst stakeholders - Information is shared with external parties

Recover	Communications	- Recovery activities are communicated to internal and external stakeholders - Cooperation efforts regarding recovery activities?

Table 1: Adjusted NIST Framework

In the Identify function, aspects regarding the understanding of the business context are taken into consideration. Here, the aim is to gain an understanding into how cooperation between public and private actors takes place in assessing the internal and external business environment as well as cybersecurity roles, policies and procedures.

The Protect function concerns actions that limit the impact of potential cybersecurity incidents. Here it is of particular importance to implement appropriate safeguards to ensure the delivery of critical services. An analysis is therefore made whether or not cooperation between public and private actors takes place in limiting such impacts.

The Detect function entails measures aimed at identifying the occurrence of a cybersecurity event. It is especially concerned with the timely discovery of potential cybersecurity incidents. In this research, cooperative efforts regarding the detection of anomalies as well as the continuous monitoring of business assets will be analyzed.

In the Respond function, appropriate activities to take action in case of a detected cybersecurity incident are considered. The communications, analysis and improvements categories will analyze the extent to which public and private stakeholders cooperate in containing the impact of cybersecurity incidents.

Lastly, the Recover function stresses the importance of resilience. Here, appropriate measures are identified that restore any capabilities or services that were harmed due to a cybersecurity incident. A timely recovery will ensure that the impact of cybersecurity incidents is minimized. Thus, an analysis will be made regarding cooperation amongst relevant actors in recovery efforts.

3.3. Data Collection

As the focus is on theory development, data is collected according to the grounded theory design. Therefore, online documents and reports are studied and interviews are held with relevant stakeholders (Burkholder et al., 2019, pg.87). This is done to ensure triangulation. By using more than one approach to research the question, possible limitations from each method are transcended by comparing findings from different perspectives (Heale & Forbes, 2013, pg.98). This particular research uses three different means of data collection, namely: desktop research, document analysis and interviews.

3.3.1. Desktop Research

Desktop research is done in order to study the available literature on cybersecurity risk management and public private cooperation. By doing so, familiarity with the relevant concepts is attained in the initial stages of this research. This serves as crucial input for the conceptualization of theories and operationalization of the theoretical framework. This is primarily done by using academic papers from Google Scholar and other open sources.

3.3.2. Document Analysis

Following desktop research, document analysis is conducted in order to gain insight into current cybersecurity cooperation measures in the Netherlands and in the Port of Rotterdam. Port documents as well as government reports indicating cybersecurity management cooperation forms an initial understanding of this phenomenon. This serves as a starting point for the analysis of this research.

3.3.3. Semi-structured Interviews

Desktop research and available documents are complemented by semi-structured interviews with relevant public and private stakeholders in the Port of Rotterdam. In this type of interview structure,

questions related to the research question are asked while probes are used to explore interviewee responses (Burkholder et al., 2019, pg.149).This is done in order to address issues that are not made publicly available or are missing and not discussed in detail in the existing literature.

All interviews are conducted online. The leading interview questions are divided based on the five functions of the NIST Framework. For each function, questions with regard to the categories are formulated. By doing so, a clear structure is followed which could help in analyzing the data. This interview protocol can be found in Appendix A. The respondents with corresponding job functions are listed in table 2.

Respondent	Sector	Job Function	Interview Date
Respondent 1	Private	IT Engineer	April 29th 2020
Respondent 2	Private	General Manager ICT	May 8th 2020
Respondent 3	Private	Managing Director	May 13th 2020
Respondent 4	Public/Private	Cyber Security Risk Officer & Program manager FERM	May 15th 2020
Respondent 5	Public	Coördinator Landelijk Dekkend Stelsel	May 28th 2020
Respondent 6	Private	Chief Information Security Officer	May 29th 2020

Table 2: Interview respondents

As mentioned and can be seen in table 2, actors from both the public and private sector are interviewed. This is done in order to get different perspectives regarding the research question, as organizations may differ in views regarding cybersecurity cooperation efforts. Furthermore, in reality, private organizations may not adhere to guidelines and standards that public organizations advocate in official reports.

The total set of respondents therefore includes four individuals from different private organizations active in the port. This is done in order to gain insight into how they cooperate with other private actors as well as with relevant public actors. Furthermore, two individuals from the public sector are interviewed: one individual from a Dutch governmental institution and one individual from the Port Authority. By doing so, a greater understanding could be attained regarding how public actors prepare for cyber calamities and communicate with private actors who lease land in the port and operate facilities.

3.4. Data Analysis

Before the interview data is analyzed, an assessment is made of existing documents and reports regarding cybersecurity cooperation in the Netherlands. These documents and reports serve as a basis for understanding the cybersecurity landscape in the Netherlands and the Port of Rotterdam. By doing so, relevant actors and cooperation initiatives can be discussed.

The interview data provides more specific detail regarding cybersecurity cooperation between the public and private sector. This data is analyzed according to the adjusted NIST Framework. For each function and corresponding category, the views of different interviewee's are taken into consideration. The interview data is labelled and organized by using the process of coding. This is done in order to identify different themes and relationships between the respondents. This could provide similarities and differences regarding their views on the topics discussed. Lastly, overlapping themes are taken into consideration in order to analyze the complexities and challenges that remain.

3.5. Reliability and Validity

Reliability is concerned with the replicability and consistency of findings, in that data collection procedures and analysis yield similar answers for multiple participants in the research process (Franklin, Ballan & Thyer, 2001, pg.273). In order to increase consistency, the interview protocol consists of pre-set questions that are asked in every interview.

Reliability is a precondition for validity. Validity is concerned with the truthfulness of study findings. If observations are not consistent and dependable, they are not likely to be accurate (Franklin, Ballan & Thyer, 2001, pg.278). As mentioned, triangulation is ensured by using multiple approaches to conduct this research. This increases the validity of this research as a more comprehensive understanding of cybersecurity cooperation in the port can be attained. However, the external validity is limited due to the number of respondents. The limited sample size makes generalization difficult and therefore conclusions drawn may not hold true for other organizations, sectors or ports.

4. Analysis

This chapter forms the analysis of this research. It contains collected data from policy documents and interviews. First, it provides an understanding of public-private cybersecurity partnerships in the Netherlands by analyzing existing policy documents. This knowledge serves as a basis for understanding cooperation efforts in the Port of Rotterdam. This will therefore be followed by a section addressing collaborative initiatives taken to manage cybersecurity risks within the port community.

In order to delve deeper into organizational views regarding these matters, the latter part of this analysis discusses the interview findings based on the NIST Framework. This section examines the findings per function of the adjusted framework as discussed in chapter three. It analyzes the views of organizations with regard to cybersecurity cooperation between the public and private sector in the port. This can show similarities and differences between what is advocated in policy documents and how organizations perceive this to take place in reality.

4.1. Public-private Partnerships in the Netherlands

As mentioned, this section discusses existing policy documents regarding cybersecurity cooperation between the public and private sector in the Netherlands. An overview regarding cooperation initiatives provides knowledge on the current Dutch cybersecurity situation. First, it discusses background information addressing increasing digitalization in the Netherlands, the effect this has on public-private partnership importance as well as key public actors in the Dutch cybersecurity domain. This is complemented by an analysis of existing cybersecurity cooperation initiatives in the Netherlands. This forms an understanding of how the Dutch government views public-private cooperation in the domain of cybersecurity as well as different forms of partnerships advocated by the government.

4.1.1. Background

Increasing Digitalization

Due to digitalization, cybersecurity incidents are not limited to one sector, but instead spread through other sectors (NCTV, 2019, pg.21). It is therefore of no surprise that Dutch government documents increasingly warn for possible cascading effects of cybersecurity in vital processes. Any disruption has the potential to cause major societal effects, posing risks to national security. According to the NCSC, the Dutch approach to cybersecurity therefore has the following goal: The Netherlands is able to safely capitalize on the economic and social opportunities of digitization and to protect national security in the digital domain (NCSC, 2018, p. 17).

Need for Public-private Partnerships

However, the government cannot provide digital security on its own. The NCSC stresses the importance of all relevant parties to take their responsibility and make the Netherlands digitally safe. This can only be accomplished if it is designed, developed and evaluated in public-private partnerships (NCSC, 2018, pg.43). Involving the business community in this matter is essential. According to the NCSC, public-private partnerships are therefore at the basis of the Dutch cyber security approach (NCSC, 2018, p.7).

The National Coordinator for Security and Counterterrorism (NCTV) has stated that threats from criminals remains high (NCTV, 2019, pg.7). As a matter of fact, threats outweigh resilience measures. This situation requires additional efforts by the government, business and citizens to strengthen the Dutch cybersecurity approach (NCSC, 2018, p.8). Furthermore, large organizations often organize their own security operations center or crisis team, while smaller organizations are insufficiently aware of digital risks. Especially organizations that are vital to national security have a better understanding of digital threats and attacks (NCSC, 2018, p.19). Thus, strengthening Dutch cybersecurity can be done by the sharing of available knowledge between the public and private sector. As knowledge is crucial for cybersecurity, the promotion of information sharing is necessary to strengthen cybersecurity in all sectors (NCSC, 2018, p.7). It is therefore of no surprise

that current Dutch government reports stress the need to include the private sector in minimizing cybersecurity risks.

The Dutch Cybersecurity Domain

As can be seen, the Dutch government is actively involved in raising awareness regarding the effects of digitalization as well as the need for public-private cooperation. This is especially done with the help of the NCSC, a key player in enhancing the resilience of the Netherlands in the cyber domain. The NCSC is a separate agency under the Secretary General of the Ministry of Justice and Security and acts as the central information hub and center for expertise with regard to cyber security in the Netherlands (NCSC, 2019, pg.1). It supports the government and operators in vital infrastructure by offering advice and expertise, threat responses as well as actions to strengthen crisis management. Furthermore, its task is to realize an open, safe and stable information society by sharing information. This is done in collaboration with the business community, government bodies and academics (NCSC, 2016, pg.5). A schematic overview of the NCSC target audience and partners can be seen in figure 3.

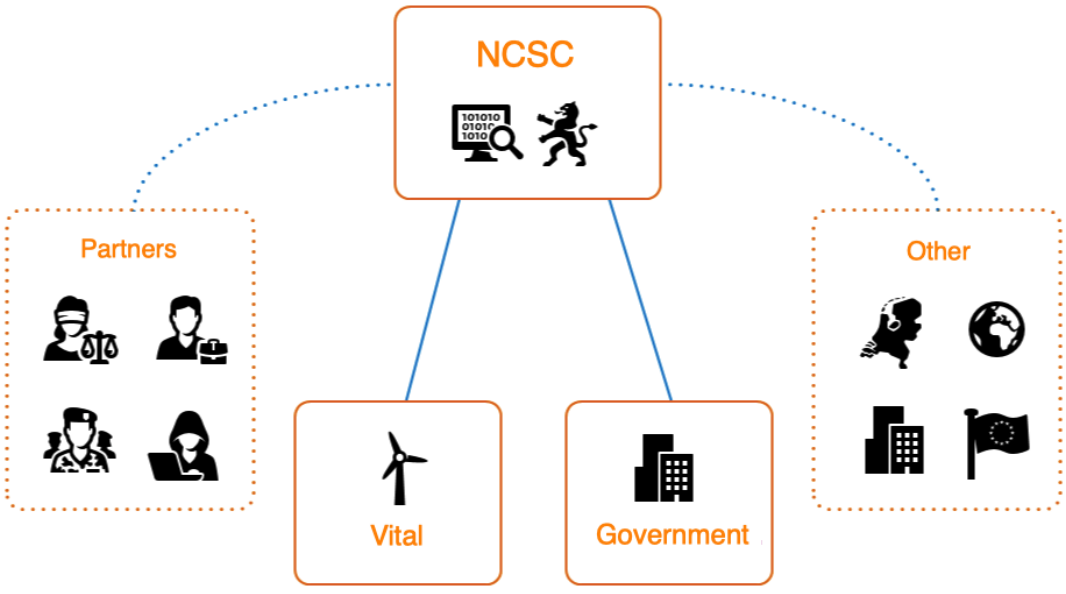

Figure 3: NCSC target audience and partners. Adapted from: NCSC (https://www.ncsc.nl/over-ncsc/onze-partners)

As figure 3 indicates, the primary target group of the NCSC is the government and organizations with a vital function in Dutch society. Since cybersecurity is too comprehensive to be managed by a single sector, cooperation is essential. It therefore cooperates with public and private parties, professionals in practice, education and academia as well as international partners (NCSC, 2019, pg.3).

In 2017, the Ministry of Economic Affairs and Climate Policy and the Ministry of Justice and Security joined forces to set up the Digital Trust Center (DTC). This organization aims to make companies more resilient against cyber threats and has two main tasks. Firstly, it seeks to give advice and provide companies with reliable information about digital vulnerabilities. Secondly, its task is to stimulate cybersecurity partnerships between companies. The DTC uses expertise from the NCSC and shares this knowledge on cybersecurity partnerships with companies in the Netherlands (DTC, 2018, pg.2). It encourages partnerships that can help its target group of 1.6 million Dutch companies to be digitally safe. By stimulating knowledge sharing, joint risk identification and joint specialized service purchasing, the DTC aims to increase digital resilience in the Netherlands (Rijksoverheid, 2018).

4.1.2. Collaboration Initiatives

Together with the NCSC, the DTC has developed three guidelines to help organizations start a cybersecurity partnership. By doing so, the NCSC and the DTC hope to boost the goal of creating a nationwide network of cyber resilience partnerships in the Netherlands. Most partnerships focus on the government and operators of vital infrastructure. These guidelines however, help non-governmental and non-vital organizations to also form partnerships (DTC, 2018). The guidelines entail regional collaborations, supply chain collaborations and information sharing and analysis centers (ISAC).

Regional Collaboration

In a regional collaboration, a large number of diverse groups interact with one another for a range of purposes. Private businesses, individuals, government bodies, processes and smart devices can

make up a regional collaboration. These actors form a network of relationships in which information is shared within a specific region. By doing so, organizations are incentivized to look outwards and counter digital threats together with other relevant stakeholders (NCSC, 2018, pg.4). An example of a regional collaboration is FERM in the Port of Rotterdam (NCSC, 2018, pg.3).

Supply Chain Collaboration

A supply chain collaboration aims at bringing organizations in a supply chain together to reduce digital risks. By working together, the capacity to recognize vulnerabilities is increased whilst reducing potential risks. This is done by sharing information, mutual analysis of cyber risks and taking counter measures together with the entire supply chain. Supply chain collaboration can vary from ad hoc initiatives to formalized forms of coordination and strategic cooperation. However, when there is a strong supply chain dependency, cooperation is necessary (NCSC, 2018, pg.5-6).

Information Sharing and Analysis Center (ISAC)

Lastly, ISAC's are public-private partnerships organized per sector and facilitated by the NCSC. Participants exchange information and experiences about cybersecurity under a strict set of rules (TNO, 2017, pg.9). A trusted environment is created in which organizations from the same sector share information on incidents, vulnerabilities, threats, measures as well as lessons learned with regard to cybersecurity. Information is therefore more quickly received whilst optimizing situational awareness. There is no standard format for an ISAC, as cooperation can be formal or informal with different mixes of working methods. Furthermore, any sector can start an ISAC without approval of the NCSC (NCSC, 2018, pg.4). In the Netherlands, many different ISAC's exist and the number continues to grow (Heuvel & Baltink, 2014, pg.121). These are based on different sectors, namely: Airport, Chemical/Oil, Drinking Water, Energy, Financial Institutions, Healthcare, Legal, Media, Multinationals, Managed Service Providers, Nuclear, Pensions, National Government, Port, Telecom, and Water Management (NCSC, 2018, pg.3).

4.2. Public Private Cooperation in the Port of Rotterdam

When looking at the Port of Rotterdam in particular, it is clear that digitalization has a major impact on its operations. The port has the ambition to become the smartest in the world and therefore aims to be at the forefront of the digital transformation in the port and logistics sector. Not only does digitalization of operations increase the efficiency of the port, but it also improves its competitive position. As it contributes to more transparency, reliability, flexibility and sustainability, the digital transformation brings about numerous positive benefits (Havenbedrijf, 2019, pg.68-69).

However, it also bring about digital risks in the port area. IT disruptions can be disastrous as they are not limited to the affected company, but can have secondary effects on indirectly involved parties or processes elsewhere in the supply chain (PoR, 2018, pg.3). As a result, cybersecurity remains a top priority for the Port Authority. Measures have been taken to raise awareness of cyber risks and increase infrastructure resiliency (Havenbedrijf, 2019, pg.66). For example, six ICT specialists are now employed by the Port Authority whilst the Harbor Master has been appointed as the Port Cyber Resilience Officer. Furthermore, as smaller companies have less money available for complex security issues, initiatives have been launched that emphasize cooperation in increasing cybersecurity resilience (PoR, 2016). These initiatives are based on the three types of collaborations discussed at the beginning of this chapter.

4.2.1. Collaboration Initiatives in the Port of Rotterdam

These collaborations are instruments in enhancing cybersecurity cooperation between organizations in the port community. Each type facilitates information exchange and experience sharing between both private and public organizations. Gaining an understanding of the following initiatives is therefore vital in understanding the cybersecurity landscape in the Port of Rotterdam.

FERM

FERM is a public-private partnership consisting of the Port Authority, Deltalinqs, Seaport Police and the Municipality of Rotterdam. The Public Prosecution Service, DCMR, the NCSC and the

Rotterdam-Rijnmond Security Region are also closely involved in the program. This initiative aims to increase the sharing of knowledge and best practices between the companies in the port of Rotterdam (Havenbedrijf, 2019, p.66). It is therefore a regional collaboration in which a large number of diverse actors interact both online and offline with one another to increase cyber resiliency:

"The Port of Rotterdam is an ecosystem which links together a great number of businesses in some form or other, both physically and digitally. Disruptions can have a major impact on the process that allows secure and smooth entry to, and exit from, the port and of course also secure and smooth loading and unloading. We forge connections online as well as offline so we can guarantee the digital security of our businesses and the port together. We are FERM. That is not an acronym, but our Rotterdam way of expressing that we are resilient." – FERM Rotterdam (NCSC, 2018, pg.4).

As part of this program, the Mayor of Rotterdam appointed the Harbor Master as Cyber Resilience Officer in 2016. This was done to strengthen cooperation between business and government in order to enhance resiliency against cybercrime. The Harbor Master is a logical choice, as its network consists of port business, the municipality, the police as well as the public prosecution service (FERM, 2016). It's task is not only to create awareness, but also to strengthen cooperation and best practices sharing between all organizations in the port. Furthermore, as part of the program, so-called Port Cyber Cafés are held regularly. These meetings are organized to facilitate knowledge sharing about digital vulnerabilities. This is done in an informal setting in which experts in the field of cybersecurity participate (Deltalinqs, 2018).

Portbase

FERM consist of many participants, one of which is Portbase. Portbase was founded in 2009 by the Port of Rotterdam and Port of Amsterdam. It's aim is to make the Dutch port community the smartest in Europe and to connect all parties in the logistics chains. Through its Port Community System, it allows organizations to work faster, more efficiently and at a lower cost. This is because it facilitates the exchange of data between organizations and information sharing with government

authorities (Portbase, 2016). By exchanging data with government systems, Portbase allows for the development of public-private initiatives. As it brings together data from government bodies and logistics companies, overall insight into the logistics chain is increased. Thus, a supply chain collaboration is formed, resulting in the government to be able to make risk analysis and organizations operate more smoothly. What is of particular importance however, is that the set-up of a well-secured system for data exchange better safeguards organizations against cybercrime (Portbase, 2020, pg.3). It is therefore of no surprise that Portbase takes part in FERM in raising cyber resilience awareness amongst organizations in the port.

"As a provider of a supply chain information system in the Port of Rotterdam, it is evident that the informal side of a logistics chain is very important. Informal relationships with other individuals in a chain ensures that you can easily reach out during an emergency." – Portbase (NCSC, 2018, pg.5).

Port-ISAC

The Port of Rotterdam is home to one ISAC, namely, the port-ISAC. It consists of large and small organizations that are part of the vital processes in the port. The port-ISAC therefore serves as a means to bring together these organizations and stimulate information sharing as well as the sharing of experiences (Respondent 5, Public sector).

"Within the Port ISAC, we as port-related businesses and organizations realize how dependent we are on each other as well as on systems, and how much we can still learn. We do not just consider Rotterdam as the largest European port in this respect, but we also seek the connection with Europe's second port, Antwerp. For this reason, we paid a first visit to Antwerp three years ago for an inside view. Although we did expect that we shared quite a few challenges and ambitions, we were surprised to learn how much we could learn from each other and reinforce one another. As a result, we meet every year now." - Port-ISAC (NCSC, 2018, pg.10)

As mentioned, ISAC's are facilitated by the NCSC. This is also the case for the port-ISAC, as the secretary position is held by an NCSC employee. It therefore serves as a platform for member organizations and the NCSC to exchange information (Respondent 5, Public sector).

4.2.2. Port Cyber Notification Desk

Another important initiative that facilitates cybersecurity cooperation between the public and private sector is the Port Cyber Notification Desk. The notification desk was established in 2018 and serves as a platform for organizations in the port to report unintentional and intentional IT disruptions. Reporting is mandatory for companies required to comply with the International Ship and Port Security Code (ISPS). This code is a set of measures intended to increase the security of ships and port facilities. Companies that do not have to comply with the ISPS Code are urged to report any IT disruption voluntarily (PoR, 2018, pg.4-6).

What is of importance however, is that the notification desk results in closer cybersecurity cooperation between the public and private sector. Once an IT disruption has been reported, the Harbor Master will take measures to ensure port security. If necessary, the Harbor Master can inform third-parties and share information about the disruption. These third-parties include: Nautical service providers, The Seaport Police, The Rotterdam-Rijnmond Safety Region, the NCSC as well as other relevant stakeholders (PoR, 2018, pg.9). It is therefore a way to involve the public sector in handling significant IT disruptions.

4.3. Applying the NIST Framework to the Port of Rotterdam

The previous section has given an overview of cybersecurity cooperation initiatives in the Port of Rotterdam. Existing policy documents and reports have given insight into the way in which public and private organizations in the port can work together in minimizing cybersecurity risks. Even though this provides a general understanding of the cybersecurity landscape and its cooperation efforts, more detailed information is needed to be able to answer the research question. This is because there is a possibility that not all organizations in the port cooperate in managing cybersecurity risks as advocated in policy documents and reports.

This section will therefore discuss the results of the interviews. It analyzes the functions and categories of the adjusted NIST Framework, giving a more detailed picture of cybersecurity cooperation efforts in the port.

Identify

As was explained, the identify function is concerned with understanding the management of cybersecurity risks to an organization's systems, data, assets and overall capabilities (NIST, 2018, pg.7). The aim of this first function is to evaluate the context of an organization and to prioritize the cybersecurity efforts and strategies to minimize its risks. Following the adjusted Framework, five categories are taken into consideration. These categories are tailored to cooperation between public and private actors in prioritizing cybersecurity efforts and strategies.

Asset Management

When considering asset management, the focus is on adequately identifying organizational assets consistent with their relative importance to organizational objectives. Cybersecurity roles and responsibilities should therefore be established (NIST, 2018, pg.24). Considering the port community, it becomes clear that this is mostly done internally without public actor help. This is especially true for larger organizations that also operate in other ports around the world. Their local IT strategy, which includes the establishment of cybersecurity roles, is often based on global policy (Respondent 3, Private sector). As a result, cybersecurity roles are an organization's own responsibility without the help of the public sector. The public sector can advise organizations in establishing cybersecurity roles (Respondent 1, Private sector). However, none of the respondents suggested that this was the case, indicating that cooperation in asset management is minimal.

Business Environment

Furthermore, the business environment can influence cybersecurity within organizations. Resilience measures may be required to support delivery of critical services (NIST, 2018, pg.25).

Since the port is part of vital infrastructure of the Netherlands, one may assume that this can affect the establishment of cybersecurity roles and responsibilities within organizations. According to the Wet Beveiliging Netwerk- en Informatiesystemen (Wbni), the port is part of Dutch vital infrastructure. The Harbor Master is responsible for the handling of shipping traffic in a safe manner and is accountable to the Municipality of Rotterdam and the Dutch government (JenV, 2018, pg.10). The Port Authority therefore has to comply to cybersecurity standards set by the government (Respondent 4, Public/Private sector). However, individual organizations in the port are not labeled as vital by the government. The private sector does not have to comply with cybersecurity standards as stipulated by the public sector (Respondent 2, Private sector). The business environment, in the sense that the port is labeled as critical infrastructure, therefore has no influence on closer cybersecurity cooperation between the public and private sector.

Governance

The same goes for governance, which is concerned with an organization's regulatory, legal and risk requirements in the domain of cybersecurity (NIST, 2018, pg.25). When looking at the establishment of cybersecurity policies, it is evident that both sectors do not work together. Here it is also the case that larger organizations base their local cybersecurity policies on a global strategy. This global cybersecurity strategy is often formulated by different divisions or departments within an organization (Respondent 2, Private sector). The public sector does not require private organizations to comply with certain cybersecurity policies. This is therefore also done on an individual basis.

Risk Assessment

With regard to risk assessment, organizations should understand cybersecurity risks to its operations and assets. This can be done by identifying internal and external threats and receiving threat intelligence from external sources (NIST, 2018, pg.26-27). One may therefore think that the sharing of cyber threat information between organizations is of importance. However, the public and private sector in the port are hesitant in doing so. Within the port-ISAC, cyber threats are shared amongst its members. This information is often received from the NCSC (Respondent 6,

Private sector). The ISAC therefore serves as a direct link between the NCSC and member organizations. However, the port-ISAC only consists of a small number of large organizations. It can therefore be argued that the majority of the port does not enjoy these benefits. Instead, the sharing of threat information is done within the organization itself or with organizational partners. Active sharing with and by the public sector is therefore minimal (Respondent 1, Private sector).

This is also because the NCSC cannot share cybersecurity information directly with non-governmental and non-vital organizations. It can only directly share such information with organizations labeled as vital, such as the Port Authority (Respondent 4, Public/Private sector). The only way the NCSC can indirectly share information with non-vital organizations in the port is through the DTC (Respondent 5, Public sector). Since the DTC is part of FERM, it acts as a middleman between the NCSC and non-vital organizations that take part in FERM. Any information received by the DTC from the NCSC can be forwarded to FERM (Respondent 4, Public/Private sector). Thus, it can be seen that cyber threat information sharing depends on the criticality of an organization. Since private organizations in the port are not labeled as vital, direct information sharing by the public sector is very limited.

Risk Management Strategy

When delving deeper into an organization's strategy, risk management efforts can be analyzed. Here, the organization's priorities, constraints and risk tolerances are established and used to support operational risk decisions (NIST, 2018, pg.27). All respondents indicated that the establishment of a risk management strategy is done internally with no public help. One respondent indicated that the port has a risk strategy, but that they are not actively involved (Respondent 2, Private sector).

For example, the establishment of risk tolerances is part of an organization's risk management strategy. Here, it can be seen that cooperation is lacking as both public and private organizations have their own requirements regarding risk tolerance. There is no fixed risk tolerance assessment scheme or requirement that every organization in the port has to use. Three respondents from the private sector indicated that this is done internally, based on standards as defined by the

organization itself. Such standards take into consideration the possibility and impact of a potential cybersecurity incident as well as the level of risk that is tolerable (Respondents 1, 2 & 3, Private sector). The Port Authority also establishes risks and corresponding tolerances on its own without external input (Respondent 4, Public/Private sector). It can therefore be seen that both public and private organizations in the port formulate risk management strategies on their own.

Protect

As previously mentioned, the protect function supports the ability to minimize and contain the impact resulting from a cybersecurity incident. This function therefore provides safeguards intended to keep an organization up and running (NIST, 2018, pg.7). Here it is of particular importance to analyze how the public and private sector cooperate in minimizing the impact of potential cybersecurity incidents. In order to do so, three categories that correspond to this function are taken into consideration as they each provide an understanding of cooperation in this domain.

Awareness and Training

Cybersecurity awareness education and training to perform cybersecurity related duties and responsibilities should be consistent with related policies, procedures and agreements (NIST, 2018, pg.31). When looking at cybersecurity awareness and training in the port, it is evident that there are many initiatives. The ways in which awareness is raised by the individual organizations varies. Phishing mails, e-learnings and infected USB's are some of the ways in which employees are tested. The Port Authority also raises awareness in the port through the FERM program. By sending newsletters to over 1500 individuals in the port, it aims to reach out to the private sector (Respondent 4, Public/Private sector). However, all respondents from the private sector indicated that their organization has their own cybersecurity awareness programs in place and that this is done internally. Furthermore, public actor involvement is minimal. The NCSC will only do so in the port-ISAC or through online means. For example, the NCSC has an online 'cybercompass' that shares global developments that can have an impact on organizations (Respondent 5, Public sector). Thus, port-wide cooperation in raising cybersecurity awareness is limited.

All respondents from the private sector also indicated that they do not take part in any mutual training initiatives with other organizations. Instead, they have their own cybersecurity exercises and trainings in place. Here it is also the case that some organizations are more inward looking and operate within the organizational group (Respondent 3, Private sector). Trainings can be technical in nature, or purely theoretical. They can involve checklists and protocols in which individuals from different layers in the organization participate (Respondent 2, Private sector). Some respondents indicated that they have never heard of any training initiatives coming from the public sector, and in particular the government (Respondent 1, Private sector). Nonetheless, cybersecurity exercises have recently been organized in the port in which both the private and public sector participate. As mentioned, FERM facilitates Port Cyber Cafés which are held five times a year. Furthermore, recently a training on operational technology was held in which 10 companies participated. According to the Port Authority this was the first time that an actual training was held with private organizations (Respondent 4, Public/Private sector). Mutual trainings including both the public and private sector have therefore taken place, but it is to be seen if these will continue to be held in the future.

Information Protection Processes and Procedures

Information protection processes and procedures contain security policies used to manage the protection of information systems and assets. The sharing of protection technology effectiveness forms part of this category (NIST, 2018, pg.33). The respondents from the private sector are hesitant in sharing the effectiveness of cybersecurity technology. Even though it is sometimes tested by external parties, sharing the outcome with others is mostly not done due to privacy concerns (Respondent 1, Private sector). Some respondents indicated that this kind of information can be shared through informal channels on a need-to-know basis. Sharing the effectiveness of cybersecurity technology can be shared without giving away too much detail, especially through channels like the port-ISAC (Respondent 6, Private sector). Respondents from the public sector also refer to the port-ISAC when asked about this matter. Even though there is no specific platform in place to do so, the sharing of experiences is promoted through the port-ISAC. The public sector therefore does not inform private organizations about specific cybersecurity technology, but instead encourages organizations to share their experiences with one another (Respondent 4,

Public/Private sector). Any sharing between the public and private sector therefore seems to be minimal. The port-ISAC is the only platform in which this may occur, but even so, organizations are hesitant in doing so.

Maintenance

Furthermore, the maintenance and repairs of information systems should be performed consistent with policies and procedures (NIST, 2018, pg.36). This is established without cooperation with other actors, as respondents indicated this was done internally. There will only be some sort of cooperation if organizations have shared IT infrastructure. However, there are very few shared IT infrastructures as most organizations in the port have their own IT infrastructure (Respondent 4, Public/Private sector). Large scale cooperation in the port when it comes to maintenance and repairs is therefore non-existent.

Detect

The next step in the NIST framework is the detection of cybersecurity incidents. Here the focus is on implementing appropriate measures that aid in identifying potential cybersecurity events. If done appropriately, these measures should allow for the timely discovery of such incidents (NIST, 2018, pg.7). Here, two categories are discussed that give insight into cooperative efforts regarding this function.

Anomalies and Events

Detecting anomalous activities should be done in a timely manner and requires IT personnel to understand each individual event (NIST, 2018, pg.38). All respondents indicated that this is done, but that no cooperation takes place with other actors. Detection is therefore instigated internally without help of other private organizations or the public sector. Any anomalous activity is detected by the organizations' internal systems. The larger organizations have global IT systems in place that help in doing so (Respondent 3, Private sector). Only if events are deemed serious enough to be shared, will this be done in the port-ISAC. The Port Authority has direct channels with

organizations in the port-ISAC to share this information. However, a port-wide system to share and detect anomalous events is currently missing (Respondent 4, Public/Private sector). Even though sharing takes place in the port-ISAC, detecting anomalous activity with one another is not done yet. If this is to be done, it would need to become more developed (Respondent 5, Public sector).

The reason why cooperating in detecting anomalous events does not take place is because it is rather complex. Detection takes specific skills and a lot of time. In essence, this would mean that there needs to be an overarching Security Operations Center (SOC) in the port (Respondent 5, Public sector). Given the fact that all organizations have their own IT systems and infrastructure, this is difficult to do. Furthermore, even though many cyber-attacks take place every day, most are not seriousness enough to share. Only if attacks are deemed serious and complex enough will it be beneficial to inform others (Respondent 4, Public/Private sector). On top of this, privacy concerns hamper cooperation, as cooperation would mean organizations have access to each other's information systems (Respondent 2, Private sector). The port community is therefore not ready to open up their systems. As a result, detection information sharing is a one way street. The Port Authority shares serious information to the port community, whilst the port community is hesitant to share any information with public actors (Respondent 4, Public/Private sector).

Nonetheless, several respondents mentioned that when it comes to sharing such information with others, FERM can be a platform to do so. Private actors in the port feel the need to work together regarding this matter (Respondent 4, Public/Private sector). In order to do so it is key to adequately appoint platforms and make rules to facilitate mutual information sharing.

Security Continuous Monitoring

Organizations in the port therefore monitor their information systems individually. All respondents indicated that this is done continuously without external help. One respondent indicated that 90 percent of the monitoring is done individually (Respondent 1, Private sector). Both public and private actors have their own monitoring systems in place. Companies without these systems are either currently setting it up or do not have the financial means to do so (Respondent 4,

Public/Private sector). This is not a surprise given the fact that most companies have their own IT infrastructure in place. Cooperative efforts in monitoring information systems is therefore minimal.

The only way in which the public sector gets involved is through the National Detection Network (NDN). The NDN is part of the NCSC and is a partnership consisting of all the Dutch security agencies. It allows for easy and effective sharing of threat information, expertise and advice. However, only the government and critical organizations are allowed to take part in this initiative (NCSC, 2018, pg.1). The NCSC therefore does not share any threat information with non-vital organizations in the port (Respondent 5, Public sector).

Some companies in the port monitor their system thoroughly, while others do not (Respondent 6, Private sector). This may be a point of concern as it is beneficial for the entire port that all organizations monitor their IT systems. Failing to do so may make it easier for certain organizations to be attacked, significantly increasing the risks of spill-over effects to other organizations. FERM may be a suitable platform to cooperate in monitoring information systems by creating a central SOC. As a matter of fact, this was once an ambition of FERM. Nevertheless, as most organizations currently monitor their own systems, this is something that may be accomplished in the future (Respondent 4, Public/Private sector).

Respond

Once a cybersecurity incident has been detected, action has to be taken to contain the impact (NIST, 2018, pg.8). The aim here is to analyze how public and private actors cooperate in developing and implementing appropriate activities in responding to such events. In order to do so, three categories of the adjusted NIST Framework are discussed.

Communications

Response activities with regard to cybersecurity incidents have to be coordinated with internal and external stakeholders. In this case, external stakeholders may be part of the public sector (NIST,

2018, pg.41). Information sharing could therefore take place according to established criteria as well as on a voluntary basis.

As mentioned, it is mandatory for companies that have to comply with the ISPS code to report significant IT disruptions to the Harbor Master and Port Authority. If necessary, they can forward the report to actors in the public sector such as the NCSC (PoR, 2018, pg.9). All of the private organizations that were interviewed are ISPS compliant organizations, meaning that they have to report IT disruptions that have consequences for the security and continuity of the port. Respondents indicated that they indeed have to report disruptions to the public sector if certain conditions are met. This is especially the case if there are privacy and confidentiality concerns (Respondent 1, Private sector). This indicates that there is definitely cooperation between the public and private sector when IT disruptions are serious enough and could potentially have significant consequences for the port as a whole. Most of the time however, cyber incidents are not serious enough that result in large scale cooperation efforts in the port community (Respondent 2, Private sector). Thus, depending on the type of incident and the extent of its impact, information sharing takes place.

When asked about voluntary information sharing, the opinions of respondents differed in the extent to which they believed this is done. Some respondents indicated that they hardly share information on a voluntary basis (Respondent 1 & 3, Private sector). Others are more optimistic and believe it does take place within the port community. According to one respondent, all information sharing that takes place within the port is voluntary (Respondent 6, Private sector). This is especially true for the port-ISAC which, according to the Port Authority, is the only place together with FERM in which voluntary information sharing takes place (Respondent 4, Public/Private sector). However, private organizations seem less inclined to voluntarily share information with the public sector. According to article 16 of the Wbni, all organizations in the Netherlands can voluntary report cybersecurity incidents to the NCSC. In essence, this is formal voluntary information sharing and will enable the NCSC to offer assistance. However, this is an instrument that is not used often by private organizations. Furthermore, informal voluntary information sharing without article 16 of the Wbni is also minimal (Respondent 5, Public sector).

This lack in voluntary information sharing with the public sector could be because a lot of organizations have their own SOC in place that offers assistance during a cybersecurity incident. Furthermore, if incidents do take place, it is more likely that private forensic companies like Fox-IT are called in for help instead of the public sector. This is because most organizations are skeptical of the government. A lot of organizations are afraid that information sharing with governmental institutions like the NCSC will result in visits from public inspectors (Respondent 5, Public sector). Organizations also hold back because of competitiveness. Letting other organizations know that there has been a hack with the result that operations are on hold is unfavorable (Respondent 6, Private sector). There is therefore definitely room for improvement when it comes to voluntary information sharing between the public and private sector. FERM is a platform that aims to facilitate this in the future, since the port-ISAC only contains a small portion of the port community (Respondent 4, Public/Private sector).

As the NCSC indicates, it is very important to develop a level of trust with the private sector. This is especially true for vital organizations. A high level of trust will result in organizations to report smaller cybersecurity incidents as well without the mandatory reporting standards. If organizations in the port report these smaller incidents voluntarily, the NCSC can use this information in improving the safety of other sectors in the Netherlands (Respondent 5, Public sector). As mentioned, Manley (2015) argues that the first step in any successful partnership is building a high level of trust. Without trust, the flow of voluntary information sharing will be minimal (Manley, 2015, pg.90).

Analysis

It is also important to perform an analysis of cybersecurity incidents to ensure effective response and support recovery activities (NIST, 2018, pg.42). Respondents indicated that cooperation in performing analysis depends on the type of hack and the willingness of organizations to work together. Cooperation does not necessarily take place in analyzing the cybersecurity incident itself, but rather in analyzing the effects and measures needed to go back to the old situation (Respondent 3, Private sector). It is therefore up to the organization to decide which actors to cooperate with in performing an analysis. These include but are not limited to insurance companies, private forensics,

police, the NCSC and the Port Authority (Respondent 6, Private sector). There are therefore no requirements in place regarding performing an analysis with certain external actors.

Improvements

Improvements can be realized if organizations learn from one another. These lessons learned can be taken up in response activities, enabling organizations to tackle cybersecurity incidents more effectively (NIST, 2018, pg.43). Some respondents mentioned that learning takes place in the port-ISAC and FERM. One of the goals of FERM is to promote learning amongst members (Respondent 1 & 4, Public/Private sector). As discussed, trainings are held involving both public and private actors. Trainings like these are perfect opportunities to learn from one another. Nonetheless, according to the Port Authority the amount of learning still needs to improve (Respondent 4, Public/Private sector).

However, what is interesting here is that all respondents referred to the APM/Maersk hack of 2017 when discussing lessons learned. This not only indicates the profound impact this particular hack had on the port community, but also that it resulted in many lessons learned when it comes to port cybersecurity. Delving deeper into this particular hack, it becomes clear that this was a turning point in cybersecurity policy in the port. It served as a major wake-up call, resulting in cybersecurity initiatives like FERM to take flight. Organizations have since become more aware of cybersecurity risks and the need to become more resilient (Respondent 6, Private sector). In particular, it became apparent that network segmentation was lacking. This was not done sufficiently. Business assets were not segmented, making it easy for the virus to spread. As a result, organizations have now segmented their networks by using firewalls and other technical measures (Respondent 2, Private sector). Before, large organizations would have global firewalls, but now local firewalls have also been implemented to secure segmentation (Respondent 3, Private sector). Furthermore, this hack resulted in the establishment of the Port Cyber Notification Desk, encouraging large organizations to report IT disruptions to the public sector. All these measures indicate that learning definitely takes place within the port community.

Recover

Lastly, the recover function is concerned with restoring any capabilities or services that were impaired due to a cybersecurity incident. It supports the timely recovery to normal operations to reduce the impact. This means organizations have taken all necessary actions to arrive at the best outcome when dealing with cybersecurity incidents (NIST, 2018, pg.8). Here, the aim is to analyze cooperation efforts in recovering after a potential cybersecurity event. This will be done by taking the following category into consideration.

Communications

Restoration activities should be coordinated with internal and external stakeholders (NIST, 2018, pg.44). Some respondents indicated this is the case. At first, a cybersecurity incident will be dealt with internally. If it is serious enough, external private or public stakeholders may be notified (Respondent 2, Private sector). As mentioned, it is mandatory for ISPS companies to report serious IT disruptions to the Port Authority, whom may notify public actors such as the NCSC. Thus, depending on the type of cybersecurity incident, restoration cooperation will take place between the public and private sector. However, one respondent mentioned they would seek for help in recovery in the private market. Private organizations like Fox-IT and Deloitte would be hired to perform forensic analysis (Respondent 1, Private sector). This indicates that some organizations prefer specialists from the private sector over public actors. Again, whether or not this occurs depends on the type and seriousness of the incident.

4.4. Summary

The interview analysis that complements existing policy documents gives a more detailed understanding of cybersecurity cooperation between the public and private sector in the Port of Rotterdam. Information coming from these interviews provides a more thorough understanding of cooperation in reality. This actuality is presented in table 3, indicating the extent to which public-private cooperation takes place for each category. This indication is based on a three level scale, namely: low – medium – high. Low indicates that public-private sector cybersecurity cooperation

is minimal. Moderate means that cooperation takes place sporadically, while high indicates that cooperation takes place most of the time.

Function	Category	Public-Private Cooperation
Identify	Asset Management	Low
	Business Environment	Low
	Governance	Low
	Risk Assessment	Low
	Risk Management Strategy	Low
Protect	Awareness and Training	Low to moderate
	Information Protection Processes and Procedures	Low
	Maintenance	Low
Detect	Anomalies and Events	Low
	Security Continuous Monitoring	Low
Respond	Communications	Moderate to high
	Analysis	Moderate
	Improvements	Moderate
Recover	Communications	Moderate

Table 3: Level of public-private cooperation per category

As can be seen in table 3, the analysis of this research indicates that a low level of cooperation takes place in most of the categories. This is especially true in the Identify, Protect and Detect functions. What is interesting however, is that the Respond and Recover functions indicate a moderate level of cooperation. This could be due to the need to work together in managing the impact of a cybersecurity incident that has occurred. Nonetheless, it is clear that public-private cybersecurity cooperation in managing cybersecurity risks is lacking.

4.5. Complexities and Challenges

There are several reasons why this may be the case. Based on the interviews, several challenges emerged that hinder cooperation. These challenges may explain the reason why most of the adjusted NIST Framework categories indicate a low level of cooperation between public and private actors.

Port-ISAC and FERM Limitations

The port-ISAC should be the 'holy grail' of cybersecurity cooperation in the port (Respondent 4, Public/Private sector). However, only a select group of organizations are allowed to take part in this ISAC. These organizations are all involved in vital processes of the port and undergo a strict admission procedure to be able to join it. As a result, the port-ISAC has a limited effect on cybersecurity cooperation in the port as a whole (Respondent 4, Public/Private sector). Since most of the organizations in the port community cannot take part in the port-ISAC, they do not enjoy the benefits of being in contact with public actors such as the NCSC.

FERM should therefore serve as a central platform in which all organizations can receive cyber threats and help one another in tackling problems. It is currently the only platform that enables the entire port community to cooperate in cybersecurity. Unlike the port-ISAC, it is an instrument to support non-vital organizations in becoming digitally secure. However, it is still at an early stage (Respondent 1, Private sector). Currently, relevant stakeholders are defining what FERM should be. Before, the aim of FERM was to create cybersecurity awareness, but now it also wants to ensure cyber resiliency in the port by testing and altering cybersecurity technology when needed. Furthermore, it's aim is to create a collective of organizations that can apply pressure on cybersecurity suppliers to reduce their costs. By the end of 2020, the Port Authority hopes to conclude whether or not this is feasible and if organizations are willing to cooperate in this matter (Respondent 4, Public/Private sector). This indicates that cybersecurity cooperation in the port is a relatively new phenomena. Even though FERM has taken flight since the APM/Maersk hack of 2017, questions remain regarding its structure and goal.

Financial Challenges

Furthermore, a big question remains who will finance initiatives like FERM. It is important that all organizations in the port can join it. Smaller companies in particular are more vulnerable to cybersecurity risks, which is why their participation is of importance (Respondent 6, Private sector). If it is too expensive for smaller organizations, they will be less inclined to join.

However, no private organization in the port is willing to make a major contribution to finance projects like these. Large investments have to be made that most organizations cannot afford. Therefore, some respondents argue that the Port Authority or the government has to play a bigger role. If the government classifies the port as critical infrastructure, they have to facilitate cybersecurity information exchange between all relevant stakeholders by funding projects and initiatives (Respondent 2, Private sector). Nevertheless, the public sector is not responsible for the cybersecurity of private organizations. Companies are often profit driven, and in order to keep being profitable they have to ensure their own business operations are secure. They have to invest in their own physical and digital security (Respondent 4, Public/Private sector). Some public and private actors therefore disagree regarding the financing of cybersecurity in the port. As mentioned, Linder (1999) argues that the hallmark of partnerships has been cooperation that spreads financial risks between the public and private sectors (Linder, 1999, pg.36). Thus, if both sectors cannot come to terms with regard to the financing of cybersecurity collaborative initiatives, cooperation will be hindered.

Limited Role of the Public Sector

The role of the public sector in port cybersecurity is therefore limited. The government encourages initiatives like FERM to be established. However, they will not be the ones to take the initiative. Ultimately, it is up to industrial sectors like the port to take action. The government will never interfere with cybersecurity policies of individual organizations. The NCSC gives advice and acts as a facilitator, but this is mostly geared towards vital organizations. They do not require organizations to follow certain cybersecurity policies or actively cooperate with the public sector (Respondent 6, Private sector).

This may be because the port consists of many commercial organizations, each with their own responsibilities and interests. Cooperation only takes place if it is in the interest of the organizations (Respondent 2, Private sector). Furthermore, the Dutch culture is one in which a lot of freedom exists, allowing organizations to take their own measures. The government regulates and gives advice, but also allows people to take matters into their own hands. This is exactly what is happening in the port. In a country like the Netherlands it is not feasible to have very extensive cybersecurity legislation and a lot of public sector involvement. Therefore, all the public sector can do is facilitate and give cybersecurity advice (Respondent 6, Private sector).

Low Willingness by Private Sector

This is especially true for large private organizations. As was mentioned, large organizations often base their local cybersecurity policy on global IT strategy. The bigger the company, the less inclined they are to cooperate with other actors in managing cybersecurity risks. These organizations are more inward looking instead of focusing on working together as one community. They are more concerned with safeguarding their market position and communicating internally within the entity. As a result, not every organization is too keen to stimulate cooperation with other actors. Some therefore do not feel the need to work together with the public sector (Respondent 3, Private sector).

Furthermore, cooperation raises privacy concerns. Private organizations are concerned that information sharing with the public sector raises the chance of visits from governmental inspectors. The private sector is therefore more inclined to work together with private organizations if help is needed. Any type of cybersecurity cooperation may also put the competitiveness of an organization at risk. Opening up information systems to others, or letting others know that there has been a major incident, is therefore unfavorable.

Disputed Responsibility

It can therefore be seen that tension exists between public and private actors with regard to cybersecurity cooperation. Organizations may belief that the public sector should not have the authority to deal with cybersecurity in private networks. On the other hand, private organizations may invest less in cybersecurity than what is socially optimal. This disjuncture is in line with what Carr (2016) argues, in that partnerships are often characterized by disputed responsibility instead of shared responsibility (Carr, 2016, pg.58).

4.6. Answering the Research Question

Taking all this into consideration, the research question that was formulated in the beginning of this research can be addressed. The research question is as follows:

To what extent do public and private actors in the Port of Rotterdam cooperate in managing cybersecurity risks?

By using policy documents and conducting interviews, the extent to which cooperation takes place has been analyzed. Five functions and selected categories of the NIST Framework have been applied to public and private organizations active in the Port of Rotterdam. These aspects have been analyzed in order to provide an in-depth understanding of this research question.

It is clear that there are several public-private cooperation initiatives in the Port of Rotterdam. Both FERM and the port-ISAC are the most important platforms for both sectors to come together and share relevant cybersecurity information with one another. However, only a select group of organization can take part in the port-ISAC. It therefore seems that its influence on public-private cooperation is limited for the port as a whole. As a result, FERM has been a leading platform in bringing together all organizations in the port when it comes to cybersecurity risk management. It has the potential of becoming an essential tool in stimulating public-private cooperation. However, FERM is a relatively new platform and not all organizations are actively involved. The Port

Authority therefore stresses that steps have to be taken to not just create cybersecurity awareness, but also resiliency. This can only be done if all organizations in the port-community are involved.

When looking closer at how organizations cooperate with one another, it is clear that cooperation is very limited. Identifying cybersecurity efforts and strategies, minimizing the impact as well as detecting cybersecurity incidents is mostly done on an individual basis. However, once a cybersecurity incident has taken place, cooperation is moderate in respond and recovery efforts. This may be due to the interconnectedness of the port-community. Major IT disruptions can have spill-over effects, urging organizations to work together in mitigating cybersecurity incidents. It is therefore of no surprise that the Port Authority forces ISPS compliant organizations to report major IT disruptions to the public sector.

Private organizations seem hesitant to work together with the public sector in managing cybersecurity risks. Larger organizations have their own IT policies and strategies in place, based on global policies. On top of this, most organizations have their own IT infrastructure. This results in an inward looking culture in which cooperation with others is undesirable. As a result, cooperation will only take place if cybersecurity incidents are deemed serious enough. Any information sharing with the public sector is therefore only done on a mandatory basis.

Public organizations on the other hand seem to be limited by governmental legislation such as the Wbni. The NCSC can only share relevant information with vital organizations, such as the Port Authority. The Port Authority is not allowed to share this information with private organizations. Other public organizations such as the DTC and NDN can also share information with the private sector, however, this is minimal. As a result, public sector actors only gives advice and act as facilitators instead of actively cooperating with private organizations.

It can therefore be seen that public-private cybersecurity cooperation is a relatively new concept in the Port of Rotterdam. The APM/Maersk hack of 2017 served as a turning point, after which cybersecurity became a top priority in the port and initiatives such as FERM took flight. It is therefore of no surprise that questions regarding responsibility and financing are currently prevalent and hamper cooperation. On top of this, current Dutch cybersecurity legislation may

have to be revised in order to make it easier for the public sector to cooperate with private organizations. If this is done, smaller and non-vital organizations can also enjoy the benefits of direct information sharing with the public sector. This can result in the port as a whole to be involved in public-private cybersecurity cooperation.

5. Conclusion

5.1. Reflection

As the Port of Rotterdam is the largest port in Europe, it is of no surprise that properly functioning public-private cybersecurity initiatives are important. Due to digitalization and the interconnectedness of organizations, a cybersecurity incident can have disastrous spill-over effects. The APM/Maersk hack of 2017 was a clear example of this. Cybersecurity should therefore be a collaborative effort between the government and private organizations active in the port. However, the issues that hamper cooperation as discussed in existing literature are also evident in this research. The analysis based on the NIST Framework categories has shown that conflict of interest, lack of trust, financial shortcomings, governmental law as well as responsibility disputes hinder public-private cooperation. Nevertheless, existing research in this area also indicates that there are means to mitigate these issues. If knowledge sharing is stimulated and trust is built between both sectors, public-private cooperation can be effective. It is evident that FERM is the only platform in the port to make this happen.

Furthermore, existing literature warns that even though government and business may appear to use relatively uniform cybersecurity standards, this is not always the case. The analysis based on the NIST Framework has shown that this is also the case in the Port of Rotterdam. While Dutch government and port policy reports promote public-private cybersecurity cooperation, the interview analysis indicates otherwise. Private organizations are less optimistic about public-private cybersecurity cooperation than what the public sector advocates. Steps therefore have to be taken in order to stimulate both sectors to work together in managing cybersecurity risks.

5.2. Limitations

Nevertheless, using the NIST Framework may not be the ideal way to conduct this research. This is because the original NIST Framework is aimed at analyzing cybersecurity risk management of individual organizations. In this research, 14 out of 23 categories were analyzed in order to be able

to understand cooperative efforts between the public and private sector. The remaining 9 categories proved to be unfeasible in studying the research question. However, only using a limited number of categories may undermine what the original NIST Framework aims to achieve.

Furthermore, the selection of interviewees proved to be another limitation. Due to time constraints, only a limited amount of individuals could be interviewed. More interviews would have increased the reliability of this research. Moreover, no interviews could be held with individuals from small organizations active in the port. The port consists of numerous large and small organizations. Including small organizations in this research would have increased the validity of the analysis for the port as a whole. Large and small organizations may differ in opinions with regard to the interview questions, which could have resulted in interesting findings. Even though not a major limitation, secrecy sometimes proved to be a challenge in conducting this research. Some interviewees were more reluctant to share cybersecurity information than others, limiting the in-depthness of their answers.

The availability of policy documents and reports proved to be another limitation. This was especially true for documents and reports of the Port of Rotterdam. Documents related to cybersecurity, and in particular cooperation initiatives such as FERM and the port-ISAC, were very scarce. This stressed the importance of conducting interviews.

5.3. Recommendations

The conclusions of this research allow for several recommendations to improve public-private cooperation in the Port of Rotterdam to manage cybersecurity risks. Involving smaller organizations in cooperation efforts with the public sector is an important first step. As of now, it seems as if the public sector only focusses on vital organizations. The port-ISAC only contains a limited amount of large organizations and the NCSC is bound by legislation. Since FERM is a platform that aims at involving all organizations active in the port, this can be a platform to do so. If public actors such as the NCSC take a more active role in FERM, public-private cooperation can be stimulated. Furthermore, enhancing voluntary information sharing and tackling privacy concerns is key in cybersecurity cooperation. As mentioned, a higher level of trust will result in

organizations to voluntarily report smaller cybersecurity incidents as well without the mandatory reporting standards. The public sector should therefore increase its effort in building relationships build on trust and make sure that the privacy of private organizations is guaranteed. Lastly, if cooperation is not desirable, providing subsidy may be a good alternative to manage cybersecurity risks. Smaller organizations do not have the financial means to comply to expensive cybersecurity standards. If the public sector provides subsidy, this will increase cybersecurity in the port as a whole. The chance of weak spots and spill-over effects will therefore be minimized.

5.4. Future Research

Public-private cybersecurity cooperation in the Netherlands is a subject that has not received a lot of attention in existing research. This is especially true for the Dutch port industry. Hence, there is still room for further research in this area. To improve public-private cooperation in managing cybersecurity risks, several areas of future research are recommended.

First of all, examining how smaller organizations in the port perceive cybersecurity cooperation to take place would be interesting. This will give a more adequate representation of public-private cooperation, as a large amount of the port consists of relatively small organizations. They may perceive cybersecurity cooperation to take place in a different manner, as they often lack financial means to have adequate cybersecurity measures in place. This will also result in a larger amount of respondents, increasing the validity of this research. Furthermore, taking a closer look at financial considerations of public and private organizations may yield relevant findings. As of now, discrepancy exists between both sectors regarding financial responsibility. Certain cybersecurity standards that organizations have to adhere to are too expensive for smaller organizations. Looking at ways in which the government can provide cybersecurity subsidy and whether or not this is feasible may solve the current disjuncture. Closer examination of how other major maritime ports in the Netherlands stimulate public-private cybersecurity cooperation is also a research area to take into consideration. The Port of Amsterdam would be a good candidate. This should result in similarities and differences in cybersecurity approaches between ports to be established, giving room for learning. Lastly, doing research into current Dutch cybersecurity legislation and how this hinders cooperation is beneficial for this area of study. As of now, legislation seems to be

hampering the public sector in cooperating with private organizations. Revising this may result in closer cooperation in managing cybersecurity risks.

References

ACS (2016). Cybersecurity Threats Challenges Opportunities. Retrieved from: file:///Users/douwebartstra/Downloads/ACS_Cybersecurity_Guide.pdf

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance-Issues and Practice, 40(1), 131-158.

Bossong, R., & Wagner, B. (2017). A typology of cybersecurity and public-private partnerships in the context of the EU. Crime, Law and Social Change, 67(3), 265-288.

Burkholder, G. J., Cox, K. A., Crawford, L. M., & Hitchcock, J. (Eds). (2019). Research Design and Methods: An Applied Guide for the Scholar-Practitioner., 1 edition. Thousand Oaks: SAGE Publications

Burstein, A. J. (2008). Amending the ECPA to enable a culture of cybersecurity research. Harv. JL & Tech., 22, 167.

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

Cavelty, M. D. (2007). Cyber-security and threat politics: US efforts to secure the information age. Routledge.

Cavelty, M. D. (2007). Critical information infrastructure: vulnerabilities, threats and responses. In Disarmament Forum (Vol. 3, pp. 15-22).

Charmaz, K., & Belgrave, L. L. (2007). Grounded theory. The Blackwell encyclopedia of sociology.

Christensen, K. K., & Petersen, K. L. (2017). Public–private partnerships on cyber security: a practice of loyalty. International Affairs, 93(6), 1435-1452.

Ciolan, I. M. (2014). Defining cybersecurity as the security issue of the twenty first century. A constructivist approach. Revista de Administratie Publica si Politici Sociale, 12(1), 40.

CISA (2019). A Guide to Critical Infrastructure Security and Resilience. Retrieved from: https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf

Deltalinqs (2018). FERM Port Cyber Café: agenda 2019. Retrieved from: https://www.deltalinqs.nl/nieuwsberichten/2018/openbaar/ferm-port-cyber-cafe-agenda-2019

Dewar, R. S. (2014). The "triptych of cyber security": A classifi cation of active cyber defence. In 2014 6th International Conference On Cyber Conflict (CyCon 2014) (pp. 7-21). IEEE.

Dooms, M., van der Lugt, L., & De Langen, P. W. (2013). International strategies of port authorities: The case of the Port of Rotterdam Authority. Research in Transportation Business & Management, 8, 148-157.

DTC (2018). Digital Trust Centre. Retrieved from: https://www.mkb.nl/sites/default/files/factsheet_digital_trust_centre.pdf

DTC (2018). Handreikingen voor het starten van een cybersecurity samenwerkingsverband. Retrieved from: https://www.digitaltrustcenter.nl/handreikingen-voor-het-starten-van-een-cybersecurity-samenwerkingsverband

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

Eichensehr, K. E. (2016). Public-private cybersecurity. Tex. L. Rev., 95, 467.

ENISA (2018). ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends. Retrieved from: file:///Users/douwebartstra/Downloads/WP2018%20O.1.2.1%20-%20ENISA%20Threat%20Landscape%202018.pdf

FERM (2016). Column René de Vries. Retrieved from: https://ferm-rotterdam.nl/nl/column/column-rene-de-vries

Franklin, C., Ballan, M., & Thyer, B. (2001). Reliability and validity in qualitative research. The handbook of social work research methods, 2, 273-292.

Givens, A. D., & Busch, N. E. (2013). Realizing the promise of public-private partnerships in US critical infrastructure protection. International Journal of Critical Infrastructure Protection, 6(1), 39-50.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2(1), 13-20.

Havenbedrijf Rotterdam (2018). Beleidsdocument Haven Cybermeldpunt. Retrieved from: https://www.portofrotterdam.com/sites/default/files/beleidsdocument_haven_cybermeldpunt.pdf?token=vGqaPtgo

Havenbedrijf Rottedam (2019). Havenbedrijf Rotterdam Jaarverslag 2019. Retrieved from: file:///Users/douwebartstra/Downloads/Jaarverslag-2019-Havenbedrijf-Rotterdam.pdf

Heale, R., & Forbes, D. (2013). Understanding triangulation in research. Evidence-Based Nursing, 16(4), 98-98.

Heuvel, E. V. D., & Baltink, G. K. (2014). Coordination and cooperation in cyber network defense: the dutch efforts to prevent and respond. Best Practices in Computer Network Defense: Incident Detection and Response, 35, 121.

Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. Computer Law & Security Review, 29(3), 236-245.

Hodge, G. A., & Greve, C. (2007). Public–private partnerships: an international performance review. Public administration review, 67(3), 545-558.

IFV (2018). Lessen uit crises en mini-crises 2017. Retrieved from: https://www.ifv.nl/kennisplein/Documents/2018-IFV-Lessen-uit-crises-en-mini-crises-2017.pdf

JenV (2018). Besluit van 30 oktober 2018, houdende regels ter uitvoering van de Wet beveiliging netwerken informatiesystemen (Besluit beveiliging netwerk- en informatiesystemen). Retrieved from: file:///Users/douwebartstra/Downloads/stb-2018-388.pdf

Johnson, K. N. (2015). Managing cyber risks. Ga. L. Rev., 50, 547.

Linder, S. H. (1999). Coming to terms with the public-private partnership: A grammar of multiple meanings. American behavioral scientist, 43(1), 35-51.

Mandritsa, I. V., Tebueva, F. B., Peleshenko, V. I., Petrenko, V. I., Mandritsa, O. V., Solovieva, I. V., ... & Mecella, M. (2018). Defining a cybersecurity strategy of an organization: criteria, objectives and functions. In Integrating Research Agendas and Devising Joint Challenges (pp. 199-205).

Manley, M. (2015). Cyberspace's dynamic duo: Forging a cybersecurity public-private partnership. Journal of Strategic Security, 8(3), 85-98.

Moteff, J., & Parfomak, P. (2004, October). Critical infrastructure and key assets: definition and identification. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.

NCSC (2018). Nationaal Detectie Netwerk: Nederland samen digitaal veilig. Retrieved from: file:///Users/douwebartstra/Downloads/Nationaal_Detectie_Netwerk_DEF%20(3).pdf

NCSC (2018). Nederlandse Cybersecurity Agenda: Nederland digitaal veilig. Retrieved from: file:///Users/douwebartstra/Downloads/CSAgenda_def_web_tcm31-322330.pdf

NCSC (2019). Operational Framework NCSC-NL. Retrieved from: file:///Users/douwebartstra/Downloads/190321_Operational_framework%20(2).pdf

NCSC (2018). Starting a regional collaboration Guide. Retrieved from: file:///Users/douwebartstra/Downloads/NCSC_Guide_Regional_Collaboration%20(2).pdf

NCSC (2018). Start een ketensamenwerking Handreiking. Retrieved from: file:///Users/douwebartstra/Downloads/Handreiking_start_een_ketensamenwerking%20(1).pdf

NCSC (2018). Starting an ISAC: Sectoral collaboration Guide. Retrieved from: file:///Users/douwebartstra/Downloads/ncsc_guide_isac%20(2).pdf

NCTV (2019). Cybersecuritybeeld Nederland. Retrieved from: file:///Users/douwebartstra/Downloads/CSBN2019_online.pdf

NIST (2018). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Nye, J. S. (2011). Nuclear lessons for cyber security?. Strategic Studies Quarterly, 5(4), 18-38.

Osei-Kyei, R., & Chan, A. P. (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), 1335-1346.

Petit, F. Critical Infrastructure Interdependency Analysis: Operationalising Resilience Strategies.

Petit, F., Verner, D., Brannegan, D., Buehring, W., Dickinson, D., Guziel, K., ... & Peerenboom, J. (2015). Analysis of critical infrastructure dependencies and interdependencies (No. ANL/GSS-15/4). Argonne National Lab.(ANL), Argonne, IL (United States).

PoR (2016). How the Port of Rotterdam is investing in cybersecurity. Retrieved from: https://www.portofrotterdam.com/en/news-and-press-releases/how-the-port-of-rotterdam-is-investing-in-cybersecurity

PoR (2018). Haven Cyber Meldpunt. Retrieved from: https://www.portofrotterdam.com/sites/default/files/policy-document-port-cyber-notification-desk.pdf?token=waAgc_VH

Portbase (2016). Portbase Service Selector. Retrieved from: https://www.portbase.com/wp-content/uploads/2016/12/43653_Service-Selector_Digitaal_GB.pdf

Rijksoverheid (2018). Digital Trust Center maakt veilig digitaal ondernemen makkelijker. Retrieved from: https://www.rijksoverheid.nl/onderwerpen/cybercrime-en-cybersecurity/nieuws/2018/06/08/digital-trust-center-maakt-veilig-digitaal-ondernemen-makkelijker

Schaeffer, P. V., & Loveridge, S. (2002). Toward an understanding of types of public-private cooperation. Public Performance & Management Review, 26(2), 169-189.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. Journal of Digital Forensics, Security and Law, 12(2), 53-74.

Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-risk management: technical and insurance controls for enterprise-level security. Information Systems Security, 11(4), 33-49.

Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. Tex. Int'l LJ, 50, 305.

Shore, M., Du, Y., & Zeadally, S. (2011). A public-private partnership model for national cybersecurity. Policy & Internet, 3(2), 1-23.

Stavridis, J., & Farkas, E. N. (2012). The 21st Century Force Multiplier: Public–Private Collaboration. The Washington Quarterly, 35(2), 7-20.

TNO (2017). Verkenning Cybersecurity Informatiedeling binnen de Topsectoren. Retrieved from: file:///Users/douwebartstra/Downloads/blg-808966.pdf

Van Ham, H., & Koppenjan, J. (2001). Building public-private partnerships: Assessing and managing risks in port development. Public management review, 3(4), 593-616.

Weihe, G., Højlund, S., Theresa Bouwhof Holljen, E., Helby Petersen, O., Vrangbæk, K., & Ladenburg, J. (2011). Strategic use of public-private cooperation in the Nordic region. Nordic Council of Ministers.

Appendix A – Interview Protocol

Identify

Asset Management

- How are cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) established?

Business Environment

- How does the business environment (organization's role in supply chain, organization's place in critical infrastructure etc.) influence cybersecurity roles and responsibilities?

Governance

- How is organizational cybersecurity policy established and communicated?

  Are there legal and regulatory requirements regarding cybersecurity in the Port?

Risk Assessment

- Is information regarding cybersecurity threats received from external sources?

Risk Management Strategy

- Is there a mutual/shared risk management strategy with other organizations in the Port?

  How is the organization's risk tolerance established?

Supply Chain Risk Management

- Are Suppliers and third-party partners routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations?

Protect

Awareness and Training

- Do the organization's personnel and partners get cybersecurity awareness education to increase cybersecurity awareness?
- Are there collaborative trainings with other organizations?

Information Protection Processes and Procedures

- Is the effectiveness of protection technologies shared between organizations?
- Are there response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) in place and managed?

Detect

Anomalies and Events

- Is there cooperation with other organizations to detect anomalous activity?

Security Continuous Monitoring

- Are the information systems and assets are monitored?

    Is there cooperation with other organizations regarding this matter?

    What kind of information exchange takes place?

Respond

Communications

- Are there established criteria to report incidents?
- Is there cooperation with other stakeholders during an incident?
- Does voluntary information sharing take place?

Analysis

- Is there cooperation with other organizations to conduct analysis of incidents?

Improvements

- Does your organization learn from others? Is there information exchange? Do existing strategies get updated following an incident?

Recover

Communications

- Are restoration activities coordinated with external parties? How is cooperation regarding this matter? Information exchange?

Appendix B – NIST Framework

Function	Category	Subcategory
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried
		ID.AM-2: Software platforms and applications within the organization are inventoried
		ID.AM-3: Organizational communication and data flows are mapped
		ID.AM-4: External information systems are catalogued
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this	**ID.BE-1:** The organization's role in the supply chain is identified and communicated

	information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
		ID.GV-4: Governance and risk management processes address cybersecurity risks
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented

		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources
		ID.RA-3: Threats, both internal and external, are identified and documented
		ID.RA-4: Potential business impacts and likelihoods are identified
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
		ID.RA-6: Risk responses are identified and prioritized
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders

	managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
		PR.AC-2: Physical access to assets is managed and protected
		PR.AC-3: Remote access is managed

		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained
		PR.AT-2: Privileged users understand their roles and responsibilities
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities

		PR.AT-4: Senior executives understand their roles and responsibilities
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected
		PR.DS-2: Data-in-transit is protected
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
		PR.DS-4: Adequate capacity to ensure availability is maintained
		PR.DS-5: Protections against data leaks are implemented
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity

		PR.DS-7: The development and testing environment(s) are separate from the production environment
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
		PR.IP-2: A System Development Life Cycle to manage systems is implemented
		PR.IP-3: Configuration change control processes are in place
		PR.IP-4: Backups of information are conducted, maintained, and tested
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met
		PR.IP-6: Data is destroyed according to policy

		PR.IP-7: Protection processes are improved
		PR.IP-8: Effectiveness of protection technologies is shared
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
		PR.IP-10: Response and recovery plans are tested
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
		PR.IP-12: A vulnerability management plan is developed and implemented
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
		PR.PT-2: Removable media is protected and its use restricted according to policy
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
		PR.PT-4: Communications and control networks are protected
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed
		DE.AE-2: Detected events are analyzed to understand attack targets and methods
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors

		DE.AE-4: Impact of events is determined
		DE.AE-5: Incident alert thresholds are established
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
		DE.CM-4: Malicious code is detected
		DE.CM-5: Unauthorized mobile code is detected
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events

		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
		DE.CM-8: Vulnerability scans are performed
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability
		DE.DP-2: Detection activities comply with all applicable requirements
		DE.DP-3: Detection processes are tested
		DE.DP-4: Event detection information is communicated
		DE.DP-5: Detection processes are continuously improved
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident

	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed
		RS.CO-2: Incidents are reported consistent with established criteria
		RS.CO-3: Information is shared consistent with response plans
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated
		RS.AN-2: The impact of the incident is understood
		RS.AN-3: Forensics are performed
		RS.AN-4: Incidents are categorized consistent with response plans

		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained
		RS.MI-2: Incidents are mitigated
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned
		RS.IM-2: Response strategies are updated
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned

		RC.IM-2: Recovery strategies are updated
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed
		RC.CO-2: Reputation is repaired after an incident
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams