MOT2910 MASTER THESIS

Towards an analytical model for collaboration to secure cyber space

---

Neeti Hattangadi

2/2/2015

MSc Management of Technology program
Faculty of Technology, Policy and Management
At The Delft University of Technology

Graduation committee

Chairman	Prof. Dr. Yao-Hua Tan	ICT Department
First supervisor	Prof. Dr. Ir. Jan van den Berg	ICT Department
Second supervisor	Dr. Martijn Groenleer	POLG Department
Company supervisor	Raymond Bierens MSc MC	Atos International

A heartfelt thank you to

my dear friends and family

for all their love and support ☺

If it wasn't for your questions

(When Are You Going To Finish?!)

this thesis would still have remained incomplete..

Acknowledgements

Like the age old African proverb ‘it takes a village to raise a child’, it is my pleasure to be able to express my gratitude to the metropolis – many wonderful people, who helped me in the past two years to assemble this report you see before you.

First and foremost, I would like to thank my amazing sister, Aditi; who patiently read and gave thoughtful & detailed critique for all 72++ versions of my report. Mom, you too deserve most of the credit for this thesis. Your loving support and undying faith has and will continue to help both your daughters overcome any challenges in this world. Thank you, Daddy for all those numerous sessions where we walked through a variety of sentences, word for word, in order to make my research understandable for normal people ;)

My brilliant friends also deserve some credit for bearing with me, during the (what some may call never ending) writing process. Thank you Mark, Claudia, Claudia, Shuzheng, Lulu, Nandyka, Maurice, Satish, Aditya, Akshay, Eef, Youy, and Eric!! It really meant a lot to me when each of you went through the dozens of drafts, giving me kind words of encouragement (and/or chocolate) when I needed it the most. A very special thank you to Muriel, Henk, Ingrid, Coen, Frank, Tiago, Kailas, Mark Patrick, Ronnie, Harry, Anniek and Joost. You all not only shared little nuggets of wisdom that helped wrap up this project, but also gave me a very warm welcome into the ABN family.

Additionally, many field experts have helped shape the empirical section of this thesis. Thank you Ed Ridderbeecx, Marco de Graaf and Rob Mellegers for not only participating, but also forwarding me to others to get even more valuable input for my thesis. I am equally grateful to Dennis de Geus, Kick Stoppelenburg, Ewald Beekman, Jeroen Bijl, Roy Jansen, Paul Ducheine, Jelle van Haaster, Shekhar Gainda, Richard Kok, Jacques Tuin and Abbas Shahim. Thank you for your precious time and patience; explaining the various definitions and methods that are used in practice, and giving me food for thought by discussing different topics within the field of information and cyber security. Each of these interviews further motivated me to join your noble endeavour in securing the vast domain of cyber space.

And lastly, I would like to thank my supervisors. Jan, Raymond and Martijn; without your reviews and suggestions from start to finish, I would never have been able to complete this final chapter of my Master program.

Executive summary

In recent years, information technology (IT) has grown from an enabling technology to an important technology we depend on in our everyday lives. For example, IT is required for the proper functioning of personal devices that store our personal information, but is also present in the on-board computers in pacemakers and systems controlling nuclear reactors. Next to the diversity in ways in which IT can be applied, interconnectivity of devices is also an important characteristic in the IT world. This is because interconnectivity between devices allows geographical distance to be immaterial for activities taking place in cyber space.

The extent to which we have incorporated IT into our society, is illustrated by events in which incidents damaging IT structures have led to serious consequences for individual, organisational or even international Internet users. Recent information technology (IT) incidents like the Heartbleed bug illustrate how having the same Transport Layer Security/Secure Sockets Layer (or TSL/SSL) protocol vulnerability can result in serious consequences for these previously mentioned Internet users. Similarly, if incidents such as Diginotar had become widespread, the use of eGovernment services would have been put to a stop. This would have been done in order to protect the public from hackers, who would have used this opportunity to obtain personal information. Thus, cyber security now extends beyond physical borders because of the important place IT holds in influencing today's society and the direct interdependence between different kinds of users and IT. The after effects of crimes and exploitations on the Internet harm individual users as well as government agencies, (non-) commercial industries and international institutions. Yet, because instances such as Stuxnet[1] have not led to high impact incidents, the importance of IT security may not be evident to many of us.

Although most incidents do not become widespread, protecting cyber space is still seen as a great challenge. This is mainly because the IT environment could be seen as a vital nervous system that has strong connections with the various IT components. Currently, there are several different types of approaches to ensure protection of cyber space. These can be categorized on an individual, organizational, industrial, national and international level in order to provide security. Examples of such approaches come from articles published by the media, but also from consultancy agencies who present this information in trend reports and security methods. Subsequently, the term "methods" used throughout this thesis is derived from these approaches in the form of international standards, best practices, and national security regulation in the form of strategies, industry guidelines, and company security models.

[1] Exploiting programmable logic controls (or PLCs) of an Iranian nuclear plant in order for it to be disabled.

While each of the different approaches and methods highlight the importance of proper protection against cyber threats, they focus on mitigating risks in the immediate environment of the respective stakeholder. Thus, each of these approaches only lends itself for proper protection of a single party, not cyber space in its entirety. Another limitation is that current methods originate from the field of information security, which is technology-driven and thus focuses on individual risks. This leads to inability of the resulting models to address the challenges of socio-economic aspects of cyber space. Our problem analysis thus shows that there is a gap between what society expects and what technology delivers. This is highlighted by the lack of an overarching framework that attempts to address mitigation of systemic risk extending beyond the individual stakeholder's area of interest. In order to overcome this gap, this thesis aims to give an outline of requirements for an analytical model that enables multi-actor cooperation to jointly secure cyber space.

To understand the complexity of the problem, the first step is to analyse which types of stakeholders are active in cyber space and how they secure themselves and their assets. This is analysed in Chapter 2. In chapter 3, desired properties are provided which will deliver an outline for a model to support multi-actor cooperation. This is done by identifying the actors and methods from literature and practice to support various security approaches. Interviewing practitioners in turn contributes to show which theories are still widely used and motivate method choices in Chapter 4. Ultimately through these various analyses, this research provides an outline of a model that enables multiple actors to collaborate and coordinate security within the various domains of cyberspace.

The result of our work is a collaboration model to bridge the gap, shown in detail in Chapter 5. It provides a new perspective of how various stakeholder groups could work within a network setting. Key features of this multi-actor cyber security collaboration model are:

- Identifying roles and responsibilities of various stakeholders in cyber space, varying from individual users to global players;
- Combinations of interacting with external actors in order to jointly resolve an incident or crisis.

The Diginotar case study in Chapter 6 was used to conduct thought experiments that validated our model's analytical perspective and provide key investigations for further research. Limitations of time and available sources meant that this thesis is just a starting point for analysing the possibilities of integrating the perspectives of various actors into one close entity. A complete analysis and integration will in future enable us to coordinate efforts in jointly securing our cyber space. Because our designed model briefly touches upon these complex subjects; further studies could look into initiatives within each level to find more details e.g. roles and responsibilities, as well as actions that could help collaboration and seek out the effectiveness of interaction within every level.

Keywords: analytical model, IT risk management, cyber space, information security, multiple stakeholder perspectives.

Table of contents

Executive summary 4

Chapter 1 – Introduction 8

1.1 Difficulties securing cyber space 9

1.2 Problem statement 14

1.3 Research approach 16

1.4 Report outline 17

Chapter 2 – Beyond information security: From a technology-centric to a multi-actor perspective 20

2.1 Past: Information security 21

2.2 Present and future: Cyber security 27

2.3 Answering (sub) research question 1 35

Chapter 3 – Mapping existing IT security measures and identifying requirements for cyber security 39

3.1 Information security standards and frameworks 40

3.2 Cyber security standards and frameworks 46

3.3 Answering (sub) research question 2 53

Chapter 4 – Experts' view on cyber security collaboration 59

4.1 Introduction and conduct of interviews 59

4.2 Expert's view on key issues 64

4.3 Answering (sub) research question 3 74

Chapter 5 – Designing an analytical model to improve cyber space collaboration 77

5.1 Introduction to design and internal analysis of proposed model 78

5.2 Applying design theories in our model 79

5.3 Internal validations of theoretical and practical issues 87

5.4 Answering (sub) research question 4 94

Chapter 6 – Model applicability 96

6.1 Model validation through case study analysis 96

6.2 Reflecting on the contribution of our research 98

Chapter 7 – Concluding remarks 100
7.1 Results of our study 100
7.2 Future research 102

References 104

Chapter 1 – Introduction

In recent years, the increase in the level of sophistication and types of applications using information technology (IT) has made it possible for different sectors to apply this technology in automating their business operations. A recent survey by PricewaterhouseCoopers shows that information security is considered to be a very important issue, as industry respondents detected 25% more attacks on average than the 2989 incidents recorded over the globe last year, leading up to an increase of 51% in the available budget – catapulting the average expenditure to be at an all-time high of 4.1 million dollars (LLC, PricewaterhouseCooper, 2013). As a comparison, the same change in percentage (25%) is also reported in terms of financial losses (for $10 million or more) by leading industries such as the oil & gas and the technology sector.

In literature, we notice a shift in the approach and methods applied in the recent branch of IT security known as cyber security. At the start of their developmental cycle, computational systems were considered to be a highly advanced field, where technology could only be used by a limited number of experts such as mathematicians and researchers (Hafner & Lyon, 1998). Due to this exclusivity, the first computer security issues around information distribution were resolved by only implementing technical changes in the IT architecture (von Solms, 2000). A major change occurred when the technology's installed base grew with the evolution of the personal computers (or PCs in the 1980s) and the Internet (1990s). It was then that IT became much more than an asset to a core supporting technology.

When the knowledge became available to other user groups through the commercialisation of PCs, different domains also implemented IT to support their crucial operations and processes. This first trend enabled IT interdependence, as many different institutions relied on the IT infrastructure, which was crucial for the proper functioning of core activities (Rinaldi, et al., 2001). IT adoption and application varied in contexts, e.g. from using IT in managing patient data in hospitals to automation in plants through supervisory control and data acquisition systems (SCADA). As communication between devices and users increased the exchange of (sensitive) data, interconnectivity of networks became another key issue. This interconnectivity gave birth to the concept of a global cyber space, where IT could be seen as the nervous system through which all sectors communicated (Clemente, 2013). Over time, security issues changed from worms to viruses and exploits, which meant that the general population could also be affected (such as the LoveBug). This transformation in issues also lead to more sophisticated, targeted attacks e.g. Stuxnet targeted attacks in Iran. These attacks were targeted on nuclear power plants, which are critical for the proper functioning of Iranian civilian life.

It is clear that currently information technology does not play a central role anymore, but it is rather the proper functioning of IT within the society that is being stressed. With a wide variety of stakeholders and users with different knowledge, tools and approaches available to tackle the problem of cyber security in the same ecosystem, the goal of this research is to contribute to the development of a model that incorporates the multiple perspectives into one framework to secure the cyber space. This chapter aims to briefly explain the research problem, by illustrating the development in the first subsection. From here we look at questions that have been identified, this to be able to analyse the problem from two different perspectives, theory and practice. This also allows a look at the steps taken to build and test our initial multi-actor collaboration model. This introductory chapter concludes with a short overview of the upcoming chapters for this report's outline.

1.1 Difficulties securing cyber space

The challenge in this evolving field of information technology security (IT security) has always been in defining (i) the boundaries and (ii) the scope of the field. These two topics are seen to have changed rapidly to from specific to general definitions, when field development coincided with mass-adoption of IT. This field is also seen as the general umbrella term for information and cyber security, as in literature there is no clear definition on whether cyber security exists. To further clarify the difference between both fields, the first era emerged to separate information security (or InfoSec) from computer security, by classifying information (or processed data) deemed to be critical for the operations of organisational and international groups as information security. Further information on this movement is explained in subsections 1.1.1 till 1.1.2. Cyber security aims to protect cyber space, which is at risk because interconnectivity, interdependence and globalisation take place, and thus allow for greater risks to originate in cyber space. These three trends are explained in detail in paragraphs 1.1.3 and 1.1.4.

1.1.1 Origin of Information Security

When research began in the 1960s, computation focused on technology. This technology was then seen as the central component. When security issues occurred within early networks, component-driven (e.g. hardware, software, material) security standards were created to address challenges such as sharing data. Systems were limited to specialised environments; such as ARPANET, which was created by the US department of defence in 1959 (Hafner & Lyon, 1998). The 1970s also brought a significant change, as this is when the diffusion of development occurred. This allowed commercial stakeholders to emerge as a different target group. On the other hand, companies like IBM focused purely on professional applications for multiple industries from airlines to hotel reservation systems. At the same time, firms such as Apple and Microsoft were founded to allow information technology to become widely available to a broader base of users (Campbell-Kelly & Garcia-Swartz, 2005).

As computer systems were adopted by this broad base of users, a variety of incremental and radical developments occurred. A prime example of such a development was that components and software were being constantly improved to accommodate new functionalities to entirely new industries, e.g. nanotechnology. Standards were developed to define a baseline of what is necessary to secure a certain technology. In time, these particular security models grew to include security trends from other fields. These fields also applied IT, but here IT was used in a different manner and included new developments such as cloud computing as well. Despite the broader base of users, information security continued to address challenges mainly from a technical perspective. Challenges of technological nature in security could easily be limited by placing certain boundaries on the scope of security (von Solms, 2000).

1.1.2 The evolution of Information Security

The following decade, the 1980s, led IT applications to slowly move from universities (Massachusetts Institute of Technology, Stanford) to consumer driven companies (IBM, Apple, Intel). The introduction of personal computers (PCs) and other devices enabled users to share information remotely through (wired) networks. This was also when security regarding sharing information grew increasingly important for its users, as a threat to security could breach personal privacy of users. It therefore touched upon the early laws of privacy (Naughton, 2010). In addition to the commercial industry, information technology foresaw its components being integrated into other sectors for automating processes such as reservation systems at airlines (Campbell-Kelly & Garcia-Swartz, 2005). Because of the broad spectrum of users, an ambiguous definition for information security emerged, varying from being a certified methodology to guarding key IT processes to only securing critical IT components (Anderson, 2003).

A wide variety in industry standards also emerged around this time for technical devices. Additionally, the massive adoption of IT applications led to the creation of protocols and interfaces on which multiple devices could communicate with each other. Research was conducted into what we identify as the first type of model for security, the standards. These standards were specialised for implementing a certain method in a domain with varying factors, such as the environment and application, to determine when its use was important (Heasuk, et al., 2010; Heasuk, et al., 2010). The second type of standards focused mainly on upholding a certain norm and seeing whether the internal model complied with certain requirements. A principal example is the energy sector, which has a couple of standard guidelines for its programmable logical control devices. These guidelines need to be regularly checked for proper functionality to ensure that the standby devices are available for service when demanded. From our literature analysis we observe that these systems operate in a predictive environment, lending themselves to be seen as *reactive* because they suggest additions and provide changes to measures *after* observing phenomena linked to upcoming trends.

The level of compliance with a given standard also varied greatly, as each model focuses on a different range of categories and applications within the field of business and computational technology. With the evolution in computer components, certain standards such as the BS7799 focused on mainly technical applications, while others such as Information Security Forum introduced its Standard of Good Practice to list practical issues such as risk management and classification (Höne & Eloff, 2002).

The following figure (1) summarises our own analysis from 1.1.1 and 1.1.2, by illustrating how the first cycle of IT security development only developed its own internal technical measures. The two arrows show the two perspectives addressed by managers with a technology and later on a business background, between the 1950s and 1980s. When the second cycle of information security development, which lasted until 2000, shows how information security shared similarities. Businesses in the second development model were much more closely related. This could for example be because working in same industry meant that the same rules and regulations applied for the security model, while business processes and management employed a different strategy. In turn, multinational companies irrespective of their industry and/or geographic area executed similar plans, because they were owned by the same parent company who had a given method to execute plans in a certain way or hired maintenance workers.

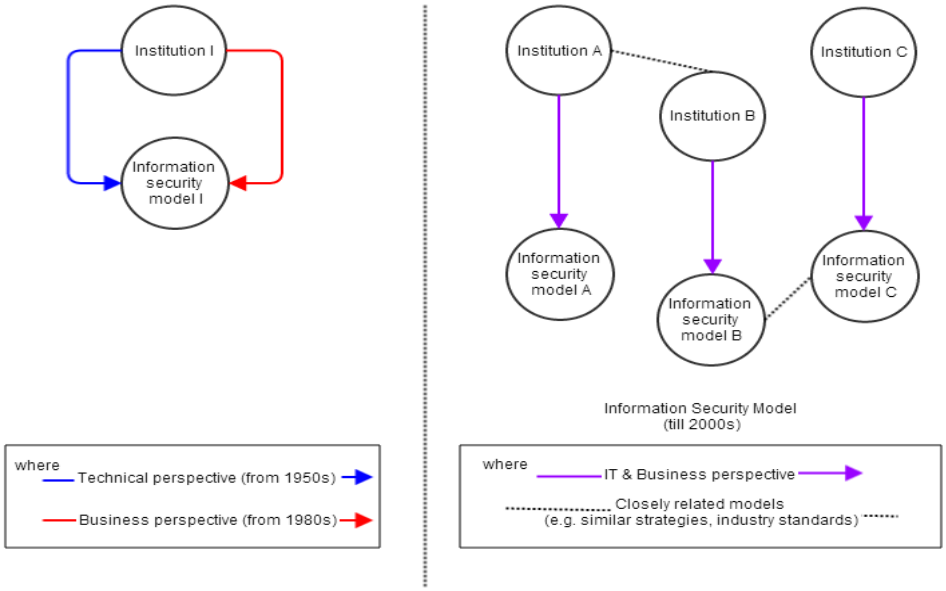

Figure 1 Information Security model development

1.1.3 Introduction of World Wide Web/Internet

Within the next decade, an exponential growth of users and applications occurred. This was due to interconnectivity and dependability onto the large and global network, which is now known as the Internet (using Transmission Control Protocol/Internet Protocol or TCP/IP; (Campbell-Kelly & Garcia-Swartz, 2005)). The reasons for IT infrastructure becoming pervasive are in threefold. Firstly, there was the rise of remote applications in the 1990s. This occurred together with the growth in the market share of PCs. Lastly, several industries invested in increasing connectivity and the technology's functionality. At the same time, users gained more autonomy on this virtual plane, denoted as cyberspace, through services offered on websites. These services ranged from entertainment, tooling, and applications or programs, to remote services.

Companies still found IT important to realize its goals, yet each had its different approach to do so. For example, in the medical industry, patient privacy needed to be protected. At the same time it was also necessary to keep in line with (inter)national regulations to operate within the health sector. This meant that while each firm insisted on having a unique strategy and vision for IT, limitations exist on the selection and implementation of the different standards and guidelines. These standard and guidelines are necessary to meet a firm's needs, so that the firm can create their own internal model. This is reflected in the emergence of many industry standards. For example, the Information Technology Infrastructure Library (ITIL) is growing, by including more volumes on IT service management. Also, the CobIT framework was introduced to deliver a renewed focus by adding more tools to improve IT-business processes (ISACA, 2008).

Destructive viruses also evolved with the use of IT technology, having critical consequences for multiple sectors. The LoveBug was the first general malware, malware being a term obtained from malicious software, to infect 2.5 million PCs. This infection came with an estimated 8.5 billion dollars in damages, in the year 2000 (Denning, 2003). Another example of a specialised and sophisticated threat was Stuxnet. This occurred in 2010, when many different experts collaborated to target and disable Iranian power plants. These power plants are a volatile part of the nation's critical infrastructure (Bencsáth, et al., 2012). Because these numerous incidents did not cause a high-impact incident, IT security was not yet seen as critical.

1.1.4 Towards a new era of cyber security

IT began playing a much bigger role being the backbone of each of the nation's critical infrastructure applications. This role was not only in commercial establishments, but also in various governments, that started to realize the importance of security. For commercial establishments, it was clear that security of information will always remain important. This was due to its direct link with the business' core activities and its earnings (von Solms, 2010). This is highlighted by the finding that a variety in service offerings from e-government to e-banking offered by a core infrastructure is the key to a worldwide rise of 10% in GDP over the coming decade. This is simply due to IT technology aiding the development of these services. Currently, these roles and responsibilities to jointly secure cyberspace also need to be debated openly. This is because of steps taken by institutions towards national and global protection, which are shifting between public and private sector. This causes a lack of definitions and boundaries specified for who protects what section of cyberspace, which in turn makes it very difficult to determine responsibility. Yet, the importance of defining these roles and responsibilities must not be taken lightly, as the consequences of decisions taken on this level could affect economical, technological, political, and social benefits derived from global networks (Klimberg, 2010).

Globalisation made it possible for public and private institutions to be based at one location, while possibly operating with several partners across the globe. This lead to the blurring of the line between what regulations need to be strictly followed and to what degree protection is offered by each supplier (Atos Nederland, 2013). In addition, each stakeholder group has different perception of incidents: citizens need to be managed differently from organisations in terms of threat awareness and response (Furnell, et al., 2007). In turn, governments also have a different approach, as IT goes beyond securing information or the ICT infrastructure. It also stretches to looking at subjects varying from crime to warfare, and accepting the fact that not everything can be secured. Yet, many subjects can be addressed by working together with public-private partners (Klimberg, 2010).

The United States of America serves as a prime example of the government working with partners, as its national government is the institution that authorises the federal authorities to secure its IT infrastructure. Their government was also one of the first to have their cyber strategy in place by 2003 (DHS, 2013). Europe started by 2007, which was the same year the Estonian cyber-attacks occurred. Therefore Europe published their own strategy, together with Slovakia, in 2008 as one of the first of this continent (Klimberg, 2010; MacDermott, 2013). Simultaneously, joint institutions also started taking information security more seriously due to their vulnerability for cyber espionage. This led to the foundation of multiple agencies focusing on joint research into important topics. These topics ranged from viable standards and designing governance to placing national security centres discussed by the European Networks and Information Security Association (ENISA, 2012; ENISA, 2013).

The new challenge that arose, was that all perspectives needed to be integrated in order to protect cyber space. This incidentally gave name to the field of cyber security, where protection and prevention conflicts to protect our cyber space take place. Figure 2 illustrates how integrating all important perspectives creates a major problem for a national (cyber security) committee, as the joint cyber security framework needs to be creatively put together in such a way that it includes all perspectives.

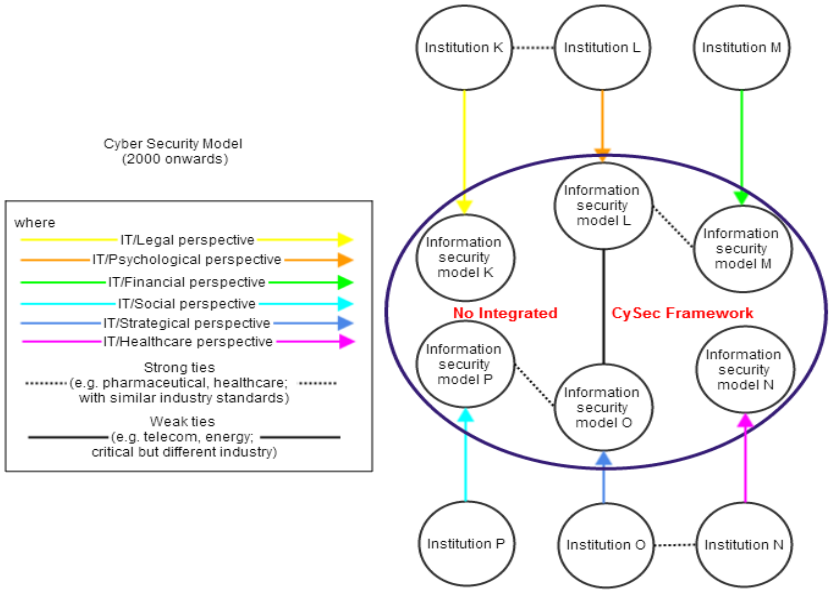

Figure 2 Cyber security model development

There is a main question for designing a model that encompasses the entire domain of cyber security, focusing on what our advice for analysing all the various perspectives needed for the protection of cyber space would be? This would include taking different individual, organisational, industrial, national and ultimately global focus into account. Next to this, it is also important to consider how we can be certain that these are all the risks that are present in cyber space. The following paragraph takes the first step in answering these questions, by first providing a research objective and sub-questions. These will aid our study, which aims to provide a multi-actor collaborative model of cyber security.

1.2 Problem statement

Our initial research in the first section points out our first problem. This is mainly that all actors have their own approach to analysing IT-related risks. In doing this, these actors are undertaking action for securing a part of cyber space. Due to this variation in methodologies, there is a large difference in cyber security undertaken by individuals and (inter)national organisations. While the individuals aim to use varying knowledge on tools and technology, organisations have access to more resources and need to protect far more assets in order to operate with regard to business strategy and environment. In turn, the problem grows more complex as similar groups of individuals in an organisation differ by the way they are governed by authorities.

On an industrial and national level there is also a difference in terms of rules and regulations that need to be followed in a district. Occasionally, these rules and regulations also vary regionally due to differences in constitution. These differences have a profound effect on IT, e.g. freedom of speech cannot be exercised everywhere in the world, and thus using the Internet to express opinions could be prosecuted. This inspires us to question whether, perhaps in the near future, there might also be one global security committee in place. This would be due to the global outbreak of similar security problems, and this committee could then oversee all cyber security activities. However, to provide initial integral cyber security, these various groups need to come together and compare strengths and shortcomings. This would lead to a better understanding of how each group's roles, responsibilities, activities and interaction should be developed.

By integrating these various views; we at least have a basic idea of how the different groups can collaborate on separate areas (as a network). This would also lead to the basic idea of how by coordinating these activities our problem to protect a large part of our cyber space can serve as an initial step to a future solution. Ideally, the implementation of this joint approach and clear roles and responsibilities to protect different areas of our cyber ecosystem, need the views to meet on two levels. Firstly all these views need to meet at one platform that is democratically determined. Secondly, this platform where these views meet should be overseen by a global committee. To achieve this, our objective in this research is to *design an analytical model to aid cooperation between multiple actors to secure cyber space.*

1.2.1 Research questions

In order to achieve our research goal of building a collaborative model, we pose the following research questions to help us proceed in our research. Firstly, in order to get familiar with general terms and definitions, we look at the historical development from the 1960s till today. This serves to identify:

1. *How do we define cyber security?*

Our hypothesis is that differences in definitions ensue from the development of computers to information to Information and Communications Technology (ICT) to cyber security. The question is whether these differences actually address and resolve the problems identified by the different generations. The next chapter looks into both questions. Firstly, it explains how development of various technical methods took place, which led to changes in stakeholder environment. Secondly, these changes enable the possibility for different actors to be part of the main driving force behind generally accepted security models in the time period. It thereby allows various approaches to the problem, which was identified by a given generation of IT security, to be proposed.

In order to identify what is important for creating a model; we must thus also have a good overview of the existing methods and how they fall short of our observations from the preceding chapter. These existing methods consist of frameworks, best practices, guidelines, standards and national security strategies. For better understanding of how these methods affect the way IT security is implemented – the following sub research question was posed for chapter 2:

2. *What can we learn from literature about cyber security collaboration?*

By comparing current methods gathered from the literature on this subject, we can identify general approaches towards information security taken by different groups of stakeholders. This is done in chapter 3. Using these best practices, we can then deduct whether a problem currently exists, because the gap we identify between current and ideal situation addresses all the problems from the aforementioned definitions of information- or cyber security, as noted in our comparison of chapter 2.

Having obtained a sound theoretical foundation for our research, it is important to consider whether practice also agrees with our problem definition. Thus we consult experts to gather their opinions on their key issues. Therefore, this leads to the following sub-research question:

3. *What do the experts see as key issues regarding cyber security collaboration?*

To answer this question, we note whether results from practice agree with definitions obtained in chapter 2 (answering sub-research question 1 and 2) and chapter 3 (answering sub research question 3 and 4). The recommendations obtained from practice could also provide different steps for cyber security. In this case, these steps are noted as empirical requirements for the design of our collaboration model.

Having conducted two very different types of analyses, we compare the requirements obtained from both literature and practice to note;

4. *How would we design an analytical model for cyber security collaboration? And what activities, roles and responsibilities are there between the different levels and/or cyber domains in our model?*

The fifth chapter tackles this research problem. It does this by comparing the (level) requirements acquired from the second and third chapter with advice given by experts in chapter 4. This advice is pertinent for tackling the important problems regarding cooperation in cyber space. This analysis then contributes to identification of the different types of groups. It also contributes to identify what activities need to be undertaken by each stakeholder to ensure that cyber security is established at a certain level. Additionally, our collaboration model also aims to provide guidelines on interaction, roles and responsibilities. These guidelines are based on the requirements and information, which was acquired from preceding historical, theoretical and empirical analyses.

To provide external validation, we conduct a thought experiment by using our initial model to theorise about results from analysing one high impact case study. We also used this experiment to look at the implications of our model, as well as look at additions to the current scientific body of knowledge. The following question is considered essential in developing a clear idea about the

scientific contribution of our model. This, mainly because such a model has not yet been proposed for this problem.

5. *What kind of common issues are found in a high impact cyber incident case study, and how can the results from using the model (not) cover the existing gap? Additionally, how can this case study analysis improve our model?*

These two questions are subsequently answered in the sixth chapter, where we conduct a case study analysis by reviewing the Diginotar case applicability for our analytical model. The analysis is to show how our model can help stimulate collaboration efforts for cyber security to combine different perspectives in one model. In turn, we reflect what shortcomings and limitations occurred in this research and how future research could help fill these gaps.

Finally, the seventh chapter summarizes the important findings of this research, which led to the development and evaluation of our multi-actor collaboration model. It also wraps up this research by providing steps for future research into some unexplored actors, who also play a key role in global collaboration on cyber security.

1.2.2 Scope

Because this paper is part of a university Master program, this research study is limited by:

1. *Detailed information on cyber security.*
   Due to the novelty of this field, many articles and a large part of research data largely focused developmental and methodological aspects of information security. Furthermore, due to the sensitive nature of this topic – the availability of in-depth, detailed articles and information on the design and use of frameworks, best practices, (inter)national cyber strategies was limited. The hazardous nature of the topic also limited the access to scientific data on the Scopus database and Google Scholar. Therefore, additional resources such as commercial (company, national, lobby groups') websites were consulted to note different perspectives in our (literature) research.
2. *The empirical data obtained from experts in the Netherlands.*
   This step helped combine several aspects of our overall analysis on individual, organisational and national cyber security measures. It should be taken into consideration, that limitations of the interviewee's response time and response topics meant that only certain sectors could be consulted. Additionally, these sectors only employed certain experts, who were consulted on their specialised in a given number of topics and methods.

1.3 Research approach

Due to the explorative nature of this research, the methodology is largely employed in favour of the information gathering phase. This is mainly because this research is roughly based on literature reviews and open interview data. This type of research was chosen, as it agrees with the theoretical nature of the research. This is because the aim is to look into how multiple actor perspectives could work together in securing cyber space. In addition, by exploring these various options, a holistic view of the problem can be created, which will feature different fields of cyber security. It will thus contribute to discovering each party's unique view on the problem.

Literature review

First, a historical analysis of background from information security is performed in Chapter 2. It hereby allows us to answer questions regarding development and available methods to implement information- and cyber security. Here we find the five important stakeholder groups to create a hybrid model for collaboration. The importance of the hybrid model lies in actors' varying preferences in hierarchy in a network. After various article reviews, we proceed to look at what each stakeholder does with regard to roles and activities. This is in order to identify the different approaches and variety of responsibilities that could be taken to secure cyber space.

Subsequently (in chapter 3), we narrow our search for appropriate methods in the field of risk management models applied by each stakeholder group. This last literature study into various methods also provides us with at least three key issues, such as an overview of activities, roles and/or responsibilities. These key issues take each stakeholder group, for our multi-actor collaboration model, into account and make this model feasible for the short term (5-year-plan).

Expert interviews

As the theoretical perspective covers a wide range of the background and methodologies, the *Delphi method* is employed to understand how practice views collaboration in cyber security. The Delphi approach involves consulting several experts (or oracles) to check whether the statements from literature are also the case in practice. This method is used in the first round to summarize our data. In the second round, case studies and questions are posed to the experts to evaluate the progress and to gain 7 important recommendations for collaboration from practice. These important recommendations focus on what measures can be taken in the short term to achieve security.

Model design and testing

These seven requirements (chapter 4) are also compared later on with the five stakeholder groups (chapter 2 and 3) to obtain 19 requirements from theory and practice. These requirements provide a set for the internal validation of our multi-actor collaboration model. The result is an analytical model that shows how the five cyber levels work in both hierarchical and network settings. For each of the five domains in which each stakeholder group operates, the model proposes key activities for each group, and their interactions with other levels. The model is tested in two ways. Firstly through internal analysis (chapter 5) and secondly through case study applicability to determine scientific contribution (chapter 6).

1.4 Report outline

This report has the following structure; after this introduction of the research the chapter *Beyond information security: from technology centric to a multi-actor perspective* states the important developments that took place. These developments transformed the field of information security into a much broader topic of cyber security. In turn, the most important stakeholders are also identified, thereby illustrating how perspectives to tackle security grew from a purely technology centred view to a multiple actors view. Each view tackles IT in their own manner. The following chapter *Mapping existing IT measures and identifying requirements for cyber security* is a literature analysis of applicable best practices for our key stakeholder groups. These best practices consist of standards, guidelines and frameworks. The analyses finally result in finding at least three criteria for each stakeholder, illustrating e.g. activities, interaction, roles and responsibilities encountered in cyber space.

As both perspectives are assumed to be quite different, the fourth chapter of this research *Experts view on cyber security collaboration* aims to use the Delphi methodology provide a solution. It provides this solution by bridging the gap between the various standards found in the literature review as well as standards derived from practice. The developments of these standards are evaluated by experts in order to get an indication of how collaboration is implemented in practice. Furthermore, approximately fifteen requirements can be derived from these developments. These fifteen requirements are built up by considering three field requirements for each of the five stakeholder groups. These field requirements and stakeholder groups are established in chapter 3 and chapter 2, respectively.

The fifth section *Designing an analytical model to improve cyber space collaboration* combines the findings from both theory and practice. It hereby provides a *synthesis* of results as well as providing an internal check for our model in section 5.4. Additionally it grants an answer to the main research question and argues how each stakeholder group and level works out in practice. After which, the model is validated and its results discussed in chapter 6, *Model applicability.* The final sections containing *Concluding remarks*, which are dedicated to reflect on the result of this study. Additionally it allows for discussion of their conclusions (chapter 7) for the future of integrated models for cyber security.

An overview of the thesis structure is provided on the next page.

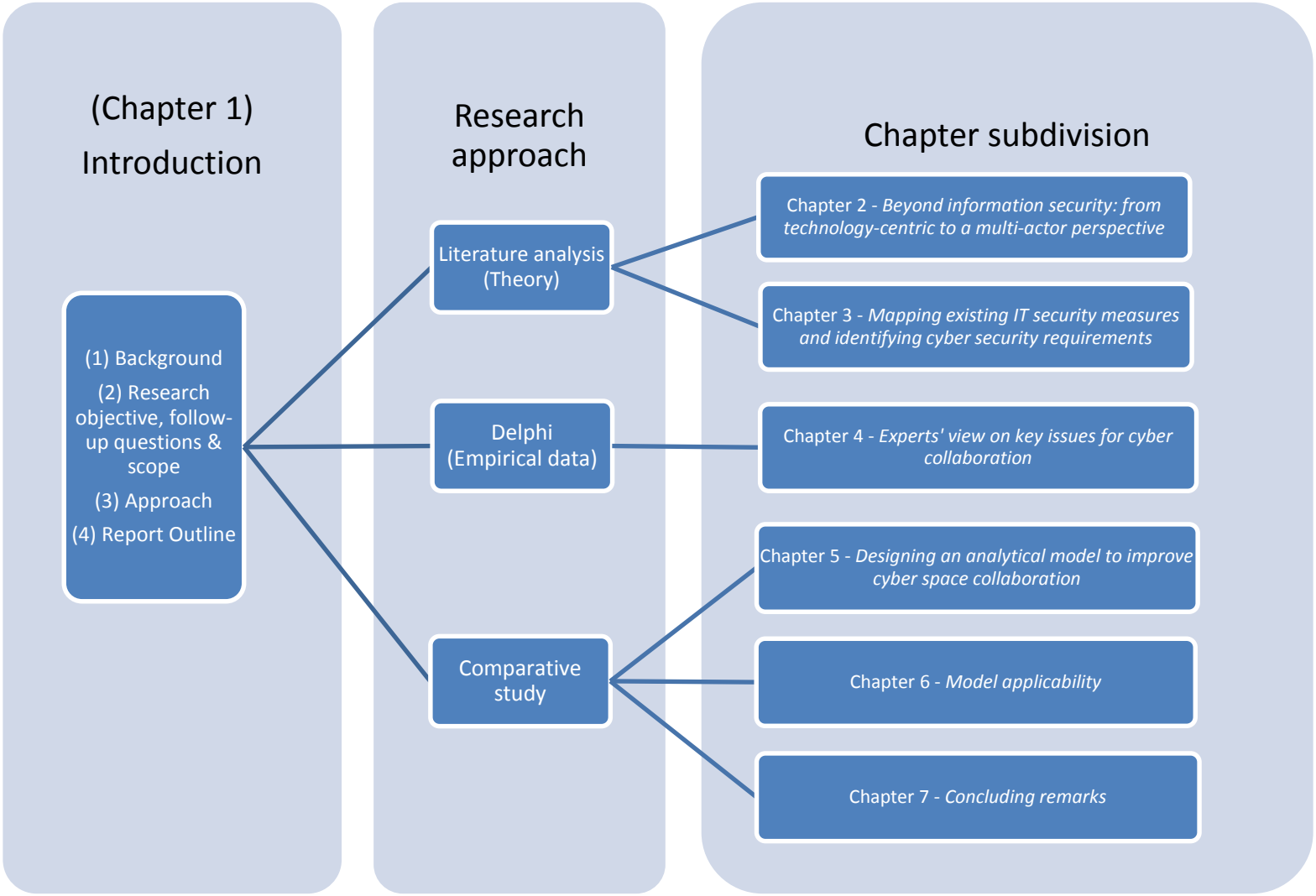

Figure 3 Thesis report structure

Chapter 2 – Beyond information security: From a technology-centric to a multi-actor perspective

Since the dawn of computing, security measures have largely contributed in protecting sensitive information. Due to the large contribution, topics and areas of interest have also been present in most security models of every decade (Bernroider, et al., 2013). The same principles are used in the first case of applying computer security to limit data access. This case occurred almost five decades ago, and benefits present-day's challenge in keeping personal information safe from identity thieves online. Multiple events have propelled a variety of applications of information technology (IT) being used ad hoc. Such applications involve appliances ranging from mini-cameras for internal operations in medicine to smart meters in our home. This shows that technology has certainly come a long way from a scientific research experiment. Yet, it also includes the responsibility to cover far more challenges than those that were predicted by previous analyses.

This chapter aims to provide insight into the historical development of the various generations of information security (InfoSec) into a new type of security of cyber space: cyber security (CySec). A comparison between current and past generations is made to point out current development. The problem with current development is that incremental changes are made to existing methods without addressing the dynamic new challenges. These new challenges are associated with interdependence, connectivity and globalisation of IT leading to the creation of cyber space. The change in context and application of security is given by identifying measures taken from the computer network´s early development to adoption. This occurred in the time period from 1960 till 1990, also referred to as the first era of information security (von Solms, 2010). When Internet was introduced in the 1990s, a new era emerged that required security in a larger context. Thus the goal of information security broadens to include protecting various stakeholders and assets from the technical and non-technical consequences of incidents in cyberspace (von Solms & van Niekerk, 2013). While newer methods and approaches by different actors protect parts our cyber ecosystem, no solution or model is provided that takes all these different views of security into account. To understand the various stakeholder's views and change in the perception of security, we look into roles, responsibilities and security methods (applications) used by groups active in cyber space.

To provide a background on IT security, the first step of our literature research explored journal articles between 1980 and 2014. This was done to get an impression of definitions regarding "information security" and "cyber security". By separately delving into both these terms on Scopus, key articles were found and summarized for a basic understanding. This initial collection was expanded by further examining the articles' historical references to identify development changes that shaped information security for networks. Whilst this initial collection expanded, a parallel search on Google Scholar was conducted to find similar papers if certain articles were unavailable. Additionally, the Elsevier journal database also provided a number of recommendations, which were utilised in identifying comparative methods and standards. These comparative methods and standards are also used in the next chapter. In addition, news and company articles together with existing security campaigns are used to complement our database approach with recent findings. The following sections of the report answer the research question: *How do we define cyber security?*

Sections 1.1 and 1.2 subsequently answer these research questions, by comparing similarities and differences in various IT security generations from the past and immediate future. These generations concert the development from computer systems, to information/communications technology, to cyber security. In turn, paragraph 1.3 summarizes the findings to show the discrepancy that occurs. This discrepancy occurs between existing generations and their methodologies (e.g. standards, best practices, guidelines) and their effectiveness to address incidents in the cyber ecosystem. By comparing how current development should ideally tackle these problems with our background, the chapter finishes by illustrating the dire need for a unified approach. This approach is vital for answering the second research question and to be able to bridge the gap between the present and desired situation.

2.1 Past: Information security

In this section, we look at what the literature sees as information security (InfoSec). InfoSec is an umbrella term in this research to denote the first generation of IT security. Historical events are consulted to show what shaped today's definitions and methods (e.g. standards and frameworks), while considering acceptable risks with regard to incidents.

When IT grew in scope towards the 1980s, the number of measures of existing or identified safety issues seemed to grow as well. This was mainly because each stakeholder introduced new topics and measures to adapt the technology to function in its dynamic and evolving environment. In the meantime, the computer became more widely adopted in a variety of industries. Each of these industries had an own network and structure to abide. In order to deal with security, separate groups of actors continued to develop their own methods varying:

- From frameworks (specific internal models with controls for a functional applicability, usually developed by commercial institutions),
- standards (comparable and measurable rules and regulations for [governmental] organisations),
- to voluntary peer reviews and reports from the community such as guidelines and best practices.

Each actor – whether it was institutional (non- and commercial organisations), industrial or national (e.g. government funded) – had their own approach to risk. This was because the consequences varied greatly from a replaceable service to a critical part of day-to-day operations (e.g. energy sector). This lead each type of stakeholder to develop their own measure that quickly exploded into a number of methods. These methods are still popular, and are being further developed by their followers.

The first paragraph explains that the need for security arose quite early on for technological counterparts, as data was shared by various systems. In turn, paragraph 1.1.2 denotes the definitions that played a key role in InfoSec development. This paragraph also briefly highlights the entailing industry applications. Finally, the third paragraph concludes with what led to a change in definition. This paragraph illustrates how the introduction and diffusion of the Internet lead to even greater environmental changes. This also explains the need to separate the former field from its successor: cyber security.

2.1.1 Origin of standard development

A well-known starting point looking into the history of internetworked computers lies arguably in the creation of ARPANET. This was an American Department of Defence project that enabled computers to exchange data packets within a network, in the early 1970s (Leiner, et al., 1997). The project was initially created to allow researchers from the Advanced Research Project Agency (or ARPA) to connect their computers. This allowed the researchers to form an internal network (or internet, with a small i) to share their resources (Hafner & Lyon, 1998).

First wave: Purely technical regulations

While ARPANET did play an important role in the development, further analysis points out that the existence of interconnected computer projects were well established preceding ARPANET. One of these interconnected computer projects emerged from the public sector. This was the Semi-Automatic Ground Environment (SAGE), which arose in 1962. SAGE was a pioneering project in creating command-and-control system for the United States Air Force (USAF) (Campbell-Kelly & Garcia-Swartz, 2005). Yet, development around interconnectivity for the private sector emerged even earlier: in the 1960s. Undoubtedly, this was because the private sector had foreseen a diffusion in the use of computer technology for applications other than engineering calculations.

An example in the commercial sector is the IBM-American Airlines SABER (short for: Semi-Automatic Business Environment Research) system. This system was based on the time-sharing principle, allowing airline personnel to process reservations in real-time from various terminals (Copeland & McKenney, 1988). This is just one of many examples that illustrate how independently private industries grew to accommodate the use of various personalised versions of existing technical computing utilities. This was in view of building their own internal (computing) infrastructure.

It is interesting to note that many basic functions which are well known and used today, e.g. remote and online services (cloud computing), also originated in four decades ago (Campbell-Kelly & Garcia-Swartz, 2005). Yet, due to diffused sources of development the focus varied from technical to managerial regulation of InfoSec. Both governance styles came together in the mid-1980s, and required further optimisation, when the new aforementioned technical innovations were implemented. This implementation was done after the popularity of personal computing, and thus commenced the dawn of the Internet (where the capital I states the use of the TCP/IP protocol).

The 1970s, on the other hand, saw an increase of computing automation. Mainframe operating systems were being applied in a variety of industries. These industries ranged from supervision control and data acquisition systems (SCADAs) in the energy industry to various accounting activities at firms e.g. banks and warehouse inventories (Chou & Chou, 2006; Shaw, 2006). Precautions for security were technical in nature, as the large mainframes carried out processing tasks. These tasks were regulated by a group of computational experts and/or outsourced to specialised IT companies such as IBM. Because of the issues regarding security could easily be resolved after adapting functionality, the knowledge about achieving a certain standardisation within the company was determined by the technical staff (von Solms, 2000).

Second wave: InfoSec is influenced by management

These barriers limiting users faded a decade later, when IT grew to accommodate the larger consumer group. This larger group had access to funds and an eagerness to learn, which resulted in more attempts in making new computing applications. The early 1980s showed a radical change with the first rise of personal computers (or PCs). Not only hobbyists and experts were being introduced to PCs, but also members of the general population were being targeted by Apple and Microsoft. This new development meant that even managers were exposed, leading to their greater understanding of different possibilities of using information systems. This could be done by identifying critical processes, thus introducing a managerial wave (von Solms, 2000).

Managers within the company turned to involve more players. At the same time, they were addressing future growth issues such as strategic planning and competitive advantage. This was done by promoting education and innovation of new information systems (IS). The aim of promoting was to find other functionalities than the ones provided by contractors (Brancheau & Wetherbe, 1987). IBM also saw major setbacks in proposing its industrial monopoly through the introduction of its own SNA standard. At the time, IBM was the only company for professional IT solutions. Meanwhile Canada, France, Britain and US-based Telenet developed their X.25 protocol as an alternative, which soon became more widely adopted. (Campbell-Kelly & Garcia-Swartz, 2005).

Simultaneously, the transmission control protocol (TCP)/internet protocol (IP) was developed by ARPANET. This allowed different IT network architectures to communicate with each other. The open systems interconnection (OCI) platform suggested a combined architectural framework. However, due to the framework's large network, the negotiations took longer than the design. Furthermore, deciding what changes had to take place were taken by the management. The management began to value IT more than an asset or tool, in this second stage of InfoSec development.

Third wave: Industrialising IT security

With the growing popularity of the PC, both the public and private sector saw new opportunities towards industrialisation. This gave rise to the third wave of information security (von Solms, 2000). The private sector flourished, because consumers without institutional access could access other users in other ways. For example, hobbyists would use a local bulletin board system that existed through national commercial networks (Campbell-Kelly & Garcia-Swartz, 2005). It was not until 1987, when the National Science Foundation (NSF) combined forces with IBM and MCI. These firms built a new privatised backbone on the existing ARPA Internet, creating the prototype of the current Internet. It was then called NSFNET, which overcame alternatives such as Gopher. Gopher had more than 2000 servers for the Internet. Another alternative was WAIS, which included an extra feature: a register to search within items. Literature states that NSFNET could have only overcome this for two reasons. Firstly, NSFNET was being backed by early adopters, e.g. researchers and politicians. Secondly, NSFNET had expertise from a decentralised management, which decreased bureaucracy about who could create webpages (Campbell-Kelly & Garcia-Swartz, 2005). In 1987, more users could connect due to the adoption of an underlying infrastructure proposed by Mr. Berners-Lee. This infrastructure was encouraged and funded by CERN. It was made accessible by the user-friendly browser Mosaic. This browser was utilised until 1993 when the World Wide Web emerged as the design of our Internet design.

At the start of the 1990s, the launch of email and other niche network services was only available to internets consisting of less than 100,000 users (Campbell-Kelly & Garcia-Swartz, 2005). However, the development of general methods had already expanded into other industries who were already familiar with IT (such as SCADA systems in the energy sector). These industries had also drawn up specific plans and standards to govern the risks involved in the familiar processes (Cai, et al., 2008). It was in this decade that a number of papers describe an increase in applications. This was particularly true for applications using internal networks, which allowed certain methods to cover trending topics regarding security of both technical and managerial risks (Armstrong & Armstrong, 2007; Brancheau & Wetherbe, 1987). Online banking was another example, illustrating the need for a whole new approach in the changing environment. This environment was changing due to the introduction of e-commerce, where shoppers could order online and pay later. Moreover, this development could be enhanced by banks by introducing the possibility of transactions, next to displaying information and services online. The former development was available since 1995, (Chou & Chou, 2006).

Concluding this historical section, we note from literature that the involvement of many (non-) technical stakeholders gave way to the exponential production of many (internal) approaches for InfoSec. A few examples of these approaches would be standards, frameworks, guidelines en best practices (von Solms, 2010)). This also meant that collective action needed to be taken in order to provide a good overview of viable standards that were actually tested and used by peers in the industry. These standards were then used to keep up with the quickly evolving I(C)T. Thus, in what is here seen as the last generations of information security; several actors came together. Coming together led to discussion of international best practices, various methodologies and identify gaps for information security in the new environment (ENISA, 2012). While negotiations took place, various analyses of the definitions show that even between industries it was ambiguous what cyber security was in general terms. Moreover, as to this date no clear definition has been found on what it means (Clemente, 2013; Halink, 2013; OECD, 2012; Hermans & Schreurs, 2013; Klimberg, 2010). These definitions are highlighted in the next paragraph, with regard to the development to show how InfoSec adapted itself over the years. Yet, this adaptation also caused confusion on the general definition.

2.1.2 Defining InfoSec and its applications

As mentioned before, the start of IT security focused on systems and data security. This was due to restrictions being limited to a couple of commercial companies and institutions in early projects (e.g. ARPANET, USAF, IBM). These were also the stakeholders involved with early developments. These early developments used to be mostly resolved through changes in the IT systems. The first reports regarding the technical insecurity was published in 1978, containing findings of the vulnerabilities in operating system security. It was a start to try to resolve what controls and mechanisms could help protect a computer system on various levels (Whitman & Mattford, 2011). This guides us to our first definition of InfoSec, which was mainly computer security founded on mainframe based problems, which could be resolved by additional facilities. Examples of such additional facilities are access control lists, user-ids and passwords (von Solms, 2000).

IT became more widespread and applicable towards the 1980s in commercial industries. Examples of these applications were reservation systems in aviation, banking for processing, and SCADA systems in the energy sector. Each sector grew to provide more data for input, but this also meant that industries were slowly growing in different directions. These different directions still aimed at similar possibilities regarding IT, such as Gopher, WAIS and ARPANET. In turn, the importance given to IT by management also grew. This was due to three reasons. Firstly, their awareness of what roles IT played in complementing core business processes rose. Secondly, how IT was utilised in different industries became clearer. This made it easier for the third reason to appear, which was the possibility of adapting IT to do more. IT had still not reached the stage where the top officials were actively involved in shaping plans, but it was important enough to look at risks to prevent errors and downtime.

This allowed us to define a second development in its definition, given by the United States stated as the general CIA concept. It defines InfoSec with tighter boundaries for protecting information and information systems. These boundaries protect InfoSec from unauthorized access, use, disclosure, disruption, modification, or destruction. This is done in order to provide

- *integrity* (guard against modification and destruction, keeping its authenticity intact),
- *confidentiality* (preserve restrictions on access and disclosure to protect privacy and proprietary information),
- and *availability* (ensure timely and reliable use of the information, (Office of the Law Revision Counsel, 2013)).

The third development circle, in the 1990s, occurred when the internet introduced the 'human' factor, as mentioned in multiple historical overviews (von Solms, 2000; Brancheau & Wetherbe, 1987). On the one hand, management and IT continued to evolve their methods of comparing their progress with regard to other players in the industry. This was done by introducing metrics, standards/best practices, and certification to gather and change data. On the other hand, consumers were just being introduced to new technology and getting used to applications that also addressed new fields and introduced new gaps of development. These gaps needed to be filled and secured for information security.

The industry addressed the first set of changes by providing a set of popular guidelines towards 1980s till the end of 1990s. These guidelines are adopted by a wide range of methods, of which the popular ones are:

- BS7799, originally the first code of practice. This grew to be the first internationally recognized certification method to measure information security aspects;
- CoBiT, which integrated managerial aspects of IT into a process-based approach. The aim was to thus govern InfoSec;
- ITIL, an IT service management library. This contains best practices and topics suited for IT practitioners;
- ISF Standard of Good Practice, which presents a guideline. The guideline is based on various best IT practices and aims to educate and improve certain controls and process aspects of InfoSec.

2.1.3 Need for change

While these development cycles identify the feedback and adaptation of IT to its dynamic environment, a major setback pertaining to drivers of the two perspective are identified in this era. First of these were the changes that were brought on by analysing from a technical and managerial perspective. Other views (e.g. human, sectorial, national, and international) were left to be unidentified. Secondly, some sectors caught on early on and started collaborating on endeavours, e.g. banking. This sector made changes to incorporate an institution's application of IT in the American Sarbanes-Oxley law towards 2003, while they also continued to develop their own internal network (Anderson, 2003). This problem was not addressed until the Internet connected all the tiny individual networks together, introducing cyberspace that strongly interacted with all actors connected to the network. This connection was regardless of the actual physical location of the actors. Assets were simpler before the Internet, due to the limited options of providing security, which was constrained in terms of physical availability.

In turn, the introduction of decentralised Internet meant that unexplored/uncovered areas were left to the different peers, which had to be sorted out individually by consumers. In turn, for institutions and industries, connecting to the virtual grid meant an equally large array of possibilities. These possibilities needed to be covered from every angle and/or user who was also on the same system. Due to the early stages of introduction, the discovery of what and how these risks could be mitigated were unfamiliar. This was because possibilities grew exponentially within the new phenomenon of the Internet, consisting of a great network built out of even more networks.

Within the next decade, IT grew to extend to more users. This was due to the arrival of mobile smart devices. This network grew to allocate even more users, by allowing consumers to educate themselves. In turn, incidents also grew in scale, affecting several more lives, including those that were not in the close proximity. An important example is the Stuxnet virus in 2010. This sophisticated virus showed that not only the Iranian nuclear plant could have been disabled, but also led to similar systems across the globe being infected (Falliere, et al., 2011). On the other hand, botnets could also be formed and could exploit unaware users if their device security was below standards or had been hacked. These implications show that the Internet has brought upon a radical change, which is still growing due to the dependency and large installed base of consumers and institutions. It also shows that other factors and stakeholders need to be brought together in order to address the new type of security issues in the interconnected world. The next paragraph explains why cyber security is the next step of information security.

2.2 Present and future: Cyber security

As highlighted in the previous paragraph, PCs and smart devices connected to the Internet show how securing information technology has surpassed predictions and developments. These predictions and developments were first identified by both technical experts and the management team. The first paragraph of cyber security (CySec) illustrates how the networked world changed the cyber landscape by introducing a variety of factors and stakeholders to the IT security problem. Additionally, the next paragraph provides an overview of cyber security definitions which address the new challenges, as well as introducing the sheer variety in methodologies used by practitioners in the stages following information security. The chapter finishes with a summary of how the future CySec is envisioned, highlighting what makes it different from what we previously defined as information security. It does this by introducing real-life case studies.

2.2.1 Challenges of a networked world

With growing use of IT in multiple industries, all using the same IT infrastructure, the dynamic environment enabled the growth of communications. The dynamic environment caused this growth by lowering costs, while being adaptable to mould and support at least 2.5 billion users and 12.5 billion connected objects and devices (Klimberg, 2010). The advantage of having such large distributed, decentralised computer networks was that its reach surpassed physical and industrial borders. Simultaneously, it still allowed dependability for content and proper functioning of the IT infrastructure for processes, thus introducing *global interdependency* (Clemente, 2013).

Within this new interconnected cyber landscape, IT has grown to take a main role of the underlying critical infrastructure. This is in contrast to its early applications as a complementary technical asset. The interconnected networks are additionally also seen to create a new problem. This problem is that interconnected networks make it difficult to denote connecting actors, with regard to their roles and responsibilities to IT security and protection. Interestingly, many authors within the CySec community argue that the IT infrastructure should be seen as the critical information infrastructure. This is because currently many applications that are crucial for society, use IT infrastructure for their communication (Armstrong & Armstrong, 2007).

This problem is also reflected in looking at our *cyber ecosystem*, denoted as the space where IT infrastructure creates an environment where there are no clear boundaries on who *owns* a certain section or part of the IT information exchange process. This transforms our society into a complex and ever-changing milieu; depicted in figure 4 (Atos Nederland, 2013). The complexity firstly occurs due to the growth of stakeholders, who each enable different activities in (partially) common areas. These stakeholders can also communicate through the infrastructure with anyone, irrespective of where they are (Klimberg, 2010). Also, due to the versatile actor dynamics, not everyone's roles, responsibilities and relationships are clearly defined. This means that the new challenge of IT security needs to address facilities that go beyond complete security of every single technical or organisational component. Yet, in order to truly manage (non) physical consequences, protection measures first must realise that not all risks can be covered (Hermans & Schreurs, 2013).

For an infrastructure that underlies an ever-growing collection of networks, the challenge remains to continue protection of IT integrity and availability as in the past. This serves also to build towards future resilience against (known, similar) attacks (Klimberg, 2010). In turn, further IT device and user development shows that from the moment that PCs were made mobile, the data that was created by these devices rose exponentially. Examples of making PCs mobile consist of the creation of laptops, mobiles, iPads and other (access to internet) devices to share and jointly create more data (from social media, Youtube, and so forth) (Hermans & Schreurs, 2013). Availability of IT services, cost efficiency, expanded education and skills are examples of this progression. This advance in technology is now not only limited to industries and professionals, but also available to low-end users who show interest in overcoming the knowledge gap (Klimberg, 2010). However, not all of these formerly mentioned parties are aware of the dangers of using (freely) distributed information. This is due to differences in (commercial) application, privacy, security and ethical use. Enabling more transparency on the (limitations of) (inter)actions needs be explored and promoted within the cyber community. This will aid the aim to create collective benefits as opposed to the current situation where each individual and organisation determines how and what to protect within their predetermined environment.

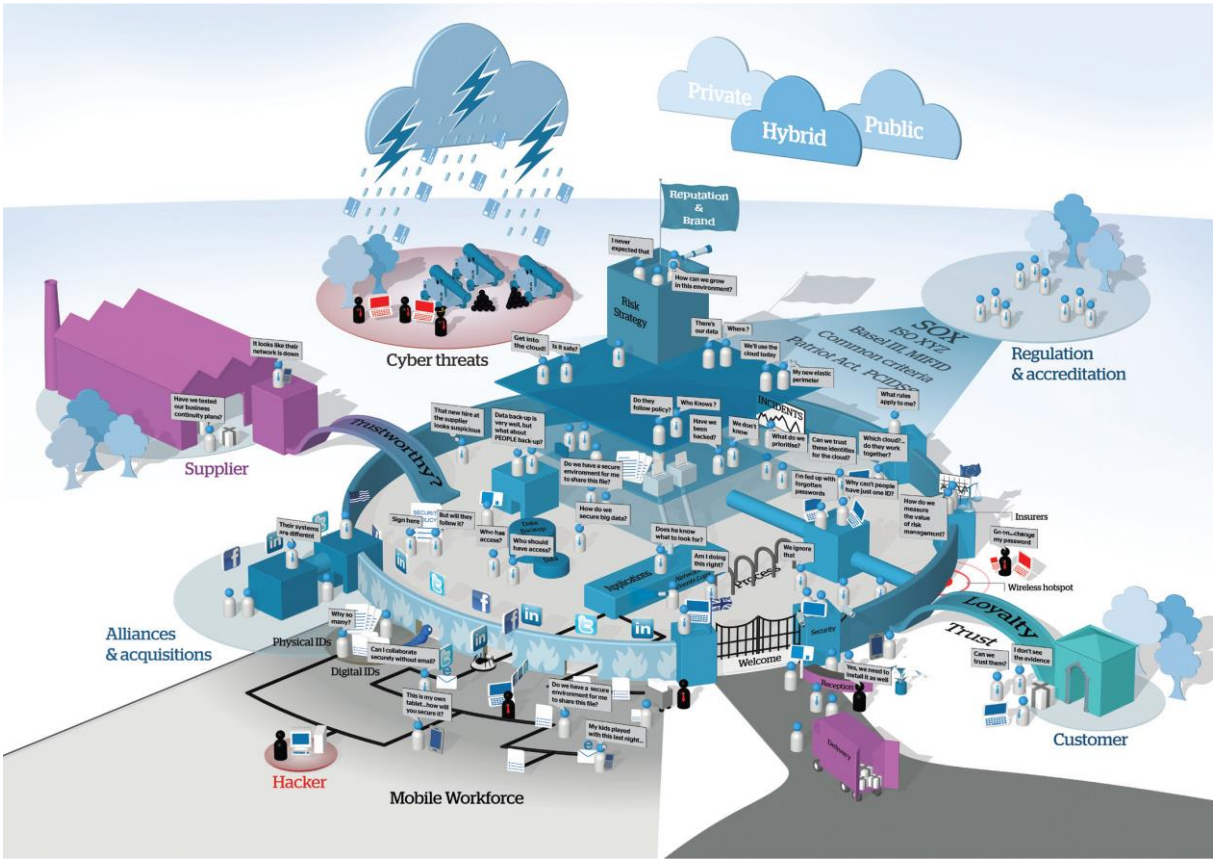

Figure 4 Schematic overview of the cyber ecosystem (Atos Nederland, 2013)

2.2.2 Definition of modern cyber security

Using the description of cyber security, extracted from the article *Mapping the Cyber Security Terrain in a Research Context*, the prime focus of this field is to look at the relationships and interconnections between the virtual world (cyberspace) and the physical world (Rowe & Lunt, 2012). The authors argue that as several security issues occur due to shortcomings on a technical or organisational level, cyber security is still seen to be a new phenomenon. CySec addresses challenges across a wider spectrum than simply information being exchanged between devices. At the same time, this field also strives to minimize the risk of unintended (additional) events that affect the cyber-to-physical domain to an acceptable level. In the early days of information security, this was not the case, as targets attempted to achieve near certainty regarding risk mitigation.

As IT infrastructure supports critical systems like the power grids and (emergency) communication channels, stakeholders from both public and private sectors insist that the infrastructure should be as secure as possible. This concern for security by stakeholders requires close cross-sector collaboration. This allows weak links to be identified, as these weak links could affect additional (highly dependent) sectors (Rowe & Gallaher, 2006). Various authors argue cyber security can also be seen as protecting the sum of all information systems' activities. This is apt, as its large range means that cyber security not only deals with a variety of attacks, but also requires multiple perspectives. Additionally, cyber security also deals with entry points for vulnerabilities and consequences that go beyond (in) tangible assets (Rowe, et al., 2011; Atos Nederland, 2013; Clemente, 2013; von Solms & van Niekerk, 2013).

The consequences of incidents as to (cost) (effective) protection also varies greatly – depending on the (financial and technical) resources of a stakeholder (group). Scale also varies as simple technical attacks could be employed to affect other (non-) physical assets as well. Examples of such technical attacks are denial and exploitation. Denial attacks stop operations, and such attacks are most seen medical devices. Exploitation attacks tap into accounts and are mostly employed to steal bank accounts. Evidently, these attacks have a tremendous effect on the health and trust of citizens (Berkowitz & Hahn, 2003)). For institutions who are unable to perform, this would result in a loss of reputation. It would thus also weaken their ability to carry out their primary task. A prime example is when the Dutch company Diginotar was hacked and could not certify secure licensed agreements or SLAs in the aftermath (Opstelten & Verhagen, 2012).

On a much larger scale, this means that for industries, stakeholders are additionally motivated to look beyond their own risks. This makes addressing joint concerns an example of a valid issue for today's cyber security challenges. In the present environment with the globalisation of (inter)national industries, this seems like a critical problem for organisations. This is especially apt for organisations that are working with outsourced and/or local partners in the value chain (Clemente, 2013). Yet, it is often unclear on how to make ends meet in terms of a joint set of rules and regulations, when each company has to adhere to different set of laws. These laws are mostly provided by the government, as seen with national cyber security strategies (Klimburg, 2012).

As cyber security tries to tackle a much wider field overlapping various industries and nations, the development into this field itself can be seen as moving towards a much more international format (Klimberg, 2010). This thought pattern prompts the general need for a new outlook for both global and national agencies, as they now need to look beyond business. These agencies also need to look beyond technical issues that are currently trending in form of standards and best practices, and move towards restructuring their regulations for security that reaches across (physical and other kinds of) borders. A joint platform (such as a national cyber security centre or NCSC for example) could help bring the expertise and knowledge of key stakeholders together to discuss long- and short term plans and activities (MOD, 2012; NCSC, 2013).

2.2.3 Versatile stakeholders in cyber security

As illustrated in the previous paragraph, a single event can orchestrate different responses from a stakeholder perspective. We duly selected five different group of actors, which each illustrate the undertaking of different activities. This also highlights the need to allocate each party on a different role and responsibility within the cyber ecosystem. Keeping these five key perspectives in mind, we look at what models and applications apply to these different groups. This is in order to outline what each group can do to observe and protect a tiny portion of cyber space in which they (inter)act. In order to become a productive member of the information society; cost, bandwidth, speed of service, education and skills, as well as access of content and targeted applications need to be taken into account. In the past, this was only available to limited to experts – yet currently, it has become available to all users through the Internet (Klimberg, 2010).

Individual users

The first of the new stakeholder groups to be included to take interest in securing the current cyber ecosystem, are the individual users. Their main interest is important, as they are in constant contact with the technology on a day-to-day basis for the short term. In turn, being the largest group targeted as IT consumers, their contribution to public opinion could make or break important long-term decisions through cementing an institution's decisions. For example, the importance of public acceptance in the debate regarding worldwide espionage by the NSA (BBC, 2014; Choo, 2011)). This acceptance can be gained by utilising applications and information supplied (commercially and otherwise) by other actors. An example of such an actor is e-commerce, which is used to order products, but is also utilised in education and to consult remote experts online. Because of the distributed knowledge and transparency available through multiple sources, awareness on security issues is present. These multiple sources range from basic knowledge on risks provided by organisations (e.g. Microsoft and banks) to using certain services (software and e-banking respectively).

Recent campaigns by governments are also taking place in different countries to create propaganda on security. These campaigns also serve to notify how enterprises and the public can help to jointly protect our ecosystem. October, for example, is the American Cyber Security Awareness month (DHS, 2013). Closer to home, the Dutch government has launched three campaigns through several public-private partnerships. These campaigns endeavour to educate various stakeholders on risks and security that takes place online, as well as how to proactively set up your own protection (especially for citizens; (NCTV, 2014)).

(Non-) commercial organisations

Since computers have been handling organisation data and processes, individual organisations have taken a keen interest in analysing various forms of threats and risks to their IT applications. This is due to these threats having a direct influence on the proper functioning of its processes. This category has been given a broad term as it is needed to encompass the different types of public- and private institutions. These institutions are represented as the first type of 'grouped' stakeholders that operate to achieve certain goals by using IT. As the approach and activities often differ for each (non-) commercial firm, because of their specialised field and variety in the kind of applications, it is important to find methods that have two requirements. Firstly, these methods must have common evaluation criteria from information security. Secondly, these methods must still keep certain aspects of (basic) cyber security in mind.

The British BS7799 for example, consisting of security controls and general principles, has evolved into the international ISO17799. The latter only recently changed its approach from viewing IT as merely a technical asset, to broadening its risk management scope to include dealing with organisational motives. These organisational motives are regarding physical and personnel security threats from the in-and outside of the organisation (Theoharidou, et al., 2005). This shows that standard development is quite a laborious and sluggish process. As the international standard was further expanded into the ISO27K family, this family served to move us into a new era of cyber security. These standards also took a variety of topics we mentioned above to expand its controls. Some of ISO27K's controls remain attached to the combination of preceding measures from information security to include organisational perspective. The organisational view means taking business application and processes into consideration as well while determining IT solutions that secure critical assets. This securing of assets is done by e.g. information handling, access control, separation of duties, administrators and creating several back-ups. Yet several newer aspects have also gained perspective.

New controls offer general advice on how to deal with organising mobile devices, social engineering, managing human resources and creating a user security awareness programme. This new control is still termed information security management, and includes several aspects of our definition on cyber security (Humphreys, 2008).

Auditing and international certification has also grown to encompass different topics. Regarding these different topics organisations offer a variety of methods for companies to partially meet certain criteria, varying in the field and type of processes and focus of the business. An example of the choice of topics is e.g. if it is important to get accreditation or simply adjust to general outcome. As authors Siponen and Willison point out: most of the management methods that are in place, or have gained a reputation in the field through acknowledgement, are too general to deal with the current environment and undeniably, the current specific scope (Siponen & Willison, 2000; ENISA, 2012). Researchers Armstrong and Armstrong in essence confirm the variety in methods through their paper on education of security professionals. Here, they illustrate again that in order to master the different standards, experts rely entirely on the fact that popularity and adaption in different environments leads to the common assumption that certain more popular methods are considered to be more effective.

These independent methods mentioned by different researches are in practice not additionally validated to fulfil their requirements in common practice (Siponen & Willison, 2000; Armstrong & Armstrong, 2007; ENISA, 2012). Yet, for various firms, it is also still important to implement changes that were suggested back in 1995. These changes suggested that institutions should be internally encouraged to share insights and information with peers and employees, which would lead to team building being prioritized over the reporting structure. It was important to share these insights, across departments and through relationships of cooperation. A security strategy and indeed policy can only be deemed successful for individual groups of stakeholders in the present cyber security environment, when these changes are taken into consideration (Duncan, 1995).

Industrial auditing committees

The specifics of creating general standards take place in several critical industries through regional committees that look for compliance of the basic requirements. This is not offered for each separate institution, nor is there an option of validation from independent and internationally recognised third-parties that can confirm these guidelines for institutions (ENISA, 2013; ENISA, 2012).

As computers have become an increasingly integral part of processing information for several critical sectors, this development is coupled with an increasing need for a reliable auditing method. This method aims to offer each industry the opportunity to check up on its members. A different type of model was required, because though institutions have been established at the same time, differences in the field and activities call for a new perspective when using IT security. For example; banks, hotels and hospitals might be using the same IT reservation system provided by a common (e.g. IBM) manufacturer for booking or arranging consultancy hours. Yet upholding the privacy of a client is quite a different matter for the hotel staff than the security. Additionally, in a hospital setting, this security must also be maintained for third parties gaining access to confidential patient data. General information system management standards (ISMS) might aid in identifying processes and controls that are similar. Yet, it must considered that each institution lies in a different field, which has its own strict national and domain-specific criteria. These criteria must be approved and met before it can operate in the same area.

The difference of generalising and maintaining specific approaches between different fields becomes increasingly important. This is especially when observing how within the public sector government officials (e.g. police, emergency aid) and military personnel follow a different governance structure altogether to suit their own tasks. Separate mandates and committees are formed to be transparent to citizens for general knowledge and information; whilst still being able to hold a level of secrecy to operate within the cyber ecosystem. This is in order to protect several of the government's assets and integrity of the infrastructure.

In turn, some confusion still exists on definitions. Field experts in literature neither confirm nor deny that the term cyber warfare exists. This is because the information regarding expenditure and classification remain hidden from analysts. Additionally, this term is applicable in many instances, such as the crippling of the Estonian IT infrastructure in 2007 by hackers (Various, 2014; Economist, 2012; Quora, 2013). On the one hand hiding this information is justifiable, as the hysteria it could cause should be considered. One example of such hysteria is the crashing of stock markets if intrinsic values such as trust and confidentiality regarding government information should be leaked. While on the other hand, values of protection and integrity cannot be upheld if there is no transparency for citizens. It also causes controversy when public institutions hold a different set of rules and regulations by disregarding basic privacy rights to protect individual users.

National cyber initiatives

Comparable to domain-specific models, even nations differ in how to organise and approach the problem of dealing with cyber security. Some countries, for example, find it important to have platforms for public-private organisations to work together (such as National Cyber Security Centres). Yet, to certain extent each country has its own extension of an international standard (ISO27K becomes the NEN in the Netherlands). This extension provides technical and organisational controls to also meet certain rules and regulations for protecting a regional ecosystem. Recent incidents such as Diginotar have shown how government intervention is necessary to guarantee the quality and trust between parties, even when certifications and industry level standards are met.

A recent document by one of the representatives of the North Atlantic Treaty Organisation (NATO), reflects on common issues that nations address. These issues focus on entirely different topics than the preceding stakeholders. Though the document is written from a defence and crisis management perspective, it illustrates how issues such as counterfeit and malicious software could damage national security systems and government services. With ICT being seen as a core infrastructure, protecting such a large scale network across different countries raises concern for these countries. This protection ranges from national cyber strategy to criminal activities in cyber space. National cyber strategy or NCS cyber warfare and defence aims to secure national and economic security initiatives. Examples of such criminal activities are espionage and using IT to conduct felonies and undermine national rules and regulations (Klimberg, 2010).

Both examples provide us with a rough sketch of national approaches to cyber security. These examples intend to show that while each country has a different idea and approach towards dealing with this issue, they all have to deal with similar risks and trends seen by different perspectives. The idea behind national level cyber security is to bring together regional public and private stakeholders. Here, these parties can discuss appropriate mandates to secure a region that is line with its legislation.

Global initiatives for cyber security

Governments have been creating collaborative groups to address a joint approach for similar topics for quite a while. In fact, several nations do collaborate internationally to join efforts and address global problems. For example, the United Nations (UN) contributes in climate change, international conflicts, development and aid programmes. Activities in cyber security also have a similar profile such as the preceding global problems, where recent cyber incidents such as Heartbleed and Diginotar surpass national borders and industry fields. Thus, they affect various public and private institutions, as well as citizens around the world. This finding calls for an international committee to oversee global developments and manage the role of informing and directing nations, industries and citizens towards a right path. This path involves a joint undertaking of specific tasks to protect our cyber ecosystem. In turn, a partnership on an international level can also help coordinate practices across borders. This serves to address criminal activities together, allowing nations to settle on a general taxonomy and viable approaches. This situation is comparable to the present organisation of policing activities to catch criminals who operate from various countries.

In line of the recent discussion on whether cyber space is a fifth domain for warfare, joint organisations such as the NATO take on a military perspective. This perspective serves to analyse how activities should be organised by governments. The results are published in annual reports such as the National Cyber Security Framework Manual, which aids nations in setting up their national strategies (Klimburg, 2012). The same organisation has also earlier helped overcome cyber-attacks in Tallinn (Estonia) by sending their technical expert team. Additionally, within Europe, it is the European Union Agency for Network and Information Security (ENISA) that brings together the EU member states and determines what standards (industry, international) and best practices should be applied. This enables the European Union to share knowledge and updates of changes in community legislations (ENISA, 2012).

Despite the existence of such collaborative parties, there are no solid examples of global collaborations in the field of cyberspace. Therefore, there are also no examples of tested or fully explored models present in the current environment to illustrate or determine the effects of such a model. This is why we leave the context for defining a global solution open.

Subtle difference between information- and cyber security

With regard to this research, cyber security is defined to focus on how different fields apply IT. These fields are always collaborating together in a variety of forms, due to interconnectivity and interdependency between them (as mentioned in section 2.2.1). Based on our literature, research argues for a new approach. This is because, as opposed to the prime definition of information security (see section 2.1.2), security can no longer be guaranteed by placing measures to protect who *owns* the given IT technology (also mentioned in 2.2.1). With the variety of IT measures for a joint environment, it is now imperative to look at how these measures can be generalised and specialised. The aim of the former is to be used between different organisations and of the latter to view for example what these sectors could learn from each other.

Whilst the previous field of InfoSec emphasized the importance of having a risk analysis preceding its actions, information security is assumed to have robust techniques. These techniques aid in gathering and processing of the data at hand, in order to apply the knowledge. However, CySec is a different story, as it is always present in some form within a network. These forms range from basic protection for software admission, to password authentication in a larger network. Therefore, CySec requires a wider analysis than just looking at a single component. This single component is within a value chain e.g. business or individual user, or similar activities e.g. business, industry or country.

2.3 Answering (sub) research question 1

By constructing the following conceptual framework (summary in figure 5), we show how historical developments progressed from the early concepts of InfoSec to methods that are still used similarly today. In addition we note the challenges need to be addressed in the future, as current methods only protect parts of our cyber ecosystem without a lot of interaction with other stakeholders.

This chapter aims mainly to answer the first research question: *how do we define cyber security?* The first paragraph aims to provide a summary of what the industry sees as cyber security; the second paragraph goes on to illustrate an ideal setting, proceeding to wrap up the chapter by identifying the gap in the current body of knowledge.

2.3.1 Current situation regarding cyber security

In the present IT environment, we see that different industries still continue to use existing historical models and measures, which are based on information security. The preceding field still maintains a stronghold, because its main concepts like CIA and PDCA form the base of widely used international standards. These basics are provided by BS7799, which are now present in the ISO27K family. These international standards also influence many organisational and domain-specific domain models. Throughout the years, each institution has created its own security model or 'best practice'. This own model is seen to function separately in terms of managing the risks when an incident occurs (island model). Recent risk management methods are also being designed to complement each other, hence the rise in harmonisation studies. A lot of examples for cyber security exist on:

- *Organisational level*, which has been active since its introduction the late 1980s. Even now we see that each company has taken to designing their own model. This model compares business and/or enterprise processes to technical specifications, and IT is the central component that needs protection.
- *Industry level* sets its own standards, where fields such as banking have their own strict code of conduct. For the security auditing industry, periodic checks of standard requirements need to be met in order to gain approval. These requirements also need to be met to be able to function within the society.
- *National level*, which requires framework strategy to be updated frequently. It also needs to be considered whether current rules and regulations still operate with the introduction of new standards or need to integrate IT of infrastructure.

However, fewer campaigns can be spotted that are aimed at *individual users*. Yet, other stakeholder groups participate in creating awareness of a variety of incidents, which occur in cyber space. These incidents range from cyber bullying (national campaign) to phishing (commercial companies). These other stakeholder groups then distribute general brochures on how to avoid such incidents. Similarly, on *global* level, countries do collaborate together. Yet, countries do not specifically work towards general protection of cyber space by assigning direct actors. This is in stark contrast to the observation that this topic seems important for international military security, as there are organisations such as NATO. These organisations come together on the military field and aim to protect cyber space from a higher level, despite the existence of blurred border lines in cyber space.

Both stakeholders need to be covered by definitions and frameworks as well, as common IT knowledge ensures protection from the basic level for individual users. This is because these individual users are by far the largest group that need protection. Additionally, overseeing international collaboration is vital while boundaries slowly fade away, as incidents in cyber space affect the physical domains and multiple stakeholders. Actions by both actors, global and national, are affected by actions in cyber space. Therefore, these actors also form the remaining two keystones in our 'level based model' to dividing roles and responsibilities. This division aids in securing the shared virtual domain.

2.3.2 In an 'ideal' world

In the present world, our current risk management approach for security (through e.g. standards, best practices and guidelines) can only cover a certain level of IT risks. These risks are for a number of stakeholders on an organisational, industrial and national level. It seems that there simply are not enough measures in place through the cooperation of individual users and global stakeholders to offer protection that encompasses the entire cyber space. The latter is much needed, because of the current interconnectivity and global dependence of the IT infrastructure. For example, one incident in our cyber ecosystem could affect many more stakeholders, such as the KPN hack, violation of SSL certificates issued by Diginotar and worldwide digital pandemic caused by the Heartbleed bug. In order for everyone to benefit from a healthy (risk-free) cyber ecosystem, we thus need a collaborative effort to secure it. This can be done by sharing roles and responsibilities.

2.3.3 Analysing the gap between both scenarios

In the first paragraph of this chapter, we noted that security for IT grew from being a purely specialised computation technology at research faculties to being adopted by other sectors. Stakeholders varying from personal computing, to medicine and nanotechnology, each used different IT applications to aid their core activities. In turn, when faced with arising security issues, each group (e.g. domain or institution) decided to employ their own standalone IT solution. This solution was based on their own information on existing risks and/or combined the knowledge to create tools employed to mitigate them. The separate approach brought up by various stakeholders led to a variety of different approaches, definitions and standards of risk management to tackle IT-related security problems.

From the commercialisation of the Internet in 1993 to its worldwide adaptation around 2000; the use of IT applications accelerated. This was due to the addition of a new layer to cyberspace to enhance connectivity between actors and IT in the existing domains. IT's public importance also increased when multiple groups networked using the Internet more frequently, next to the joint processes which already ran on the common IT infrastructure. These new developments meant that awareness of both the risk of growing interdependencies and the risk within cyber space became complicated when cyber incidents occurred.

Despite the abundance of organisational, domain-specific, and national frameworks; there was no common ground for these different models when major incidents occur. And due to the growing interdependency and interconnectivity on cyber space, it became increasingly important for collaboration between these sectors to take place. This was in order to have a unified approach, as shown in figure 5 on the next page.

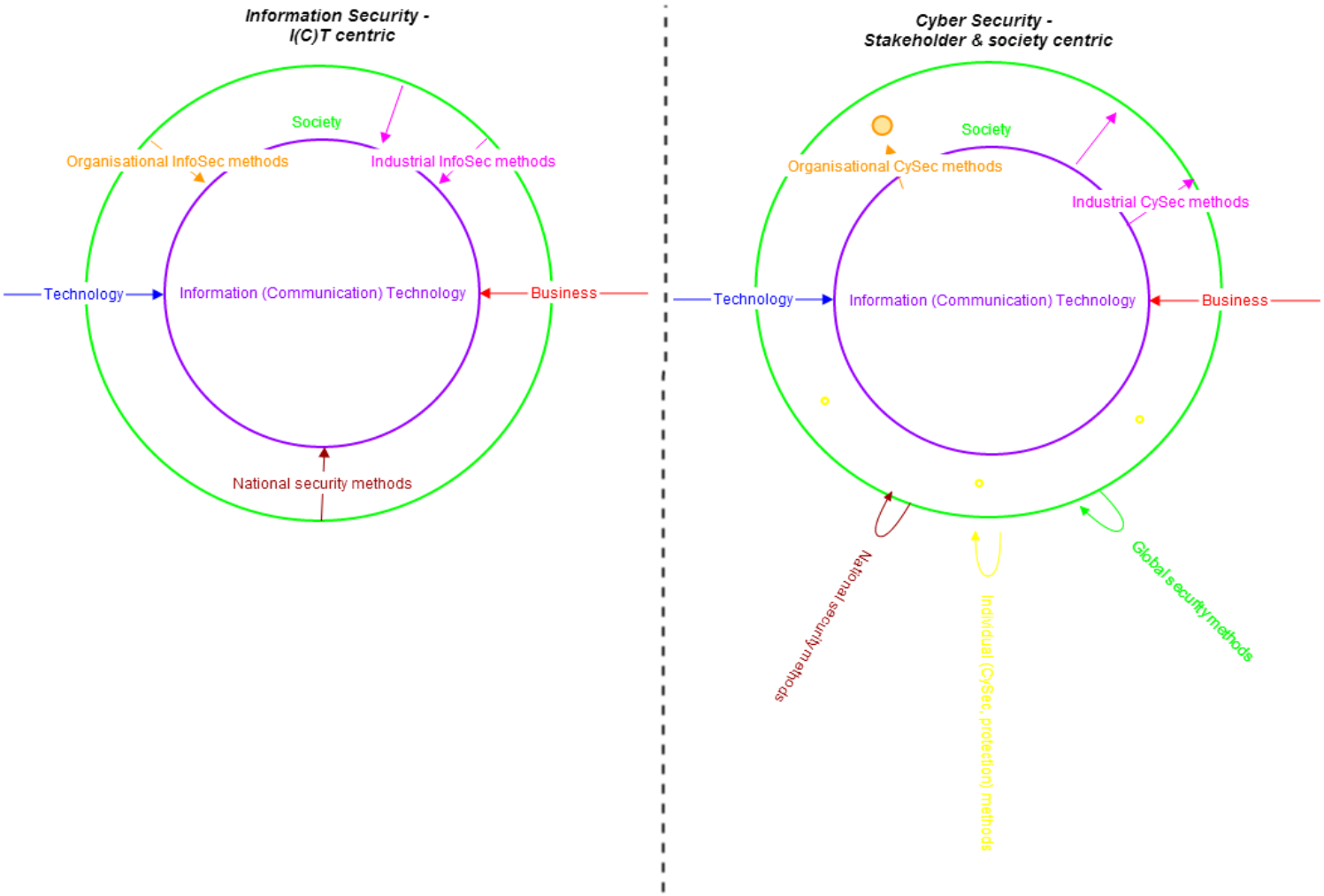

Figure 5 Gap analysis between information security and cyber security

A summary of the differences between the two fields is given in the following figure (5). Here we see that the right side depicts the information security (InfoSec) movement that regards security issues from a mostly technology centred perspective. Primarily, this means that the focus from the business and technology is on IT for coming up with new IT solutions. At the same time, even popular perspectives from organisational, industrial and national security measures look towards what IT specialists see as solutions to a problem. Consequences for the society are not yet taken into consideration for this movement of IT security.

These changes, together with the development and introduction of new actors in cyber space, have however not been taken into consideration within the older generation of information security. The definition we use further in this research for *cyberspac*e is the same as the one adopted by Atos. This definition considers cyberspace as an ecosystem where different actors (inter)act with each other and jointly influence activities within the plane. This leads to the thought when IT's ties and applications in other areas strengthened by other actors. This occurred when the technology became the underlying nervous system for many industrial infrastructures. In turn, IT's use became versatile as the technology adapted itself to society's use in different fields – from serious gaming used for educational purposes to mobile solutions such as cloud computing This is why currently, the new era of cyber security should focus on incorporating these different approaches from society. This aims to tackle security issues that affect all of us through cyber space. In short, *cyber security* is seen as the collaboration of all actors to jointly secure cyber space. This is done by carefully agreeing upon what activities, roles and responsibilities muse be taken by each actor.

Subsequent to the discovery of the gap we identify between these two different approaches or generations of IT security, a gap is also present in the current body of knowledge. This is considered as approaches that are currently used to secure cyberspace, do not differ from the original IT security. Thus, these approaches make it more difficult for actors to reach out and work together by undertaking different tasks that complement the areas that are being protected by a specific stakeholder group. The subsequent chapter (3) shows how cyber security is still being driven by technology solutions, which are derived from following InfoSec methods. However, to jointly secure cyberspace, it is imperative that the different approaches can be moulded into one integrated model.

In the first step towards understanding what key issues need to be addressed in order to create an integrated approach, we identify the differences in preceding and current methodologies. The following chapter builds on the background provided in this section. It does this by looking at existing methods and their shortcomings with regard to the previously described gap analysis.

Chapter 3 – Mapping existing IT security measures and identifying requirements for cyber security

In the previous chapters on stakeholders and developments, we observed how IT security measures have grown from being designed purely through technology solutions to being tailored according to each actor's environmental needs. This is seen by the use of many different methods; from standards for public- and private organisations, to guidelines for different industries and national cyber security strategies (Höne & Eloff, 2002; ENISA, 2013; Klimburg, 2012; Armstrong & Armstrong, 2007). The aim of this chapter is to clarify how information security differs from cyber security by examining aspects of security through risk management from each stakeholder's perspective. Information security only manages the risks in the direct environment of the stakeholder. Whereas in cyber space, the impact of such risks is larger (von Solms & van Niekerk, 2013). It is therefore important that actors should jointly interact in cyber space, and thus manage risks jointly that affect everyone.

In this section, we note firstly note that development of new types of standards is often in line with historical events. On the one hand, security measures can be determined by the focus of the technology alone that leads them to be popular after adoption. In the technology market for example, a technique or application gains leadership as the *de facto* choice or unofficial industry-wide acceptance. This then means that the security methodology is adapted in a similar fashion. Another example is the Internet, which was originally created to distribute information. Yet, we still see problems arising because the developer's choice of accessibility to users took higher priority than a bureaucratic process around the technology to manage its key components; e.g. centralised directory (Campbell-Kelly & Garcia-Swartz, 2005).

However, the type of measures can also be seen as following the same pattern of environmental developments. This is considering the addition of similar topics according to popularity of a newly introduced method, as found in numerous standards' topic emerged around that time (Bernroider, et al., 2013). Protecting computer assets from harmful activities, is still part of current methodologies ranging from best practices to international standards and guidelines (Heasuk, et al., 2010). In turn, the emergence of business also showed a new model that can be adapted to manage IT in a different industrial context. An example of this model is when the Plan-Do-Check-Act project management cycle was modified for the American national standard NIST 800-30 to tackle information risk management.

On the other hand, cases also exist where many organisations gathered to develop and increase their chances adopted together. This was due to the many alliances with companies who all used these models. For example, finding common practices between multiple industries is one of the main reasons why the BS7799 was used internationally to compare general security controls between firms (Höne & Eloff, 2002). This new development on collaboration notes the shift from purely technical solutions to integrating IT measures according to market needs. This shift is demonstrated in the preceding case comparison, where the aim was to improve the efficacy of IT security methods in different organisations. Various models emerged, striving to become the model used by a majority of the industry. This was due to adjustments in the model, e.g. CoBIT for business, or a variety such as the ITIL that aims to incorporate all IT topics.

To overcome the differences that current models have, the developers of these methods believe that practising harmonisation of both models with the IS27K would provide the best fit in the industry. This is because it combines the variety of topics to overcome the method's weaknesses (ISACA, 2008). In turn, maturity models are also an important research direction, as guidelines are often seen to be too general from a company's perspective. These guidelines also dismiss the long-term development of an organisation (Lamb & Yu, 2011).

This variety in methods and topics makes it confusing to understand what type of development can empower multi-actor collaboration. Thus the aim of this chapter is to determine what the focal points of previous and current methodologies are. Additionally, this chapter aims to answer how these methodologies are still used to secure cyber space. By sticking to a historical approach shown in Chapter 2, section 3.1 looks in the field of information security. This is in order to see how the methods are in line with historical developments. Consequently, the second section explores the same question, whilst also exploring stakeholders in the cyber ecosystem. Finally, we compare the findings for both generations of IT security. This is in order to provide an overview of requirements for each level. Collectively these paragraphs serve to answer the second (sub) research question:

What can we learn from literature about cyber security collaboration?

3.1 Information security standards and frameworks

Following the approach of our literature review, illustrated in chapter 2, the second step is specifically directed towards understanding popular methods used in the field of information security. This phase of research explored journal articles which were slightly more recent in this section, with the earliest available article from 1987. This is because publications and researchers approached the topic of information management systems, only when IT became prevalent in industries (Brancheau & Wetherbe, 1987). As to the end of this phase, some field researchers still believe that information security is present today. This is because it is considered to be updated with modern methods such as situational awareness. Therefore, 2014 is seen as the last year in which the methodology for this topic is active.

The search terms on Scopus were determined by cited articles found in Chapter 2. These cited articles for comparative studies, show how methods differ from each other. This is done by looking up articles relevant to the terms "information security" and "standards". This initial collection was expanded by replacing "standards" for "policy" and looking into "information management" and "information management systems" instead of security. This was because these methods were in line with widely cited sources regarding the move of information security towards "business security" and "governance" (von Solms, 2005; von Solms & von Solms, 2005).

While most articles' references helped identify key controls and criteria for each of the models, exploring Google (Scholar) helped find more detailed information. This information offered different development stages, as well as alternative papers if certain information regarding the methods was unavailable. As with in the previous stages of research, the Elsevier journal database provided a number of useful recommendations. This was especially for industrial methods that actively used information security, such as security of industrial control systems or ICS in petrochemical plants, also referred to as SCADA systems. In addition, company articles about the latest updates to these methods were also found by using Google Scholar and used to complement our database approach with recent findings.

The first reports regarding the technical (in)security of IT systems was published in 1968, containing findings of vulnerabilities in time-sharing systems. This was a seen as the initial start, where technical experts were trying to figure out what controls and mechanisms could help protect a computer system on various levels (Whitman & Mattford, 2011). In fact, it is due to the first widely published document on securing classified information systems, the "Rand Report R609" by Advanced Research Project Agency (or ARPA), that a formal explanation is given about what tasks related to the "computer security" of classified information systems needed to be implemented. This report was the first to give formulated recommendations (Whitman & Mattford, 2011) regarding:

- Protecting *information* (moving beyond measures taken for the physical location);
- Prompting more strict authorization *for access to data* rather than random or unauthorized entry;
- Different people from *various departments working together to protect the system* (leading to a holistic approach towards information security).

All three categories in fact, can still be found in the classical standards of information security. For example the BS7799 (converted to ISO 17799 and now ISO27002:2005) Code of Practice features *asset clarification and control*, *personnel- physical- and environmental security*, *system access control* and *compliance*.

By using the definition mentioned in classic risk management, we refer to the book by Jones & Ashenden. In this book, it is illustrated that there are three types of risks for the internal organisation:

- Risks on a *strategic* level: these risks directly affect decisions taken at a top or organizational level. These are any risks related to IT assets; from product positioning to expansion plans. However, before determining the actual risk and whether it should mitigated or left as residual, the top management should first take a look at how this might affect its (long-term) goals and objectives. To do so, the key risks could be measured in advance, or on a periodic basis, by using e.g. a threat analysis.
- On a *tactical* level, risks on this level affect the middle management and the responsibility falls between the manager and programmer or IT employee. As the manager appears at the board or has influence on making key strategic decisions, the risks on this level are mainly about avoiding losses, vigilantly monitoring key indicators, and keeping the right tools and techniques in the vicinity for additional assistance.
- *Operational* level risks were always meant to be handled by the IT worker; as it is (s)he who sees to it that the internal IT processes are working as specified by the design. This actor is responsible to keep track of the fact that no matter what kind of incidents occur. These risks are largely influenced by understanding the nuances of the work environment. If internal processes are misunderstood and immediate action needs to be taken – then a back-up plan should be in place to mitigate or keep residual risk at a minimum (Jones & Ashenden, 2005).

However, it was not until business got involved in IT security towards the 1980s, that the association between IT and risk management was taken into serious consideration. When it comes to quantitatively measuring risk, it can be defined as the probability and magnitude that a certain unfortunate event occurs. Thus it can be viewed as a predictor of scenarios that could occur, depending on the scale of impact categorized as loss or disaster (Hubbard, 2009). Mathematically however, risk can be measured by multiplying impact with threat to gauge what the consequences of such a risk would be.

In addition, the definition used by management aims to helps plan, organize, control and direct the research towards a predefined objective. This definition is thus useful in determining how failures can be tracked and prevented through various types of risk assessments. This method is also popularised as the project management method of Plan-Do-Check-Act by Dr W.E. Deming. It is still used in several international standards to execute the security process, e.g. NIST 800-30. With regard to the general topics found in information security, there are four ways to carry out risk assessment methodologies:

- *Vulnerability assessment* which is used by existing standards and proprietary tools. It is used to analyse components of the information system.
- *Information systems audit* of internal controls; this is conducted to keep management, authorities and shareholders up-to-date on financial and operational performance.
- *Information security risk evaluation* is used in order to identify and mitigate risks that are derived from the *vulnerability assessment,* thus concentrating on technical capabilities. It also aims to examine trade-offs for the most cost-effective approach.
- *Managed service providers* intend to subcontract activities to a specialized firm. This is performed through planning, detailed implementation, monitoring of progress and control small variations to keep consistency on check (Alberts & Dorofee, 2002).

Information security was highly popularized between the 1980s and 2000s. In fact, most of the emerging standards have gone through various update cycles in order to keep up with preceding definitions. These update cycles range from the CIA triangle mentioned by the American DHS department (see 2.1.3) to general security evaluation criteria used in risk management. These security evaluation criteria are based on technical, organizational and tactical aspects. To understand how these concepts functioned in practice, we provide a short analysis of popular methods with a description on how they were used. In turn, an additional analysis links these methods with the theoretical concepts mentioned in the previous paragraph. This is to show how theory is put to practice.

3.1.1 Organisational InfoSec methods

The main characteristic of InfoSec is the existence of different models. Using comparative studies, we note the differences between several standards to be quite vast as they address different criteria from information security (Heasuk, et al., 2010; Höne & Eloff, 2002). What this section additionally introduces is an own analysis by selecting four main methods. The intent of this analysis is to show the diversity and application that is still popular since the original introduction of the business perspective in the 1980s. Methods such as the BS7799, CoBIT, ITIL, and ISF's Standard of Good Practice are still popular today, being recommended by important institution such as ENISA. These methods are thus recognized by European nations to deliver important surveys and research into industry applications of security models.

The BS7799 is seen as an important landmark in security models, as it was the first model to be used by companies. These were mostly companies that are active on an international field, exploring various security domains. This is reflected in the analysis of topics or general principles, as it covers over 11 different domains where IT security can be applied. It also offers over 130 security controls and objectives that need to be met. Additionally, there are opportunities to evaluate information systems through this standard, based on extensive risk assessments and mitigations available through different methods. Therefore, this is seen as the most extensive standard published by the British Standard association for information security. Its successor, the International Standard IS7799, has been developed from a systems approach. It has been developed to an organisational standard, as later on it lent itself to be used by IT professionals from different industries. This organisational standard was one of the first to introduce a code of practise, and grew to become a (partially) compliant standard (Limited, 2012). One of the setbacks that is still seen in its current successor, the ISO27K family, is that it still remains general. It does this by only proposing principles and models that can be used, not specifying how to use the schematics which need to be filled for a specific organisation and/or industry.

The CoBIT is another model that has come far since its design. It is based on established frameworks such as the Software Engineering Institute's CMM, ISO 9000, ITIL and ISO/IEC 27002 (ISACA, 2008). Additionally, it is intended as a high-level governance and control framework. The model is used mainly to get a good understanding of the basic principles of the processes that occur in an enterprise and how to manage and control the related IT risks. Similar to the BS7799/IS7799/ISO27K family, it is also a general framework without providing any specifics into how it could best be used within a certain context. Instead, it looks at a strategic level – aiming to explain how top management and auditors can assess the processes. This assessment is done in order to establish what needs to be done for long-term vision. In turn, CoBIT also tries to explain why certain roles and responsibilities within the organisation must be held in place. These must be held in place in order to determine a hierarchical structure that determines action and punishments for violating certain base rules needed for basic information security. Due to its specific design, it does not turn to explain additional topics such as user education and/or organisation awareness – instead refers to IS standards and/or ITIL for further information.

The ITIL is a general service library that offers advice on structuring Information Technology by consulting a wide range of infrastructural standards, which are present in its database. By drawing on information provided by its various partners in public and private partnerships, the method provides a solid background for establishing the basics of IT Service Management. It does this by looking into and evolving its current practices after receiving an update from its developing partners. These partners have tested it and provide results in the various publications. Due to its wide use in different industries, ITIL is thus not organisation-specific. However, ITIL provides general outlines on how certain tasks, procedures and processes can be structured in order to work with existing internationally used company frameworks. For example, frameworks such as Prince2 and MSP can be used for project and program management. This standard is also a continuation of a previous ISO/IEC standard, named the 20000 on IT Service Management (Axelos, 2014).

ISF Standard of Good Practice is also of British origin. Referencing the 2007 version, we see 166 different regions in six different areas. These six different areas are enterprise-wide security management, critical business applications, networks, system development, end user environment. These areas serve to replace the internal standard in conjunction with other ISF methodologies and tools. Examples of such tools are risk and security assessment, as well as identifying the return and third party involvement (Limited, 2007). The ISO27k family emphasizes the applicability of certain sectors to implement a general code of practice and is oriented towards reaching the controls. Yet, this method uses the organization as a starting point. This leads to a division in the roles and responsibilities according to each layer in the management hierarchy for a certain area of expertise. The option of having Special Interest Groups also adds value, as it aims to attract members with an interest in the security and risk assessment. This allows more managerial insight from a certain industry's perspective (Limited, 2012). The ISF standard is chosen as a counterbalance to the preceding methods, as it is developed by members who might have noted certain changes in the environment. It thus encourages these members to take a different perspective. Adopting this standard would also make it possible for organisations to be the first in applying a tool, which harmonizes several new concepts. Examples of such concepts are resilience, supplier validation and awareness; next to the 118 topics such as compliance and policies.

3.1.2 Industrial InfoSec methods

Thus, several general auditing measures exist for specific domains or industries (ENISA, 2013). Banks for example have BASEL II. BASEL II are the international settlements reached together with national central banks. Another example is the American Surbanes-Oxley (SOX), which banks need to comply with in order to operate within that region. As payments through the mobile industry become increasingly popular, the Payment Card Industry Data Security Standard (PCI DSS) is becoming an increasingly important, international reference point. This reference point is in aid of how card brands can for example individually structure their schemes, to set up contracts with partnering vendors and suppliers. However, in the field of e-health we see differences in standards that can be adopted. Examples of such differences are seen when comparing the U.S. to the Netherlands. In the U.S. there is a Health Insurance Portability and Accountability Act (HIPAA), which covers aspects of electronic health care transactions and privacy to health identifiers and security. On the other hand, Dutch hospitals need to follow and uphold several national standards (NENs). These standards range from the NEN2510 for e.g. ultrasonic devices, to the NEN2799 which is in place to protect the patient's privacy.

These former issues have led to our general analysis of industry applications, in which we identify the following two common approaches to standardising IT systems;

1. The Information Management Systems Approach, which for example is purely used for industries that run IT. These industries use this approach to complement their core activities e.g. airline industries, and programmable logic controls (PLCs) for the energy industry. The same way, general techniques are taken from local hard- and software standards to establish a baseline for common uses. For example, the technique using minimum requirements to support an application until a newer version appears (e.g. Windows XP that is not supported due to the availability of newer operating systems).

2. Additional standards that aim to control core IT activities, such as the Sarbanes-Oxley act and/or Basel (II). These examples control banking opportunities. Additionally, there has been a recent evolution of international methods in order to involve privacy and protecting citizen's data across border into standards. Examples of such an evolution are when recently multinationals such as Microsoft and Google were chastised for collecting data and using this data without the individual user's consent. Similarly, even safeguarding patient data has been included into (inter)national requirements. These requirements must be met before a hospital is granted permission to legally operate.

3.1.3 National InfoSec methods

Just by analysing the countries cyber security strategies, we see how different they approach the problem. Ideally, countries should have multiple contingency plans based on analysing all-hazards risk management. These plans are in order to note all possibilities that could (in)directly affect national vulnerabilities. While in InfoSec incidents were technically related, current strategies point out that viewing these incidents from a broader perspective show new incidents to look into. Additionally, new trends that can also be observed, such as the impact of political activism. Current trends indicate countries, such as the United Kingdom and United States, combine different aspects of public and private partnerships in their national security strategies (NIST, 2012; Clemente, 2013).

By coupling security policies with economic and political dimensions to involve multiple actors, these nations strive for an overall ecosystem resilience. They do this by keeping track of trends from different industries. Countries such as Canada show progress towards using civil with complementary military assets. This allows us to look into possibilities to combine the two conflicting areas (constitutional vs. societal) effectively. This will lead to the ability to jointly address incidents with their networked or 'comprehensive approach' (Quigley, 2013; Klimberg, 2010). The Netherlands uses a different societal approach to create a constitutional status. It does this by allowing the National Cyber Security Centre to collaborate on information sharing through the vital sector. Thus, expertise on their governmental computer emergency response teams (or GOVCERT.nl; (NCSC, 2014)) is improved. The United States of America has yet another national approach to involve its government in protecting its information infrastructure. This involves stating different policies for national and organisational institutions to comply with, before being able to operate with information systems (DHS, 2013; NIST, 2012).

3.2 Cyber security standards and frameworks

As explained in the previous chapter, we have identified various stakeholders groups. We use our own insight from sources mentioned in Chapter 2 and section 3.1 to identify issues that we feel are important for stakeholders operating in cyber space. The following five groups are considered in our analysis: public, organisational (firm), industrial, national and global. The domain of individual users has not been argued as frequently as the other groups. This is because no 'user safety standards for cyberspace' or similar guidelines have been put in place for this actor. However, government initiatives are slowly picking up to increase user awareness on the dangers in cyberspace. Examples of these methods are the Alert Online campaign by the Dutch Government or cyber bullying prevention by American National Crime Prevention Council.

Results from our literature section have been taken from various sources, where media to literature sources observed different ways to govern IT security. Here the depth of details for managerial and technical issues depends largely on what standard is used for a certain application. However, when consulting comparative studies in academics as well as surveys, the methods vary greatly. Furthermore, it is difficult to determine what the best method is and this also depends on the context for a given institution. The research question for finding requirements is to be answered in this section by:

- listing the different methods, and
- determining what the focus of certain stakeholder groups is;
- thus providing us with a method to split the framework into different levels.

These requirements are also similarly stated as key issues throughout this section.

3.2.1 Public CySec methods

Looking further into sources initially identified in section 2.2.3; we see that the level of education and experience varies between the new generation of users. The younger generation are currently schooled in considering risks and using tools through courses. This generation also experiences varying degrees of cyber exposure because of an increase in devices. This might not have been possible for older generations; as they were educated through profession and interest. This education was mostly gathered by looking up information, which is freely available through media. Additionally, new phenomena such as cyber bullying and cyber fraud have recently emerged. These have mainly risen due to the digitalisation of many activities. This digitalisation varies from every day interaction with friends in society (social media and chatrooms) to internet services (banking, shopping).

Public knowledge about computer protection and proper use of its autonomously secure IT devices is actively being campaigned. However, two scientific papers indicate a conflict between the effectiveness of education and a user's actions towards security (Furnell, et al., 2007; Davidson & Sillence, 2010). This is due to internet evolving to being used by the public, which led various institutions to look into educating the public on the risks involved in acting in cyberspace. In the following section, we note four issues that are important for individual users.

Various institutions should be able to empower individual users by:

(1) *Education on IT risks*. Currently we notice that public and private institutes provide digital pamphlets for individual users. For example, when phishing was detected by many companies, information to the public was given by different companies. These companies varied from Microsoft to banks with internet facilities. In turn various types of media also offer a broad coverage of recent events that occur, though sometimes the perspective might not be completely objective. On an international level, many public and private institutions such PricewaterhouseCoopers or ENISA publicise their research and insights. This is designed to share their views on what is upcoming in IT technology and security. While these views may show that there is a wide variety of information available, there is not a single dedicated program to educate individuals on the consequences of their actions.
Schools, high schools and universities presently do offer programs and/or awareness campaigns to the younger generation. This offer may vary geographically. Companies may do the same, as they aim to educate their workforce. However, options should also be made available by the government. This could also be conducted in collaboration with private parties, in order to provide opportunities to citizens. This is especially for those citizens, who might not have access to information from these sources, such as the older generation or less experienced users.

(2) Raising *awareness*. October in America is seen as national security awareness month with its various activities. On the other hand, the Netherlands had an own Alert Online campaign. The intent of this campaign was for different interested parties to come together to look at how different parties were developing IT technologies. This platform also provided insight on how different parties and the Dutch government tackle IT and its national cyber strategy. Another Dutch institution that prides itself in getting known is Bits of Freedom, who look into privacy and legislative issues concerning user data in the post-Snowden era.

(3) *Provide tools* and *tutorials* to safely explore cyber space. Due to the decentralised nature of the Internet (using TCP/IP), users gained autonomy on finding and applying the information found on the Internet to act as they chose. A variety of applications destabilised current economies, because they provided a market with smaller costs. While peer-to-peer technology enabled illegal media and software to be freely distributed amongst users, positive changes like e-Markets emerged to provide cheaper and faster services to broader (international) audiences.

Currently these three opportunities to broaden the public's IT knowledge are freely offered. Yet, despite the prevailing role of this technology in our infrastructure, users have not yet been formally educated in dealing with such important issues. This is crucial as a small mistake could not only cripple a sector or region, but also have intangible consequences for other sectors. In doing so, it would also be important to add a tentative requirement:

i. Incorporate *whistleblowing* mechanisms for cyber incidents. As in the present day users are astute in exploring and finding vulnerabilities in the ecosystem, there should be a sound protocol, which enables the largest stakeholder group to contribute to protecting cyber space. This contribution also enables this stakeholder group to report when other authorities or individuals are a threat to cyber space due to their actions. It also allows them to gain more importance by looking at the presence of sufficient checks between levels, and allow them to report these to higher authorities if this is not the case.

3.2.2 Organisational CySec methods

Comparative studies match different standards to certain (non)technical characteristics. By analysing these studies, a summary can be made of what each standard focuses on ((Höne & Eloff, 2002) (Heasuk, et al., 2010)). The authors of both comparative studies show that even in the early growth stages of IT security, none of the standards covered all the grounds or characteristics. Therefore, none of the standards had a specific and unique approach to tackling IT security issues, through the use of certain combinations of characteristics. Looking at the preceding versions of BS7799, BSI, CobiT, GASSP, GMITS, ISF's Standard of Good Practice, CC, ITPMG, DITSCAP; all standards concentrated on a particular aspect of security to the current general library. This current general library has become the ISO27k family and ITIL.

We note that the focus has given away from a specific application to a general library. This library contains all the information which is available, but needs to be customised to fulfil a specific need. In turn, a 2008 study by the IT Governance Institute and American Office of Government Commerce showed that although each framework is utilised, none of the topics can be covered. Thus, *harmonization* needs to take place, which will combine three different standards to get a perfect pyramid structure for IT service management. These standards that need to be combined are: CobiT v4.1, ITIL v3, and ISO/IEC27002. The same trend is also seen in developments of added topics to the most frequently adopted industry standards (ISO27k, ITIL, CobiT, ISF Standard of Good Practice). This is because best practices are being included to reflect on new industry trends. Cross-sector collaboration, from committee-only development of ISO to ISF which grows through member contribution, is taking place. This is intended to offer new insights, and within industries hierarchies are taking place. These hierarchies will encourage the development of expert knowledge.

In the section below general requirements are presented, which are derived from the comparative studies. These requirements intend to reflect common goals for organisations to develop a mixed guideline (Höne & Eloff, 2002; ENISA, 2012; Heasuk, et al., 2010):

(4) *Allow organisational freedom to implement a unique vision for incorporating IT in (non-profit) business*: in certain aspects, each of the institutions should be allowed to choose its own direction. This is because whether or not a company meets its future responsibilities, it should still have the freedom of being able to choose how it reaches its goals. Yet, there is a pitfall given for most integrated frameworks in the preceding 2008 comparative study. This shows that while certain surveys recommend a change in a situation, it does not necessarily mean that a company should follow standards and/or best practices within their industry. They should not follow these guidelines when it is not relevant for their own developmental path.

(5) *Promote the combination of different methods for a harmonized outlook*: As we see in the aforementioned section, certain models focus is on a small given section of activities. This is generally within a given scope, but is different for each institution. This difference depends upon which sector and strategy they choose to implement, and it is logical to combine and apply parts of many different general standards. The trend analysis (Chapter 2 and 3.1) shows that certain standards (such as CobiT v5 includes some new models, but most of which are made by its own industry) follow only a thought pattern that has been active in the industry for quite a while (tunnel vision). An example of such a standard is CobiT v5, which includes some new models. However, most of its models are made by its own industry. To counter tunnel vision, a more holistic approach can be formed to diversify the perspective. However, currently there are no sections that emphasize how these perspectives are to be implemented.

(6) *Cater to specific needs*. These needs are catered to by providing detailed implementation plans instead of general, overlapping methodologies. Different standards, guidelines and/or best practices could be selected, all depending on *what* should be done (technical: ISO27k, CobiT) and *how* it should be handled (managerial, ITIL). As the offerings and strategy of a company differ from its competitors, so does its application of employing certain characteristic guidelines to make its own IT model. Currently, methods offer an array of generalised topics, yet none provide detailed implementation.

(7) *Provide information on development through various stages of maturity. This information is necessary to interact with different actors within the model.* The demand may shift between the need for technical or non-technical. This shift could vary after reaching or growing towards a certain level of maturity. In turn, if the results of being included in a collaboration led to a change in roles and responsibilities, then the long and short term plans should also be flexible as well. This includes taking changes in planning into consideration. It is thus important to have incremental changes and check-ups to assure that a path is followed. It is also necessary to check that the changes in following certain frameworks are meeting expectations.

3.2.3 Industrial CySec methods

While the previous standard touches upon factors that are important for an individual organization, domain-specific institutions often collaborate together. These institutions need to meet certain requirements in order to operate in a given environment, e.g. government-employed firms must have regular security checks. This is also vital considering the influence it could have by being a chief authority, yet allowing its members to contribute. Therefore, it is of consequence to also include this important level for an integrated framework, where in the domain-specific level different organisations from the same industry can meet. Here they can also discuss trends and developments, which are important for their activities.

In the Netherlands, banking institutions have a joint platform. In turn several examples of academic partners can be found, who schedule a periodical meeting in order to note developments and plan future endeavours. Following these examples, it is noted that certain standards also have taken this into account (e.g. PCI DSS for payment industry, Sarbanes Oxley standard for banking in America). It has also come to our attention that this might improve tooling and trend development within industries. This is within those industries, where benefits could be obtained for creating a (de facto) standard.

By observing domain trends in certain IT sectors, the following requirements have been noted:

(8) *Enabling a self-organised authority to look into official industrial matters (autonomously and objectively)*: currently, most industries work on a de facto basis or have a very formal committee which looks into important matters. The idea is to combine both types of organisation and create one central committee for each industry. This central committee will not only decide on important matters, but can also - on a voluntary basis - assign roles and responsibilities to its members. It can also publish their reporting on a periodic basis. Subsequently, this team can consult higher (inter) national parties when problems occur. These observed developments can be shared, depending on the specific interest of these higher parties. By sharing their observed developments, a broader spectrum of monitoring is covered. This spectrum of monitoring offers a platform, where the findings could be compared and related in a cross-sector, (inter) national manner.

(9) *Allow a platform for mutually accepted standard for industry by allowing contribution from members*. By working together, all actors can contribute to points, such as creating an industry maturity model with experts working on best practices. Thereby, these actors help establish a stronger, more secure environment. This involvement will perhaps also allow new innovative methods to be shared with its members and further development to be sustained. This is done by creating a niche and observe its developments to see whether it can prove to be beneficiary for other parties in the same sector. Presently, complications arise because power-play and connections allow a certain method within the industry to gain foothold.

(10) *Promote collaboration efforts to expand knowledge.* This is done by pooling resources, so that organisations can work together to look into incidents. By assessing industry-related incidents and their impact on different firms, it could be easier to determine effective solutions for known or unknown problems. Subsequently, by joining financial assets, larger (long-term) projects can be funded that could improve entire industries. An example of such an improvement is a new form of infrastructure, or a method to improve processes.

3.2.4 Cross-sector/ national CySec models

The most common form of these guidelines can be found in international contracts concerning laws and regulations. In turn, having official cross-sector operators can improve the nation's initiatives to have a national cyber-security centre (such as the Dutch NCSC). In these centres public and private partners from various sectors can meet on a joint platform. Additionally, these partners can discuss trends with the associated roles and responsibilities that come with it. As noted in the previous paragraph, governments are slowly rising to the challenge of creating their own national security strategy. This is due to issuing their own national standard that needs to be upheld. Countries within Europe, such as the UK and the Netherlands, work with public-private partnerships in order to collaborate jointly in securing cyberspace. In cyberspace, companies and law enforcement work together to solve cases.

However, the US has a different approach altogether and takes the lead in protecting its critical information infrastructure. In the US it is mandatory for companies that want to operate in their country, to meet certain requirements for each sector. As each country defines sectors differently and operates its cyber security operations in a thoroughly different manner, it is decided to determine crucial factors by recommendations of multiple organisations (NIST, NATO, ENISA) and published experts (e.g. Dave Clemente, Alexander Klimburg).

From these sources we identify that cross-sector national parties mainly focus on the following:

(11) *Enable methods to specialise in preparing an inventory of various cross sector capabilities.* Here it is important to note what to improve and gain a firm understanding of the assets in the country's vital information infrastructure.

(12) *Democratically determine strategy of a nation together with (long- and short-) term priorities.* This is in order for all parties to partake in jointly securing cyber space. Subsequently, it should be possible to involve various sectors when making a list of goals that need to be achieved in terms of securing a given part of the cyber ecosystem. This is vital, as the cyber ecosystem is crucial for a country, as it can also be seen as national subsection of cyber space, so to speak. In this stage it is also vital to determine what the governance structure should be, due to the variety in approaches seen on different levels. This serves to determine what will work effectively when the following steps are implemented.

(13) *Understand which requirements need to be met by which parties*. Due to the involvement of many stakeholders, it is very important to clearly list roles and responsibilities to (non-) members. This is in order to determine the level of participation, which is expected. The level of participation includes certain incentives e.g. economical or benefits in future collaborations or growth in role of national cyber security organisation. Additionally, it is vital to define how periodical reporting and checking is done by various parties.

(14) *Jointly determine who are seen as representatives and how these can be engaged in important activities and decisions.* This is achieved by inviting important members from each industry's chief committee. Yet, non-invitees are also allowed to participate in formal sessions, to draw out knowledge and fuel progress. By assigning a specific role and responsibility to each key player, these can later be fulfilled during divisional meetings with industry institutions. Additionally, these roles and responsibilities can be filtered down to more (non-) technical tasks. Furthermore, participants may contribute and achieve goals that they find important through voting or following the listed priorities that need to be met. This allows these participants to encourage the role of being a self-organised democratic committee for cyber security.

(15) *Establish trust mechanisms.* These mechanisms are established by identifying threats and vulnerabilities, but also by organising meetings to expand knowledge and involve participants in plans. By providing transparency for parties, members are encouraged to contribute and share progress and/or knowledge. This progress and/or knowledge is obtained through their individual event or development detection centres. Encouraging public-private partnerships to take place on a secure platform will also help achieve a higher level of trust. This is because both sectors employ different methods and combining their approaches will help triangulate efforts in a more efficient manner.

(16) *Check whether all parties understand why and when compliancy is achieved or needs to be improved (research and experiment).* This involves periodic checks to ensure that not only approach and plans are followed thoroughly, but also whether it improves efficiency by being implemented. Often plans need to be tried out first before ensuring success, especially in novel areas. This in turn will help create public investment in resilience when involved parties can choose to contribute or look into different ways of improving a certain part of the infrastructure. Additionally, involved parties gain experience in collaborating with other parties on a higher (national) level.

3.2.5 Global CySec methods

In order to have a clear objective for taking action on cyber security at a global level, the idea is for all standards to be integrated and governed by one party. Yet, it must be considered that each sub-layer follows their own method of implementation. For the purpose of this thesis it is proposed that cyberspace should be seen as a giant virtual plane, similar to air and ground where certain agreements had to be made. These agreements are in order to establish a proper code of conduct and responsibility over a given task. The ultimate goal would be for all nations to properly work together side by side, where all parties (public, private and individual citizens) partake in actively providing a healthy and secure environment, which prevents cyber activities from taking place.

Currently various nations do work together on a global level, yet this is only limited towards membership in certain organisations. For example, there are organisations for European countries only, or in NATO where the focus is on military operations. The ultimate goal would be to have an international committee that not only promotes, but also provides a platform where multiple parties can work together. Similar to the NATO, the idea would be to create a United Nations Cyber Security Council that would bring together all national (and cross-sector) parties. This council would focus on overcoming issues based on separate borders and/or government styles. Examples of government styles are the Anglo-Saxon model used in US, which is in contrast to the Rhineland model used here in the Netherlands.

Having this joint committee is also a logical step if all countries need to be made aware of the dangers lurking for national infrastructure. It is also a logical step for reporting to a central authority that provides roles and responsibilities for each nation to note and take care of. This reporting can be done not only in times of crises, but also to maintain a healthy ecosystem. An example of a noteworthy crisis is the series of Estonian cyber-attacks, which could have severely affected the public.. In turn, by publishing for and being reported to by multiple nations will increase the central authority's public appeal, and create more awareness about upcoming activities and incidents. It could also work in creating interest for outsider parties to read and partake in meetings, e.g. offering more voluntary help for the global organisation.

(17) *Overcome border problems on one common platform.* Ideally, we see that there should be one party available, who will be able to govern all nations. This allows for provision of a platform where issues regarding international collaborations can be resolved. Due to the interdependency, all parties need to work together. However, when conflict occurs, there should be a central committee all nations can address to remain neutral and solve these problems. Yet another, perhaps better, solution would be to democratically vote and determine which representatives could come together and work within the multi-level governance panel. This panel could offer input from different stakeholder types across cyber space. These types of stakeholders may or may not have seen changes happen or take place. This solution would be better due to its setting in a dynamic environment. Additionally, it is a complex problem to solve.

(18) *Provide international governance in order to set objectives and rules and responsibilities on a global level*. This step involves setting an agenda for actions that need to be taken for a global healthy cyber ecosystem by various nations. These actions may vary, as the maturity may differ. Thus, a regulating party is needed to share and improve conditions for those who are still in the beginner's phase of development. Additionally, trust in this establishment must be gained to allow nations to share non-confidential information about further developments. Trust also aids in planning improvements in global efforts across border to secure public resilience. This is because borders have disappeared on the virtual plane due to interconnectivity.

(19) *Promote one idea for awareness on cyber activities between different stakeholders*. Currently, all nations have different views on what needs to be achieved for their own part of the critical infrastructure. However, in contradiction to a passport, not many countries have set basic guidelines for users regarding their interaction on the vast virtual plane. Due to differing focus and varying societal influence, it is therefore practical to have one central party publish international reports and trigger different parties to agree upon one definition. Promoting this definition will help coordinate public interest for awareness. Yet, this requires all actors to agree upon what is seen as activities, roles and responsibilities regarding securing cyber space.

The final paragraph aims to show how these general requirements are formed into design solutions.

3.3 Answering (sub) research question 2

From the previous paragraphs we observe that both fields have different approaches. This paragraph summarizes and answers sub-research question 3 in 3.3.1. Paragraph 3.3.2 then addresses research question 3 and 4.

3.3.1 How CS methods differs from IS methods

From the method analysis of cyber security, we see that more stakeholders need to be addressed than simply organisational, industrial and national stakeholders. Hence we use the five structures mentioned in 2.2 and 3.2. In information security, we see that only technology and business process are at hand for influencing topics for security methodologies. Yet, recent historical and organisational developments show that even more levels are present due to the introduction of the Internet.

The problem of governing cyber space thus requires more collaborative effort on various levels as resources are now inevitably joined. This being joined of resources leads to interdependence and interconnectivity. It also means that interaction and activities should be communicated to other parties that are active on the same level (and if it is a committee, higher or lower levels to partners might need to be informed). By combining current efforts with newly spotted trends, a globalised cooperation with distinct group of stakeholders can be identified. These newly spotted trends range from harmonisation of the model to conducting analyses to identify maturity models. Additionally, in this globalised cooperation each level acts differently. While some of the trends hold, others need different solutions. This explains the need for a multi-level approach where each type of stakeholder has a general model to explain interaction. Yet, this interaction must be within a level, which has different focal points. This is illustrated by the requirements in 3.1.1 till 3.1.3 and 3.2.1 till 3.2.5.

3.3.2 General idea obtained from requirements

The ideas obtained from the requirements (or req's) are quite general to a certain extent. Therefore, in this short section, we illustrate how the generalised requirements can be further expanded. This can be done by expanding into definitions and possible solutions for a model in the following table.

General requirements	*Definition & example*
(1) Education on IT risks	Due to the global nature of cyberspace, it is only natural that the users are expected to be treated the same everywhere. In order to overcome (inter)national issues, a clear idea must be present on what the roles and responsibilities of individual users are in cyberspace.
(2) Raising awareness	Following up on common approaches, illustrated in req. 1; the idea for raising awareness is to give cyber security equal importance. This is done by giving it a special reference through campaigns and active pursuit, which will result in sticking this issue to its current status.

General requirements	*Definition & example*
(3) Provide tools and tutorials to safely explore cyber space.	Just like education (req. 1) and awareness (req. 2) is needed to provide cyber security for today's public; tools and tutorials will provide a voluntary reference set. This reference set is available to all users who want to actively stay alert and be guaranteed of a free (albeit standardised) tooling kit that provides for basic safety to act in cyber space.
(4) Freedom of implementation	Currently, best practices (such as frameworks and standards) are either partially compliant or require mandatory follow-through. The methods are quite general in what is required to secure an organization. This is why this requirement is important to test and adapt multiple standards. Adaptation illustrates whether industry or practical methods work best for an organisation.
(5) Promote harmonizing different methods	As argued in req. 4, the combinations of best practices would help organisations personalize and match different combinations. Subsequently, these combinations use the large availability in the field of computer, information and cyber security.
(6) Ability to personalize methods	General standards seem more popular to determine the level of maturity. On the other hand, best practices seem to be more frequently adjusted by actors for specific industries, e.g. case studies. This shows that by combining and personalizing methods more meaningful feedback for organisations is provided on how preferred methods can be complemented, and how examples from other industries can be used as well.
(7) Guide interactions between different (mature) actors	Similar to req. 6, guidelines should be in place to help different types of actors interact and develop throughout their relationship. This will enable feasible roles and responsibilities, as well as activities to direct their efforts towards the same cause.

General requirements	*Definition & example*
(8) Create a self-organising entity	In order to enable actors to work together, a multi-level committee must come together. This committee will collaborate together, in order to create some form of discipline. It will also serve as a platform for all actors to come together. This is similar to the example given by industries, as they established an objective committee to look over different organisations. Each of these organisations has different strategies and implementations to govern and support their members. Fortunately, this is also the aim of this entity for cyber space.
(9) Enable (and eventually establish) mutually agreed upon guidelines through member contribution	In order for req. 8 to agree to be in each member's favour, some industries mutually agreed upon guidelines and/or approaches. Ideally, these guidelines and/or approaches should be established first. By doing so, the idea of how to work in a network shall also be clearer for all actors. This will also allow them to adjust to their roles and responsibilities accordingly, as they know what is expected.
(10) Pool resources and knowledge	Similar to req. 9, it must be allowed for members to not just offer contribution, but also enable them to share resources. Additionally, they should also share knowledge to allow closer collaboration. Furthermore, this allows them to learn to manage, when resources are limited. This is specifically relevant when these resources might be adequate if they are joined together.
(11) Catalogue resources and capabilities	For collaborations between sectors (across national levels) to work, it must first be established what is available. Additionally, an inventory must be made on what needs to be worked on. This inventory can also be done on a lower level, through req. 10.

General requirements	*Definition & example*
(12) Create and share (long and/or short term) strategy	For multiple parties to work together, a common strategy must be developed and jointly adjusted to fit everyone's need. Only by promoting a suitable guideline can all parties be motivated to work together on protecting common resources.
(13) Understand what actions are mandatory (and not).	For parties to agree on terms, it is first important to decide what terms are crucial for success. Additionally, it must be decided what activities can have a lower priority in order to move in a common direction.
(14) Jointly agree on tasks and actions	This requirement creates an understanding between all parties, which allows for more transparency. It may also aid in breaching problems when things may (not) work out, thus also allowing for improvement. By jointly deciding, more actions can be allocated and/or determined to be met.
(15) Establish trust mechanisms	With so many parties working across industries, common agreements on what can (and cannot) be shared should be determined. Additionally, room for trust in the system should be allowed. This will acknowledge issues and problems to be important, when these are addressed or shared in a joint platform.
(16) Create and understanding of why certain formal agreements are in place and why they are used	In order to prepare some form or process control, certain formal guidelines should be present. They should also be explained to all parties involved, so that it is clear how and why they are in place and/or used.
(17) Show that problems can be overcome on one platform	Create importance for all actors to share and work together. This can be done by proving and reaffirming the effectiveness of sharing. It also involves solving issues in a joint platform to encourage future use.

General requirements	*Definition & example*
(18) Provide international governance	As cyber space reaches across borders, so should its approach in dealing with issues expand across formal borders. The issues addressed by actors show that there is a need for an entity which encourages trust between nations, allowing for sharing of resources and jointly tackling problems.
(19) Compose one general definition to promote cyber security awareness between levels	Right now, each stakeholder group focuses on informing and educating their peers. However, a common education program and definition would be more beneficial, as cyber space can be freely used. This would make it much clearer for all global citizens who use the cyber ecosystem.

Viewing these key issues, we move in the next section to see how experts deal with these issues. These experts discuss how cyber security, methods and issues for collaboration are defined within the Netherlands. In chapter 5 we design a model with the insight from both analyses. In section 5.4, a comparative study is provided to see where theory and practice match and what points are feasible for future studies.

Chapter 4 – Experts' view on cyber security collaboration

In this section, we ask thirteen experts from the public and private sector how they experienced the changes from the field of information security to the new era of cyber security. Based on the developments they saw, this report can help identify a more practical, and perhaps pragmatic, approach to how different perspectives can be resolved into a model. The data obtained from the empirical research aims to answer the questions:

What do the experts see as key issues regarding cyber security collaboration?

First, we briefly touch upon highlighting the key findings of the interviews for issues addressing both information and cyber security. The chapter is concluded by insights and recommendations the experts feel are vital. This results in a harmonized framework incorporating both reactive and proactive measures or a completely different result altogether.

4.1 Introduction and conduct of interviews

For this qualitative research expert interviews were conducted with people who have experience working for both governmental and/or commercial (collaborative) institutions. These experts are also closely involved with the analyses and measures. These analyses and measures concern the managing body of the organisation's approach towards cyber security.

Their insight into development might prove fruitful, as we get to test our development taxonomy. This is a taxonomy concerning information security, the different fields involved and certain characteristics that have been included within a method. These types of information; provide an essential stepping stone when both theoretical and practical insights are combined into recommendations. These recommendations serve for designing and setting up guidelines for future (improved) cyber security controls.

Each evaluation or discussion is done using *the Delphi method*. This evaluation consists of interviewing field experts in a semi-open interview. This interview is conducted to obtain (un)biased opinions on the findings of the report. This method also stresses the importance of leaving room for re-checking certain points or asking for examples when certain topics need more elaboration. The results of the discussions and further topics are also evaluated in the section on *future developments* in this thesis.

To prepare each of the experts beforehand, a short summary of the research was sent. This was sent with a confirmation of the interview date. As the interviewer, definition lists and case studies were examined. Additionally global (Google) internet searches on articles and background information were conducted regarding the expert's work in the field of IS/CS. This resulted in an estimate of what answers could be given, and in turn, provide some examples to look at during the interview. These examples would serve to highlight what may or may not be interesting with regard to their activities. These activities were in terms of designing and making (internal and/or external) standards and/or policies within the organisation.

The first stage of the interview was to determine whether the expert agreed on the definitions used in the thesis. The next stages involved checking whether the expert was familiar with the standards and frameworks. Additionally, it was observed which standards and frameworks were used for their own internal models[2]. As ten out of the thirteen experts had worked for at least ten years in the field of IT security, it was logical to assume that they could elaborate on the development and use of the IS definition rather than CS. In turn, most experts also provided follow up documents to look into complementing or occasionally conflicting information. This information was concerning the developments and organisations they found leading the discussion on security standards, and this new data was also taken into consideration.

4.1.1 Interview structure

The main queries asked during the interview can be devised into two categories. The first group contained 'general idea' questions. These questions were quite open to gain insight, whilst 'follow up' questions elucidated these general ideas. The fifteen questions posed to the experts can be found below.

As mentioned before, the first group considers theoretical concepts. It is discussed in the subsections of 4.2; as it answers:

1. Do you agree with the proposed definitions for separating information security (InfoSec) and cyber security (CySec)?
   Definitions from various sectors are discussed in 4.2.1.
2. How do you see standards? And frameworks?
   Expert insight on this topic is dealt with in the sections 4.2.2
   a. (follow up) Which standards and frameworks are used (or consulted) in your organisation and why?
      The details can be viewed in tables A and B from section 4.2.2

The second group of questions investigates what underlies both perspectives. The focus in this part is if experts see a difference between proactive and reactive thinking. This is discussed in detail in section 4.2.3 of this report. It answers the following questions:

3. (general idea) Do you recognise these methods as reactive[3] methodologies?
   a. (follow up) Do you think cyber security is moving towards proactive[4] thinking?

---

[2] ISO standards are often used just as a guideline and can be partially compliant. Hence, the research conducted in the previous section was noted as quite important. This is because this preceding analysis helps establish an understanding into how the internal model functions in terms of security. This analysis is done for each of the 8 different organisations.

[3] This is based on risk management methodologies. Thus, risks are first organized based on which action is predicted. This means it is based on long-term goals, strategies and priorities. Here plans are taken into consideration and the time to react is somewhat longer than the adapt/attack mindset.

[4] The time to react to incident is relatively shorter. This is because there is no predetermined step-by-step plan. As this planned approach might take days which is unfortunately unavailable during incidents, adaptive thinking used in crisis management is encouraged to allow multiple actors to swiftly come to a decision.

This question will be answered 4.2.3, which will mainly focus on how the public sector will contribute.

b. (follow up) What measures do you think would encourage changing the current information security mind set?
Specialists from the auditing are more active in this discussion, and will answer this question in subsection 4.2.3.

c. (follow up) Is the necessity to have a detailed long-term planning necessary for cyber security? Or is it also acceptable to adapt on short-term, but keep the long-term goals in check?
Due to questions raised on important issues, it is important for both sectors to see whether CySec focuses on short-term or long-term. Additionally, it is important to see how these changes are handled. The answer to this question is found in subparagraph 4.2.3.

The third part of questions illustrates the important components from proactive thinking. Additionally, it shows how they still fit (or are partially) present in InfoSec.

4. (general idea) How do you envision the future of an effective cyber security measure?
    a. (follow up) Will it be proactive or reactive?
    Both questions (general and follow-up) are answered simultaneously as both public and private have different ideas. This is an assumption, based on their different approaches for securing IT. Summary of results can be found in subsection 4.2.4.

The fourth part of questions investigates ideal ways to combine models:

5. (general idea) Do you think standards and frameworks can be compiled into a proactive or reactive measure?
    a. (follow up) Could you name some problems and recommendations on how to combine standards and frameworks?
    Both questions (general and follow-up) are briefly discussed, as to see how the 'gap' between the current view and future outlook is experienced. It also acts as an introduction leading up to the final recommendations of the succeeding subchapter. The answer can be found in chapter 4.2.5.

Part 5 looks at future developments, and is explained in chapter 4.2.6. Here, the following question is answered by experts, who provide seven solutions for future changes.

6. (general idea) Looking at your area of expertise, what are you currently looking into that would be interesting for the future of cyber security?

In turn, when conducting the interview, the following guidelines were set in place for the interview to resemble a conversation:

- Greet each other at the start of the conversation and give a brief *introduction* or *background* of previous conducted research. This is to shortly explain the purpose of thesis. Additionally, it acts as an introduction to let the expert know where his insight and experience could add to explore both fields of interest in 10-15 minutes.

- Walk through the topics (standards, frameworks, reactive vs. proactive approach, future trends and developments) mentioned in the questionnaire.
    - This includes conducting a 'warm up' session. This session is firstly to understand the experts view on definitions, and secondly to gain some (off-topic) insight. Additionally, the semi-structured approach is followed, having kept a list of questions and tables aside, as it would be easier to ask questions and tick off certain topics if pauses occurred. This adaptable approach, following the flow of the conversation, would help quantify the experience working in the field of cyber security and help gain insight into the topics.
    - However, to keep some track of the answers, ask the expert during the last 15-20 minutes of the interview to fill the questionnaire form and/or answer the questions once more. This allows for their rewording of their own answers from the previous rounds.
    - Finally, utilising case studies an answer can be highlighted or illustrated if the analysis is misunderstood. It is also possible that there is need for some more clarification.
- End the conversation by thanking the expert for their valuable input and assure them of a follow up if it is deemed necessary.

The duration was an estimate of 90 minutes as proposed, so as to converse freely without taking too much of his or their time. Switching between various areas of interest (standards, frameworks, models, and case studies) would help keep the conversation flowing, were it to come to a standstill.

4.1.2 Sample size of interviewees

Experts were chosen from a variety of fields. At the start of the Delphi phase, it was decided to interview five to eight people. However, fifteen people were approached. This was because some answers seemed insufficient and the categories standard-frameworks and public-private were insufficiently covered. This was due to inclusion of highly specialized experts in the first phase, with little overlap between categories. From this sample, twelve experts responded to the request. Additionally, two experts were tentative, but unfortunately dropped out due to scheduling conflicts.

An overview of the twelve interviews regarding specialities and insight into specific topics is shown on the next page. These specific topics offer insight into *experience with standards or frameworks,* discussed measures in field of *information security or cyber security in detail,* followed by experience in working with *public and/or private institutions.*

Interviewees with their specialty of the public field offered their expertise in national cyber operations. This varied from Dutch department of defence or DOD, to the national police. Additionally an IT security expert from a medical centre and the IT security manager of the TU Delft were consulted. This served to balance the specialists from governmental institutions. It was also vital in noticing the difference between the levels of cyber governance. The other group of specialists offered their view, coming from a commercial perspective. These were all specifically from the banking and auditing/advisory sector. The common factor was that they all, with one exception, had a technical background. Furthermore, they had often worked in cross-sector collaborations. These collaborations ranged from internally to externally, and were within one or multiple organisations.

Table 1 Experts vs. expertise

Expert w.r.t. background and interests	***Standards***	***Frameworks***	***IS***	***CS***	***Public***	***Private***
Senior advisor at the Korps landelijke politiediensten (the Dutch National Police Services Agency) • **Involved in (inter)national public-private partnerships regarding information/cyber security**	x (gov. framework)	x	x		x	
Partner at the Identity, Security and Risk Management department (ISRM) at Atos Consulting and Technology Services • **Involved in ISACA (CobiT) development committee**	x		x		x	x
Cyber Competence Lead (Manager) of **ISRM unit at Atos Consulting and Technology Services** • **Also worked at the Dutch Department of Defence (DoD) as an internal auditor**	x		x	x	x	x
Security Principal, Technology Risk **Atos Consulting** • **Works actively as a Risk Management auditor in telecom industries**		x	x		x	x
Full professor Cyber Operations and president of the exam committee of the master Military Strategy Studies; together with PhD candidate at Dutch DoD (supervised by prof.)	x (military doctrine)			x	x	
Information Security Manager at the TU Delft / Shared Service Centre ICT • **Insight into conflicts in value chain and outsourcing**	x		x	x	x	x
Security Architect and ADICT Staff Operations, Academic Medical Centre of Amsterdam • **Worked with NCSC, academic MC initiative**	x	x	x	x	x	x

Expert w.r.t. background and interests	*Standards*	*Frameworks*	*IS*	*CS*	*Public*	*Private*
Head of CSC's Dutch Cybersecurity Consulting branch **Addressing technology value chain issues**	x	x	x	x	x	x
ABNS – Senior IT Auditor at the ABN AMRO, • **Primary focus: internal audits** • **Technical background (networking)**	x	x	x	x	x	x
KPMG – IT Security Professional at the KPMG IT advisory organ (regarding Information Protection Services) • **Advisor for multiple organisations (NSCS, ECNS, Telcom, ISAC)**	x	x	x	x	x	x
ABNJ – Junior IT Auditor at ABN AMRO • **Using his IT, economics and business background to look into cybercrime**				x	x	x
RB – Continuity Manager ICT Operations at Rabobank Utrecht • **Insight into interdepartmental collaboration and high level governance**		x	x	x	x	x

4.2 Expert's view on key issues

While comparing expert's thoughts on important issues that we needed to consider for cyber security, we found that there was a vast difference in five categories; as explained below. First we found a difference of opinion in definitions and boundaries of the fields within information security, which is explained in 4.2.1. As experts have unique experiences, they thus identify different theories that they feel are relevant. Moreover, these experts then use these theories to motivate their choice for appropriate models, mentioned in 4.2.2. In turn, the way they adapt models within the organization is also different. An example of this difference can be found while assessing issues such as the familiarity and applicability of the given model within their field of expertise. In turn, the vast differences within the immediate environment is seen to be a main factor that shapes. Additionally, this changes the way security is applied within a field, as shown in 4.2.3. This change is also reflected in the way tools, thought processes and problems are identified by various experts. For example, some might see a problem other fields do not find important enough to follow through upon. The second last section, 4.2.4 shows which short term initiations help move towards the direction we identify as cyber security. This is because these initiations move beyond the individual scope and try to address the systemic risk of cyber space. Finally, we see seven changes that experts identify as important steps in the last paragraph. These first need to be worked out, before different actors can work together and jointly address cyber space.

4.2.1 Difference in IT definitions

The most important difference between the interviewees was that some had reached an agreement on a pre-defined (internal) guideline, while others had not. These agreements served to determine the boundaries for each subsector. This was done in an enormous field, which also needed to match the roles and responsibilities accordingly. Specific industries such as health and banking currently look more towards (inter)national regulations to plot their envisioned growth. This is opposed to the past, where standards and/or frameworks were precisely integrated into their internal models. Their intrinsic preference to roadmaps and maturity models sketches a guideline, which can be used to connect public and private development in terms of maturity.

This subsequently brings us to the latter group of auditors. These auditors also agree on the need for a governance structure, resolving their various disagreements on defining boundaries for subsections. This solution was proposed by jointly discussing how to reach a particular decision, whilst taking guidelines/qualifications from a certain level derived out of generic solutions into consideration. This stems from their difference in use of best practices, industry regulations and priorities. Yet, some do see the advantages of using or harmonising with other (stricter) standards to improve their own internal model.

Still, few experts from both fields stress that it is best for an industry to first establish its own (internal) harmonised maturity model (for formal definitions). This must be done before moving on to cross-sectorial collaboration. A detailed summary of the four public and eight private sector interviews is given, which highlights a few differences in both understanding and application.

Government institutes, such as police and defence, felt that with regard to cyberspace, there were measureable observations. These observations showed a difference with regard to the traditional information security. From these observations, four phenomena can be observed: cybercrime, cyber sabotage, cyber espionage, and hacktivism. Cybercrime, cyber sabotage and cyber espionage all have in common that they introduce varying degrees of data exfiltration. The measures taken to prevent cyber incidents, are extracted from measures that enforce the traditional idea of the CIA[5] triangle, which is used in IS. Yet, one of the four experts felt that cyber is seen more as a buzz word. While stating this, he was referring to Thomas Red's explanation in his book 'Cyberwar will not happen'.

The unique definition of CS as part of an ecosystem is seen as a good touch, as it highlights the need for collaboration. It does this by being directly related to the social interconnectedness of IT, regarding the vital infrastructure. For CS to work, it should consist of the following four disciplines: IT security[6] (IS), Information Risk Management[7] (IRM) and Information Assurance[8] (IA).

---

[5] Where the three sides of the CIA triangle are: confidentiality (declare that all measures are set up correctly), availability (the aforementioned measures are set up to act at the correct time) and integrity (the measures have not been compromised, and hold up to a predefined code of conduct).

[6] Information technology (IT) security is seen as a part of Information Security, but is solely based on protecting the hard- and software solutions for the physical attributes of the system.

[7] Information risk management here can be seen as IT being part of the organisational risk management portfolio.

However, there is a slight disagreement whether this integration should be step by step or done simultaneously:

Step (1) The need to have technical knowledge (which follows from IT sec),
Step (2) IRM (as IT should be seen as a part of the organisational risk management),
Step (3) Enforced by IA (by CIO from top management who also defines the strategy and prioritization).

In turn, the hypothesis is that it is currently important to have a clearer decision making structure, as this will provide a clear context for technical solutions to be employed. Furthermore, even the auditors agree to this approach. Additionally, this narrow scope helps improve (or shorten) the (reaction) time taken to implement a solution. Subsequently, it provides a solid method to predict the impact of a (counter)measure. Technical knowledge should be supported by the organisation and in turn should be invested in to improve itself. Ironically, this is where the university is one of the few parties who disagrees, as they choose to invest in good outsourcing partners and contracts.

In the CySec field, it can also be noted that institutions are no longer dealing with a linear development in technology. This is because the current situation of technological development is illustrated by using the law of Moore and Metcalfe to demonstrate growth on a logarithmic scale. However, by providing a sound division between task forces and roles/responsibilities, the need to have a common list of definitions naturally follows from agreeing upon what strategies and measures need to be taken in a certain situation. These divisions can be made by e.g. sectorial collaborations, which follow the example that is set by the (inter)national Military doctrine.

The experts stress the importance of first identifying what should the structure look like. For InfoSec and CySec the essence remains the same as it always has been:

- The first priority is to **prevent** any incidents from taking place. This is done by;
- keeping adequate **detection tools** in place. An example of these tools is advanced data analysis, such as the CSC. Yet another example is radical technical measures, placed in the correct spot to measure specific changes;
- constructing the correct **response,** using adequate measures and carefully planning to execute them accordingly. Ideally, it should be instantly effective.

However, in the field of IT security, each company auditor disagrees on the other organisations' use of InfoSec – IRM – IA definitions. This is because they each feel that the incentives should come from a different level in the organisation. (Internal) Auditing experts would rather have step 2 done first to get a complete overview, before applying step 1 and then adding step 3. Yet, (external) multi-actor collaborators feel that it should it go in reversed order e.g. 3-2-1. This is because it is eventually the top management that gives direction in terms of objective and strategies.

[8] Information assurance is the last step in securing IT. This takes place after technology and governance are secured, in order to guarantee that all measures are placed properly. This is done in order to protect the organisation's IT. This protection is done irrespective of its function: be it for a key technology, a product group or the entire value chain that belongs internally or externally.

All specialists do agree that the addition of the collaboration component in cyber makes the term far more interesting than internet or IT security. IT security is the term, which is being used right now, as it encompasses the broader term or different fields collaborating together. For companies it is important to divide their IT according to the value of the chain. For example, telecom, banking for public/private clients and public sectors in terms of eGovernment or citizen services all have different values. Their approach towards securing an asset or part of product group, using this term in its broadest sense, could also be from operations or the department. Therefore, this could differ in terms of methods employed as well. InfoSec is still considered to be a vital part of the internal (governance) structure followed by most of the auditing experts. Their perspective matches the views shared by the preceding field of security, and their existing methods are slowly updated depending on if the communal activities of the interviewer are greatly affected. This occurs after thorough testing because the experts feel that CySec is an addition to what they already have. The essence of security, whether it is called information or cyber, has not changed and nor does changing methods work against unpredictable incidents. Perhaps in the future, by post-analysing bad situations through multiple perspectives, companies can gain insight into what is missing. Furthermore, it is these developments might shape other partners for the better.

4.2.2 Purpose of using different security methods

Experts feel that standards should be seen as common functional requirements, instead of checklists. These checklists imply that they need to be completely followed and fulfilled in order to achieve goals, whilst standards should most importantly fulfil requirements. Governmental institutions still see their operational use as checklists, whereas educational institutions want to connect radical research with system safety. This could be used for example to ensure privacy of sensitive documents and/or data. This allows multiple parties to secure a certain part of the internet ecosystem, yet letting information sensitivity determine the level of protection. This is achieved by using a cryptology example to relate exclusivity of information to the duration of protection measures. Standards can also be used as contracts to determine arrangements between parties and clearly define organisation structure, rules and responsibilities. Thus, these contracts can be used to allocate tasks accordingly.

An example of providing awareness can be provided using De Leeuw methodology[9], which shows the different levels of interaction. Here the three parties; *(1) an environment, (2) the managing group and (3) the managed body,* interact with others. However, depth of knowledge and notification level differs rapidly. Governmental institutions thoroughly believe in this approach, whereas educational institutions have a limited view on this topic. This is because they don't feel the need to burden clients, such as students/doctors/researchers, with a strenuous amount of details.

Awareness is also seen a critical issue by experts. Additionally, they feel that changes are necessary in cyber incident management for operating experts to act quickly. Later on, top management can be informed about actions. This is more productive than seeking permission by going through the entire (existing) structure, especially in severe moments of crises.

[9] This is a reference to (Dutch) Wikipedia page (http://nl.wikipedia.org/wiki/Ton_de_Leeuw_(bedrijfskundige)) on management models.

Frameworks are thus seen as models that are generally used to make abstract comparisons. In turn this way of (in)formal thinking is more often applied in internal models, It serves to illustrate how procedures are played out. This can be done by using more analyses and assessments, such as risk profiling. These analyses require a clearer context before implementation.

Standards can be seen as regulatory guidelines. In some cases, these guidelines are quite necessary for certain industries to meet requirements before being allowed to operate. For example, SOXs standards must be adhered to in the banking industry. In contrast, one can even say that it is better to have many different standards, as this allows a firm to look at what aspects they find important enough to be added towards their internal model. This is especially the case for internal auditors who are in charge of providing technical solutions, and have a model uniquely adjusted for a certain client (or region).

Internal frameworks in turn would be ideal to share, compare and develop accordingly. However, no company would openly distribute their information regarding the changes, as may well be quite a profitable business. It could possibly impact millions, if not billions in revenue. This is also why collaborations are set up to have sector specific changes. In the public sector, (inter)national government enforcement services meet and collaborate on occasion. Likewise, governments at the EU, ENISA and NATO meetings also meet and collaborate. On organisational level, private firms seem to be less transparent. However, changes have occurred across fields. For example, more and more academic hospitals aim to collaborate together. In turn, online communities are being set up for those who are interested, while physical ones such as the NCSC in the Netherlands and the interbank committee have also developed.

The following page illustrates in detail the differences between standard- and framework, in terms of awareness and applicability. This is done to differentiate between public and private sectors as well, in order to highlight the market's preference. Colours are used to indicate special changes or comments for a certain sector. Here, the green colour is used when experts from the public sector share a particular insight. Blue refers to the commercial specialists' opinion. Black is used for combining both data from public and private sector into one answer. In addition, x* shows the most popular answer between the (un)familiar categories. This helps us fill in the blanks, to get an indication which standards or frameworks are used (for harmonising). It can also be deduced by whom and how (by referencing the description).

Table 2 Cyber security standards used in practice

List of standards	*Familiar*	*Unfamiliar*	*Used where and how?*
ISF Good Practice	**X***		Familiar for all sectors, used for trend analysis
ISO27002 (General Code of Practice) to be ISO27032 (Cyber Sec Standard)	**X ***		Partial compliance for each different sector
ISO27005 (Risk Management or RM)	**X ***	X	RM also used in aMC, TUD to combine with other faculties, very popular in private sector
ISO27011 (Telecom)	X	**X***	Managed individually (sector specific, hardly used outside as connected network safety is quite different).
ENISA Best Practices	**X***		Frequently used to update internal model
NIST Best Practices	**X***	X (RB)	Trends/developments
NATO Best Practice	X	**X***	Mostly government institutions who directly dealt with implementing part of the (inter)national cyber strategy (w.r.t. international collaborations)
NIST 800-30	**X***	X (RB)	Familiar from cryptology, used by government
Other standards used	NEN7510:2011 (Dutch IS Health org), Military Doctrine, PCI DSS (Payment Card Industry Data Security Standard) is also used in other industries, ISM3 (Lean Maturity model), ISO 31000 (for Risk Management), SOX (banking industry standard in America)		

Table 3 Cyber security frameworks used in practice

IRM Framework	*Familiar*	*Unfamiliar*	*Used where and how?*
ENISA RM Process	**X***		Trend/developments
ITIL	**X***		Referenced when necessary
CobiT	**X***		Referenced when necessary
NIST 800-30 Framework	**X***	X (KLPD)	Many private clients in USA
Risk IT Framework	**X***	X (KLPD)	ISACA embedded in new CobiT and ISF
INTegRISK		**X***	
PDCA	**X***		Internal model, popular in private sector
OODA	**X***		Monitoring step proposed to be used for (PD)C(A) cycle
Other standards used	SPRINT (cycle), ISO31000 (RM standard, also noted above)		

4.2.3 Differences between fields

In the private sector, we see that experts agree towards the proactive movement. This is because auditors and managers can state many tools, methodologies, and plans that are offered to their clients as products. These managers do this in order to achieve certain IS/CS goals within a given number of years. The public sector uses a different approach, also using service-orientated framework, but more with regard to governing their weakest link. This weakest link is the human employee or client whose vision is limited in terms of time (periodical checks), quality (assurance of achieving goal) and cost (investing in relevant tooling).

Commercial tools

Most experts can see their environment leaning towards taking proactive action, as they do see an increase in the use of current available tools. Examples are the RSA algorithm for public key encryption used in cryptology, which uses semantics techniques to process information naturally. Additionally, LogRhythm is used for (security) log management, and ArcSight for big data security analytics.

Some sectors implement the change faster than others. For example, banks have more data to their disposal, which they get from public and private clients. This opens options for big data analytics and trend analysis to allow some predictive capacity for identifying future (security) priorities. This is also empowering as data can serve as an investment towards backing up design choices, but also guide sectors to look into potential and identifying new ideas. These new ideas can help the firm in the near or far future.

Shift in governance mentality

In this sector, the people who decide to place the technology according to their interpretation of the context, can be seen as the weakest link in the organisational structure. This is because their actions are found increasingly important in considering how to fit IT correctly within the organisation. This is in order for it to be developed properly and checked from time to time.

Thus for effective results, the governance should also be in place and verified. This is to assure that it is indeed correct after a given period. In turn, reports on quality assurance help certify that all is in working order. Though this is periodical and cyclical for a given time range, applying transparency and making use of shorter cycles will help it become agile. Additionally, this will help it to adapt to the rapid technological environment.

By using tooling available for monitoring more carefully, better data can be obtained to prepare in advance for attack. However, all this has to be done whilst staying in line with regulations and honouring the current legislations.

Looking at the news, government institutions feel that the wrong way to create attention is by using the buzz word “cyber” for IT security. This is primarily because it is a serious topic, which has had undue attention in media. For example, as the media currently alerts that any threat given will be an imminent threat leading to a cyber-war. This creates entirely the wrong kind of interest, which in turn might have reverse affects in creating awareness. By explaining why it is necessary and promoting the message responsibly, any annoyance for top management’s sake might be discouraged.

In America however, October is seen as the national cyber security awareness month. Thus, this provides ample opportunity for various stakeholders and groups to present their thoughts on the matter. As it is a joint responsibility to secure our cyberspace, every effort seems to be a step in the right direction. Experts thus say that by in turn being pro-actively protective of individual safety, the national security can encourage overall resilience (DHS, 2013).

However, auditors do think that the awareness which is raised through cyber incidents and publications provide a better argument why management needs to invest in such measures. The same argument from the aforementioned section, which was albeit by the public sector, does state how reporting can be used to an advantage, This is because the measures and investment in new thinking (education, motivation and/or awareness) can cause more people from inside the organisation to vigilantly uphold a high security norm. This in turn aids the cause and encourages managers to look at this matter intently.

Reactive thinking is seen to be based on risk assessments, assuming factors are known to develop long-term plans and encourage thinking about the future. However, as mentioned in Chapter 2; it is impossible for any stakeholder to make reliable plans 5-10 years ahead in time, while technology is moving chaotically and rapidly. To look into actual measures taken, internal development (own technology) vs. external development (increase network value, industrial knowledge) must be considered. Then, it is important to note what governance measures specialists see taking place in their environment. This helps map some level of maturity, as implied in the expert insight on the thesis' theoretical sections in 4.2.1.

Use of issue framing in practice

Short-term planning is interesting because technical knowledge through analysis and monitoring is basically what drives computer emergency response teams (or CERT) and Red Teams. These teams serve in penetration testing and offensive security, which is used by one of the experts to encourage 'crisis' training. This kind of training is used to directly combat such incidents. One of the experts referred to using the concept of issue framing for 'cyber', as working on a hot topic or framing the IT issue as cyber would help allocate a larger budget. This is in stark contrast to the medical sector, where an 'expert' or mentor is always close by. This person serves to educate the inexperienced and resolve any issues regarding crises and/or emergencies.

For example, many sources say that cyber war is coming. Yet, institutional experts see that as an idea that does not differ from the original idea of using malware or data. This malware or data is then used to get or change information. Therefore, governance still plays an important role. Considering the step methods mentioned earlier in 4.2.1, technology needs to be in place correctly and managed (especially by standards) to provide proper governance. Assurance can later on be achieved when it is all correctly placed. However, in order for multiple parties to work together, a system to manage operations must be created.

Awareness and assurance are crucial

Awareness is crucial on for both leaders and followers of cyber policies. For leaders, awareness shapes their cyber strategy and determines this strategy's implementation. Awareness also leads to future support when the InfoSec or CySec department runs out of cash. Additionally, it determines how firmly the rules of security are followed. If the system itself is relaxed and informal, then the correct values can never be put into action. However, when operations and top management collaborate together by discussing critical issues and placing priorities correctly, experts feel that there is a possibility. This possibility is determined by the formal definition for a long and short term strategy, which can help shape a good strategy that is placed in the right context.

In turn, assurance through compliance encourages new and old clients can rely on the expertise of people who check and provide feedback. This compliance is partial for ISO, but full for the sector specific requirements. In turn, moving upwards from reactive styles can help identify what aspects can be identified well before the product group is pressurized in a later stage of development. This reactive style involves planning and prioritizing according to available resources at first, after which resources can be allocated according to growth. This allocation also occurs according to determination of implementing certain measures as a precaution.

4.2.4 Important steps towards a new era of security

In the coming section, the use of PDCA model will be named proactive for risk management and prioritisation. Additionally, the four measures mentioned by Dave Clement were also analysed, while keeping the use of the OODA loop in mind. The main focus was on quizzing the experts on the perspective they used frequently. The results indicated that the private sector had clearer vision of important criteria for each perspective. These shifts were clearer for the telecom and banking industry. On the other hand, the public sector would rather integrate parts of the OODA loop, rather than specific steps recommended by Mr Clemente, in the PDCA cycle. However, choosing just one step or method appears to be problematic, as there is no consensus on their motivation for giving a certain criteria more importance.

Steps towards resilience

The four important factors that affect infrastructure criticality have been discussed, as these are the findings of paper published by the UK cyber security expert Dave Clement. Among these four factors resilience seems to be the most important step for government institutions who have IT as their backbone. This is because the focus is shifting to proper functioning of an organisation, rather than the technical tools that are being used right now (Clemente, 2013). So looking at the recent news; KPN turns out to be quite a pioneer as they have created a new IRM department. This department includes policy and risk management, red teaming and SET. Carnegie Mellon have also published a comprehensive scientific paper about this CERT (computer emergency response team), which consists of a red team (enemy group set up to stimulate attacks) and a blue team (enforcers who try to combat the incidents).

Adaption of model

The experts from various industries agree to design their model, different sections from different methods are necessary. These sections could be standards, frameworks, best practices and/or industry recommendations. As the industry differs quite a lot of examples in terms of variety and size, it is difficult to place a 'one size fits all' solution. This is also a general argument against using a framework or standard. This was because these were originally derived from a good model, which was then generalized and made abstract to a high level. This level was so high, that it could only be referred to once or twice as background information (guideline or checklist), but never applied to its full potential. This also explains why each company has their own internal framework, which is updated quickly and adjusted to the best practices accordingly. However, this internal framework is never published or shown to competition in the same sector.

Naturally some measures (banking, medical centres) are generalized, but not all competitive advantages are shared for the benefit of this research. Experts explained that sometimes secrecy is required, even though it might impede the eventual development of resilience. This is because it also prevents other (malicious) threats from directly hacking into the system, as it then directly knows how internal security is designed.

Effective cyber security measures

Most of our experts do agree that proactive measures are necessary. Yet, an interesting suggestion was made by one of the experts active in the military sector. This suggestion was that to assure that no one attacks your institution, pretend to hand out harsh repercussions and portray your reputation as almighty. Even though this might not be the case, it still proves that effective bluffing is a much cheaper solution than actual investment.

We see that many industries are moving towards proactive measures, as defined earlier. However, the changes (caused by incidents) often occur faster than predicted. This means that new methodologies such as CERT, and Red Teaming would help in taking action immediately. Incidentally, these are also one of the few methods that are currently being backed by investments from the public sector.

In retrospect, even the best measures cannot always prevent activities from happening. Neither can they prove to keep threat levels within limits. Externalities often noted in theories of economics, can be beneficial to some. For example, the PRISM project by NSA, was involved in keeping tabs on everyone. Thus, it could be suggested that cyberspace is thus secured to some extent. Yet, this technique of ensuring safety is damaging towards the (inter)national right to privacy.

Benefits of combining efforts

Investment in technical solutions are done by individual companies and depend on their priorities. Examples of these priorities are e.g. to improve logistics and deployment of these solutions. This investment allows removal of inhibitions or start of initiatives towards public-private information sharing and improving expertise between fields.

For governance, especially with public organisations, strict policies and regulations have been specified to determine which party does what kind of task. This is done without interfering with the citizens' rights, such as privacy. Privacy is a new issue that also needs to be added to frameworks. This thought is well in line with the current petition by Bits of Freedom stating that making a stricter policy should not be done by sacrificing an individual's privacy, as individual security will more than make up for its ill effects. Thus, it will contribute towards a better resilience (Halink, 2013).

Experts from the private sector expressed their gratitude if a few methods could be developed or already be launched in the market. This launch would guarantee that harmonisation of different standards and frameworks still provide a good guideline for all companies to follow. However, due to uniqueness, this seems impossible. A good starting point however would be to look at which standards are being used currently and what measures would help improve them to turn towards the proactive mentality (KPMG, Banking auditors).

Subsequently, it was suggested about risk management also needs to mature for the field of IT before being implemented in such rapid manner. Advisory companies pride themselves in analysing the consequences for a specific client before suggesting radical (or in this case never been used before) measures to secure the virtual domain of a given organisation.

In order to answer the first research question; how experts interpret the development, we see that the interviewees have different opinions about definitions and changes that have taken place in the field of general IT security. Some agree that CySec is a different domain and would require more collaboration; for we see that medical centres, banking and educational institutes already do so with other parties within their industry. Others say that this is a variation using a new interface by using different IS applications for many sectors: showing how some requirements (prioritising, setting baseline and constant maintenance cycles) still occur in current practice and thus remains the same solution for the same problem. What they identify as the main problem is the lack of a clear definition that can help them determine when they can or cannot participate in solving an incident. This shows how organisational sciences also influence this process in determining an appropriate solution for a multi-actor collaboration. In fact, we effectively see definitions such as issue framing, and working together in an arena-like setting. This setting is used in practicing IT security match organisational policy theories, which are mentioned in literature.

4.3 Answering (sub) research question 3

The key issues addressed by experts also vary due to their different perspective and personal experience in the field of information security. For example, some want the structure and interaction between levels to be clear and limited. This is because it is important to have a form of hierarchy in place for a formal outline, in order to get a common idea on goals and definitions before implementation. Whereas others encourage to increase the number of informal meetings and seminars between different parties to create a new platform to share information, as opposed to creating an integrated framework that will allow transparency.

These interviews help determine activities for each sector that need to take place and allow us to identify that the stakeholder types are different. An important finding is that there is a need for general requirements; some issues for example exist in across various sectors. An example of such an issue is who should govern what part of the ecosystem. In turn, we also see differences within the region that require specific types of requirements within levels to address issues. An example is to show differences between the way things are handled within the private sector, because the commercial institutions have many subsectors that each react in different way towards an IT crisis. For example, the energy sector might need more government intervention (prices or allocation of assets) more than IT services for example. For the latter industry, mitigating problems should be left for (sub) level employees who have more insight into technical matters.

Looking at the subtopics discussed with experts in the first four paragraphs of 4.2, we summarize these findings to obtain a list of seven important requirements from practice. The aim is to complement literature's requirements from practice. These requirements have been derived by analysing the detailed interview data from all participants, comparing suggestions made by experts on the changes that could be made on the short-term (5 years) for each sector. This comparison is accomplished by combining contributions from various experts; such as combining the definitions they felt were important (4.2.1) with their association with current models (4.2.2). The expert's motivation for using different tools and approaches (4.2.3) was seen as crucial. This was because this could be combined with remarks made on steps towards improvement, leading to (4.2.4) the compilation of the following requirements:

1 Actors from different sectors stress that an official hierarchical governance model is the main priority. This is because it provides a **clear decision making structure with roles and responsibilities**, across and between different industries. These actors feel that each specialised technical expertise is on par with the developments in the field. In addition, having clear objectives on how to improve knowledge for their individual SET (security emergency team) are examples of progress.
2 Another recommendation by auditing experts is to **focus on trends from other** (disjoint, incident on an immense scale or purely out of interest) **sector** to monitor and improve developments. This is done to include approaches from different methods to provide another perspective. This perspective could help in creating an effective pattern for faster cycles to take place. These faster cycles could be used by emergency response units to detect and react to cyber incidents.
3 In turn, something that is not mentioned is to actively **start peer benchmarking, frequent reporting/publishing and collaboration between various sectors** (as is done in the National Cyber Security Centres or NSCSs, medical centres and banking sector). These collaborative areas are important platforms as planning such meetings will initiate exchange in order to promote collaboration.
4 Use **strategic planning and tactics** as opposed to technical solutions to appropriately deter any efforts of threatening cyber space, making other actors and stakeholders aware of their boundaries. In turn another strategy of **framing problems** to illustrate that benefits concern all. This will not only allow the allocation of joint adequate funding, but also encourage efforts for multi-sector collaboration. This collaboration would be most effective when accompanied by a reputable and powerful player in the industry.

5 **Promote research expanding on exploration into individual domains.** Experts agree that there is a lack of knowledge and coverage of (risk management) frameworks. This is because these were built on preceding measures when IT/technical perspective was central. The measures were taken without focusing on societal consequences, and more importantly, impact on a certain domain. Therefore, this needs to be further explored. Considering, the idea of having a general approach, it is equally important for each sector to have insight into risks, interdependencies and consequences of its IT activities.

6 External auditors all agree that the frameworks in place are quite robust because they incorporate practices from various sectors. However, each stakeholder group needs to incorporate a structure that also decides on what is **relevant for effective measures and governance.** This can be found in e.g. government institutes and the banking sector, due to close collaborations that take place there.

7 In turn, more work and effort should go into **cross-level interaction, determining joint initiatives across sectors.** This is because these interactions and initiatives could really aid efforts towards building better education, awareness, and (social) acceptance. Social support would mean support and allocation of costs. This all taken together would aid in moving towards cyber space and building further resilience.

We note that while seven general requirements will not completely match the requirements we obtained from theory; there shall always be room for discussion on whether these are the right topics that need to be addressed. The following chapter shows how theory and literature can be combined to provide a model for collaboration; addressing the various issues that have come to our attention in Chapter 2, 3 and 4.

Chapter 5 – Designing an analytical model to improve cyber space collaboration

In line with the analysis from Chapters 2, 3 and 4; our proposed solution would be to create a model that *enables us to analyse and improve each level's current security activities, roles and responsibilities. This model will allow them to collaborate with others in the cyber ecosystem,* so that different types of stakeholders from citizens, to firms and industries can come together. This will allow these different types of actors to take initiative and to some extent determine what their own role and responsibility will be in protecting cyber space. Yet, the model should also *provide a formal structure to achieve these collaborative efforts.* This is because this structure is not in place, as experts explain. The structure is much needed for the industrial, national, and global level. This is because, while many domains interact each other, there is no clear cut approach or coordination for these interactions. However, this is seen to be a crucial step in collaboration. Both theory and practice have shown that there is no formal outline yet of how these various parties can come together. This coming together would be on a joint platform, intended for these parties to resolve cyber security issues.

Our idea is to build upon this view and provide a general pyramid structure to govern the different levels. This is ideally done democratically, by allocating the various stakeholder's roles of responsibilities within the ecosystem. Additionally we try to fit the role of an international structure into this model. This model is necessary to govern national activities due to the global nature of cyberspace. In turn, this global nature is to be further determined and fulfilled by the multi-level governance panel, which could involve adding a representative from each sublevel to be informed and undertake action. However, the model shall still enable each stakeholder to apply its anatomy within its level structure, by enabling networks to exist within its structure. This network will enable actors to consult the higher layers of the triangle. Subsequently, this consulting will allow for democratically determining joint vision, strategy and actions to secure cyber space.

This chapter aims to design and internally validate our analytical model. Furthermore, it aims to answer the main research questions for this section, which are:

How would we design an analytical model for cyber security collaboration? And what activities, roles and responsibilities exist between the different levels and/or cyber domains in our model?

The first paragraph provides a detailed approach on methodology. It provides this by explaining how the analysis of the preceding papers contributes to designing a model and what aspects it takes into consideration for designing a hybrid. The second section focuses on how this hybrid structure is achieved, by illustrating our formalized collaboration model. In this model interactions, roles and responsibilities of the stakeholders are given. The last section answers the first research question through a comparative analysis. This is designed to cross-check whether certain sections for the design do or do not match our initial idea gained from literature and practice. Furthermore, it can be investigated why this mismatch occurs. We end this chapter with a brief summary of the key features of our multi-actor collaboration model.

5.1 Introduction to design and internal analysis of proposed model

In order for us to construct such a collaboration model, we use two different theories on modelling multi-level governance. Firstly, we consult Ms. Elinor Ostrom's idea of multi-layer collaboration. In this collaboration, each meta-layer has a different purpose and own approach to the problem (Ostrom, 1990). This theory is also applied in analysing the problem known as *tragedy of the commons*, applicable to certain fields of science. Including the background analysis in Chapter 2, we see that our problem regarding cyber security can also be depicted as a *tragedy of commons*. This is because actors within this ecosystem all tend to secure their section of cyberspace according to their self-interest.

Because it is not possible protect a collective good (in this case the cyber ecosystem) without a collective approach, individual actions with regard to IT security are seen as not contributing to a growing security of the environment. In fact, this only leads to an excess of similar actions taken by each of the different groups of stakeholders, as they all strive to protect their own subsection of cyber space. Ostrom argues that when all these layers come together, they interact as an informal hierarchical model. This is similar to the idea represented by Koppenjan & Groenewegen.

The latter two authors argue that often a problem is too complex to take project-oriented joint action. This is due to differences in influences, which are taken into consideration from various institutions (Koppenjan & Groenewegen, 2005). Instead process-oriented change is recommended for designing a model, because it incorporates different views. Both ideas are key in creating our model, as network settings seem crucial for merging multiple actors together. These multiple actors interact within the ecosystem differently than with other actors (as seen briefly in section 2.2). Conjointly, this also contributes to defining how to implement security in a different manner (as we see in Chapter 3).

From literature we note that there are many governance structures available and applicable to design an institutional model. Yet, in practice combinations can often not be thoroughly tested to identify where the gap lies during the creation of a multi-actor collaboration model. However, as the scope of this research is limited, we have decided to identify the relevant actors and provided an analysis of working methods. These working methods will be in the form of design requirements and provide an idea of interactions that play a large role in enabling multi-actor collaboration.

Literature by De Bruyn and Ten Heuvelhoff was also used to understand the nature of hierarchy and networks. As this hierarchy would be adaptable, the aim is to move more towards a hybrid structure. This structure would not contain any formal or rigid guidelines, in order to retain its plasticity to adapt to the dynamics of our increasingly complex cyber ecosystem. Using definitions identified by these two authors, we empirically studied the application of the concepts and can identify which notions play an important role in designing a multi-actor collaboration model. The problem regarding cyber security matches several definitions of network setting. This is for numerous reasons.

Firstly, this is due to the variety of actors and approaches taken. Chapter 3 can be reviewed for the numerous methods used in both information and cyber security. Secondly, actors that are invited to collaborate in public- and/or private partnerships are able to decide on key issues. This collaboration is due to the propinquity associated to networks. A final analysis of the problem also shows that the interdependence and dynamics are another example of processes in network settings. This is due to the finding that interdependence and dynamics motivate actors to act in their own interests. This last section is also described in the comparison of the problem of cyberspace to theories mentioned by Ostrom and Koppenjan &Groenewegen.

The analysis and model design of combining multiple hierarchical perspectives in a network setting is thus used to emphasize the need for a hybrid structure. This network setting is suggested by De Bruyn & Ten Heuvelhoff. We choose this specific approach, as it bridges two extreme perspectives. This is due to the preference for network settings to link all sectors, as is shown from literature. Yet, experts counter this argument by suggesting a dire need for hierarchy and formal structure.

The combination of the three theoretical models (by Ostrom, Koppejan & Groenwegen and De Bruyn & Ten Heuvelhoff) provide an outline of important issues, which need to be considered when designing the model. This illustrates challenges that need to be checked and avoided if they are outside our research scope. Furthermore, this analysis has also influenced the choices in designing the domains and environment interactions defined in 5.2. Additionally, findings from the comparative model, which serves as an internal validation of the model, have been reflected upon by comparing the key issues from theory and practice.

5.2 Applying design theories in our model

The previous paragraph states the different theories to relate to our levels within our model. The idea was to come up with a hybrid governance model that took both generic and specific requirements into consideration. Additionally, this model had a different focus per layer. The choice of hybrid networking from De Bruijn & Ten Heuvelhoff was selected because our literature study showed a strong inclination towards network setting for integrating different stakeholders. Yet experts would rather have a clear cut decision making entity in place who leads and determines what actions each actor needs to undertake.

Another important outcome of the empirical research is to have governance, which is achieved through an overview of roles and responsibilities. These roles and responsibilities need to be met by five different cyber space domains. This is met by having a multi-level governance panel to oversee whether the security within a sector of the cyber ecosystem is upheld. Additionally, the roles and responsibilities of stakeholders within a given domain must be managed. However, literature showed that due to the interconnectivity on the global IT infrastructure, this framework also needs to fulfil the necessity of cross- and inter-sector networking. Because we provide a high-level design for a preliminary method for different institutions, examples of interactions are also given for each level. This is given in order to collaborate and contribute to the actions of the preceding or subsequent layer.

Existing methods have a comparative guideline on a *national level* (focus of cyber strategies varies per country), *industry level* (different specifics) and *firm level* (different focus due to commercial strategy). As noted previously, none of the literature research counterparts identified citizen or global level collaboration to be integrated. This finding makes our model unique, as it aims to integrate citizen and global level of collaboration. Our key observation is that appointing a *global level* entity to oversee collaborations in the virtual (cyber) space has the highest priority. This is because it currently functions without taking physical boundaries into consideration. Additionally, a global level fills the important missing link that connects and provides transparency on activities across nations. In turn, it also provides an example for institutions to group certain parts of the ecosystem together. This allows them to decide which level to approach in tackling a certain problem, further illustrated in 5.3, which is a case study.

Additionally, cyber security has solely addressed commercial (industry, firm) and governmental institutions until now. It has not taken the growing number of users who form a greater part into account. These users are also (indirectly) approached by all the preceding layers. Our idea is to also include these different institutions to be actively involved as a group within the industry, domain, national and global layer. This is done, because as their individual group's IT security is addressed and upheld, a minimal level of safety is upheld. This is upheld through general requirements for accessing the IT infrastructure which is not covered by the other layers.

The following subparagraphs on framework design shall explain why risk management is imperative for each level. This is mainly due to their separate interests, which also leads to the importance of integrating all views. This is because all views can help achieve in integrated approach. Additionally, a short introduction to the hybrid (hierarchical) model is given. This is given by the following figure, which shortly summarizes the roles and responsibilities of the different stakeholders in each level.

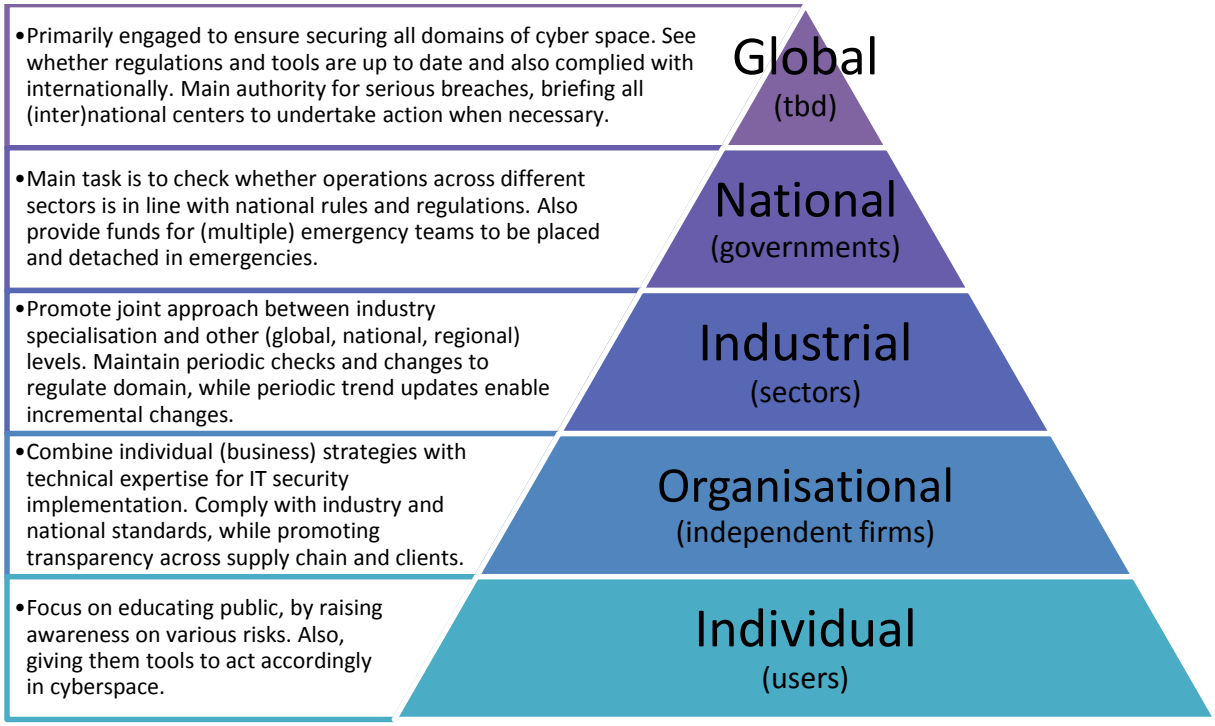

Figure 6 – Multi-actor collaboration model for cyber security.

5.2.1 Defining various cyber subdomains

As mentioned previously in 3.2, standards have originally inspired our outlook for this model. This is because their focus was spread over a broad area. This area varied from being internationally recognized, to including specifics for each different nation and industry. The ISO27k is taken to inspire a methodology, which will be internationally recognized. It also allows for customization on different levels. Firstly, it can be customized by blending its generic framework idea with each nation's rules and regulation to become a national standard. Secondly, it also observed to contain specifics that allow most users to focus on a different type protection, whilst looking across methods used in different industries. This allows for customization, which depends largely on the firm's area of interest.

Starting out our explanation of the figure from a bottom-up perspective, we start at the largest group of individuals. The *individual* level aims to protect the users of the IT infrastructure through their own (mobile) devices. With the growing interdependency of using IT for a number of activities, its importance has elevated in our daily lives. Yet, general knowledge about protection and safety are not taught or equally known by all users. By ensuring a level awareness through education, it is made sure that every person who makes use of IT within the cyber ecosystem has a basic understanding of the risks involved.

The next level is a bit more advanced with more users working together on *organisational* level protection. This level is essential because of the growing use (in varying degrees) of IT to support businesses' core activities. Each public or private institution has its own model and method. Yet, it undoubtedly depends on the specialisation and strategy which model is adopted. This is because the specialisation and strategy give a clear indication of what guideline and/or standard is helpful in building an individual framework. Due to the exponential growth of methodologies used, our initiative for this level is to determine what generic and specific guidelines are considered important for an institution. These guidelines are used to fulfil their part in keeping a certain area of the IT infrastructure safe.

Domain or *industry* level groups these different sized individual firms into one area of interest or one area of operations. The focus is to look at tools and methods that are needed to tackle common problems within their expertise. Collaboration between similar institutions forms an important step to pool their resources. Additionally, by working together matters to reduce large scale disasters are addressed, e.g. Dutch national initiatives taken by banks but also triage in crisis situations. In turn, this will help regulate the operations by experts with the proper expertise on process and operations.

National level collaboration is seen to go beyond the industry boundaries, taking rules and regulations into account. It also provides a regional base for different industries to come together and discuss their problems. Because each region has its different style of governance, cross-sector collaboration on a national level allows parties to come together and shape their joint view. Currently, most governmental institutions are seen to take the lead in this level. Yet, it is our suggestion for each industry's chief committees to have a level of influence which is in line to their roles and responsibilities. This way, parties will be encouraged to share information on a platform and be encouraged taking initiative. At the same time, these parties will be allowing a democratic approach, which in turn will allow multiple parties to determine and provide crucial points on security. These points are essential in maintaining the nation's IT security.

As our current IT infrastructure is going beyond national borders on the virtual plane, this means that a new entity is needed. This entity is necessary to supervise the global IT infrastructure and facilitate issues or discussions regarding cyber security to take place on neutral ground. This is addressed in the final layer, as it is on a *global* level, where a main authority is established that safeguards collaborations across boundaries. At the same time, this authority provides a single platform for national institutions to approach, when dealing with issues that take place across (physical) borders. Additionally, trends can be viewed and internationally important findings can be published. This will aid each subsequent level to keep its involved parties informed about trends and developments regarding their own roles and responsibilities.

With each layer emphasizing a different domain of cyber security, the next paragraph on design requirements illustrates how these operations, both generic and specific take place. Additionally, this layer emphasizes what each level should look to achieve within and beyond the boundaries of this level.

5.2.2 Implementing the design solutions into a multi-actor collaboration model

Preceding chapters illustrate how each level within our integrated model function differently. The following section follows the pattern by illustrating the varying degrees of focus through the following three types of design requirements. Firstly, each level has a generic *integral approach to the risk management*, which can be seen to be the same for each level because these levels operate on the same platform.

However, based on the following individual preferences, two different design requirements can be identified. Based on specific needs, *requirements are also tailored by its individual participants* within a level. For example each industry has their own specialisation, while firms have various types of strategies. In turn, the *levels are linked to a specific group and types of interaction*, as the focus of a global level (getting *countries* to work together, based on their national cyber strategy) is far more different than on national level. This is because the global level features countries who must work together based on their national cyber strategy. On the other hand national levels offer rules and regulations, which must be followed. This allows for different parties to come together and work across sector divisions. However, the national level also provides campaigns for its citizens.

The following sections show how each level can be designed with a generic risk management approach. These sections also show how, specific integration between domains can be identified, and with which levels it interacts.

5.2.2.1 Individual level

As the latest addition to the framework, we note that many literature articles do not shed enough light on the individual level, other than the occurrence and activities of groups set up by public or national awareness initiative. Yet, internet and media sources do emphasize better results by incorporating the 'human' component in IT. Practice also supports the benefits of education and creating awareness between IT users from an organisational perspective.

Due to its limited activities on the larger levels, IT security on an individual user level should focus on raising awareness and educating the public. This is apt to prevent incidents caused by novices, who are interested in understanding technology or attempt to breach the higher level's cyber security by using other devices. An example of such an attack are the botnets, which were used to hack Estonian institutions in 2007. During this attack, many individuals were affected, which could have been prevented if they were concerned to protect their own property first. Not only national governments, but also citizen/consumer groups should look into issues that affect the privacy, as well as matters involving the proper use and safety. This proper use and safety is also addressed as cyber hygiene in some papers, and is applied to ensure that individual responsibilities, which aid in protecting the global cyber ecosystem. These groups could do this, based on deducing necessary actions and contact groups on a higher level employing our pyramid structure.

- *Activities on individual level*: educate users on usage of mobile/internet devices and their risks. Additionally, provide (free or paid) standardized tools and methods for own protection.
- *Interaction with other levels*. This is ensured by being able to contact other levels if a risk has been identified and needs to be dealt with. At the same time, it involves checking whether responsibilities are fulfilled or need to be done by other authorities. This ensures a hygienic environment for all. In turn this group is also valuable, due to being the largest group active in cyberspace. This means that if they are aware of how data and information is used and processed by other levels, they can deduce how to take action and protect their own assets. Thereby, they ensure security by taking small steps to be less vulnerable in cyber space.
- *Examples of*
  - *Generic guidelines*: for example, all users need one code of conduct, which clearly guides them on how to operate and interact with other parties in cyber space;
  - *Specific guidelines*: expert subgroups can enrol for "extra rewarding" initiatives to educate others. Thus, they have access to more advanced information.

5.2.2.2 Organisational level

In this level, it is important for each institution to have central coordination to determine a strategy and outlook for how they want to implement security. Autonomy is provided by deciding how to implement its unique vision. In terms of the preceding levels, a firm should have more freedom to choose the direction on achieving its goals. However, the method on how to do so is mainly determined by its board, and could be tailored to their demands. This is especially so in terms of IT strategy, where the different structures such as popular methods, as well as standards it needs to meet to operate can all be adjusted. Another method of achieving autonomy is by working together with industry committees to gain more clarity on their roles and responsibilities. Additionally, this involves interacting with their clients to understand their needs, which is necessary to ensure proper security for important processes.

The interaction with citizens is not as important as the interaction with their employees. Thus education and awareness raised on this level could provide beneficial rewards for both public IT safety, e.g. by promoting proper conduct). This is similar to the private IT industry, by e.g. ensuring that their own internal standard is met. Yet, if a firm would run into legal trouble, it could also ask for national committee to provide aid, e.g. national IT crisis team.

- *Activities:* by setting fixed goals and activities for firms, it allows clear structure and adds a hierarchical reporting structure to make sure that its responsibilities are met. This is done by helping secure or take part in committee action to secure a shared cyber ecosystem. In turn, the structure also allows each corporation to grow into taking an active role to protect multiple parties in cyber space, such as corporate IT responsibility.
- *Interaction with other levels*: By being transparent with trends on an industrial level, clarity on what can be expected by different firms is ensured. These firms can jointly do so in order to take measures, educate employees and help others in improving protection/security within organisations. Additionally, they can also aid in providing resources and communication channels for a(n) (inter)national level if incidents occur and action is required. This help usually involves sharing their expertise.
- *Examples of*
  - *Generic guidelines:* how organisations follow rules can improve the set by industry and nation regulations by including their experience. This aids in adapting regulations, by using experience for example;
  - *Specific guidelines:* Organisations need to be clear on how they meet requirements. For example, operating across different regions with multiple or different applications means that some tailoring is required. Currently, all guidelines aim to be specific, but usefulness from case studies would be vital in improving transparency. This will in turn help to share information on what works for certain firms and why it works.

5.2.2.3 Industry level

From this structure onwards, the specifics colour the approach to dealing with individual sectors. Because each sector is seen to have a different approach, industry level collaborations are necessary to tackle standard settings. This provides a platform for peer-benchmarking and sharing trends to illustrate developments that might affect a number of its participants. In turn, this level in our design is seen as the level to interact mainly with firms. Additionally, on a national level the roles and responsibilities that need to be fulfilled can be determined, as to achieve a given strategy.

The medical sector can be seen as a foremost example as it operates as a self-organised authority. This is in order to view whether certain rules are upheld and met by its peers. In turn, it also provides a platform where issues can be looked into, certifying proper conduct and punishing wrongdoers. This is why another generic requirement could be to encourage interaction between parties with similar interest. This would be in order to maintain collaborative efforts to look into joint efforts to improve tools and methods.

- *Activities:* Appoint a specialised committee to check if roles and responsibilities for individual parties are being met, which will lead to a secure cyberspace. It is also important to keep an individual mandate for changing industry guidelines in order to remain flexible. Actively applying experience will also help improve current knowledge on how members in an industry operate. Additionally, this application will lead to discovery of efficient ways in which individuals can protect themselves from similar threats. Protection can be achieved by using a variety of resources.

- *Interaction with other levels:* Offering feedback on national level and other sectors on trend/developments enables governments to look at whether customers (citizens) are satisfied. It might be possible that they require more education in using radical IT functions.
- *Examples of*
  - *Generic guidelines:* By setting a foundation on how technology-based rules should be put in place. This is regarding privacy, where industry regulations will also give clarity to users as well as corporations. Collectively these measures will make it less confusing on what is expected of them when acting in cyberspace;
  - *Specific guidelines:* By encouraging intermediate players to coach beginners regarding IT risks for joint security, members within an industry can help train each other. This is in order to teach and perhaps learn from each other's experience. From our interviews we saw that most industries use contacts to keep themselves informed, but active engagement would help improve all players to collaborate. This would be more efficient than the alternative of competing to achieve similar security levels.

5.2.2.4 National level

A national cyber security centre is seen as a prime example to illustrate the requirements for designing and understanding activities taken to assure cyber security on a national level. Different parties provide the input depending on their specialisation. Yet, most of them operate within a given margin of the same rules and regulations. Therefore, these rules provide a main document on the code of conduct with regard to IT security in a nation. The idea is to have the heads of all industry committees come together and provide a main strategy. Thus, all parties are involved instead of just the government, which provides a full picture on developments are going to take place across different specialisations. In turn, it is also vital for a national committee to provide planning and approach. This is in order to achieve certain long- and short-term goals to ensure proper protection to its (cross-sector) partners, as well as its citizens.

The generic requirements follow the example provided by global level. Yet, an addition is the integration of regional facilities that are in line with a certain nation's approach and partners available within the region. Specific requirements of these facilities however differ, because each nation has a different focus. For example their maturity level of IT security and the type of activities also differ, as well as parties involved and their incentives. In turn, some of its industry parties may differ, as well as the democratic structure in which decisions are taken. Additionally, how these facilities interact with the public may also differ, e.g. how publications and campaigns and education facilities improve public awareness. In turn, this level is said to interact frequently with industries, firms, and citizens. Examples of these interactions are providing a platform, following up through regulation checks and providing education and promoting safe use of IT, respectively.

- *Activities:* Creating one platform for cross-sector collaboration, will provide parties with transparency regarding information obtained on global level, according to relevancy. In turn, checking with various parties on this platform will make it easier to update and see that rules are followed through on a regular basis. On this platform government, public and private parties can also discuss how to contribute to operational organisations. This is done by taking joint decisions on topics, such as discussions on: tasks that need to be undertaken, who takes what role and/or responsibility within the group and how projects can be (jointly) funded.
- *Interaction with other levels:* Checking whether all sublevels satisfied. National actors can do the follow up by looking into complaints from e.g. industry, organisational, individual level. They can also do this by, appointing sub-committees to look into issues and pass verdicts on improper behaviour and/or adjusting regulations. These regulations would improve in efficacy after getting input from practice.
- *Examples of*
  - *Generic guidelines*: National parties can determine what rules and regulations need to be followed by encouraging input from 'lower' levels in the model. For example, taking up individual levels to see whether rules are upheld by these levels, and to what degree.
  - *Specific guidelines*: Limitations regarding time for taking action with respect to crises is different for sectors and organisations. For example, the energy sector would react differently than the entertainment industry. Solutions regarding time-outs and incidents must therefore be addressed separately for each industry. This must be done according to resources that are available. In turn, spreading information to improve transparency vs. controlling situations is an example of the considerations that national parties need to examine during high impact incidents.

5.2.2.5 Global level

The main function having a global committee in place is that there is a governing body to oversee collaborations between nations. Additionally, this committee can govern activities which take place between its various international partners. The risks and incidents which it shall deal with are thus mainly on a larger scale. This scale considers parties who disagree on integrating several different rules and regulations, rather than dealing with technical requirements which are necessary for the industry. Therefore, it is intended to bring together national parties who are the highest authority in their country. These authorities will list developments that could aid international visions. Additional tasks of this committee are focusing on maturity and international trend development.

The main requirements based on risk management approach are planning meetings for the different parties to come together. This allows them to set a plan to integrate all standards into one generic mould. This mould could help determine a blueprint on how to tackle issues. In turn, a manifest should be made for each participant to follow and uphold during collaboration. This manifest will state the global platform's long- and short-term focus and how each international party contributes to achieving this through specific actions. Subsequently, important trends are noted by major and minor players. These should be discussed to help indicate growth and best practices. The approach on how to undertake activities may differ, which is why interaction with other layers would be necessary check whether results are achieved. As a global committee, partners from lower levels can also be approached on a quarterly basis. This is to see whether results are satisfying or need to be improved, as well as to provide published documents to further improve their activities.

- *Activities:* Create a multi-level committee that oversees activities on international level. From here we can set goals for collaborative efforts and regulate the international (IT) market. Check if that bigger parties e.g. cross-sector industries are kept in check by also allowing smaller groups to be represented when dealing with issues that affect different parties. In turn, also continue investigating whether regulations are met and check the privacy status. This status particularly focuses on if privacy still upheld or given up through transparency to public.
- *Interaction with other levels:* This is regulated by a top-down approach, by starting at the head of CySec model. It involves needs that require to be reported frequently and require keeping in touch with issues. These issues might need to be addressed or followed up. In turn, some level of abstraction is needed when publishing a framework, as it must fit multiple environments without being too specific for a given situation. However, problems in this framework can be reviewed.
- *Examples of needing*
  - *Generic guidelines:* The most important task is to keep track of other levels through reports from committees to see whether periodic improvements are being made. The improvements are made are specified across the globe, in order to have an equal system in place;
  - *Specific guidelines*: Check whether changes have been followed through in each level or need to be regulated differently. This is because there can be differences per level as to what may seem logical due to regional differences. Examples of these differences are political systems and beliefs. It might therefore not be equally effective to compare countermeasures.

5.3 Internal validations of theoretical and practical issues

Keeping the different types of requirements in mind, the following paragraph compares the requirements obtained from both the literature review and the given empirical data. We see that certain elements reoccur in both literature and empirical data. This is because, they address the same topics or hold on to similar notions; while others differ vastly. An overview of both similarities and differences is presented below to show how different analyses affect our internal check:

Empirical requirements ***(Chapter 4; pg 66-67)***	***Literature requirements*** ***(Chapter 3; pg 50-52)***
1. Clear decision making structure: hierarchy to oversee activities and interactions	Similar to **Req. 8**: Create a self-organising entity (industrial) shows that it is also important to determine how to organise different entities within a layer. For *individual* level – governance through national and global level helps determine one line; while *organisations* also adhere to local and international rules and regulations such as international governance (**req 18**).

Empirical requirements (Chapter 4; pg 66-67)	*Literature requirements (Chapter 3; pg 50-52)*
2. Use trends from other sectors	Several methods promote sharing between levels in the model. **Req. 3** (tools & tutorials) relies on technical expertise that might not be familiar to average users; **req 5 and 6** (harmonise & personalise methods) takes multiple sources into account for creating guidelines. While **req 7, 9, 10, 14, 15, 17 and 19** show that on multiple levels (organisational, industrial, national and global) joint agreements need to be made to exchange and determine information that could affect many people.
3. Peer benchmarking, reporting & whistleblowing options	**Req I** focused on checks from individual users. Additionally, **req 7** from organisational and all requirements from industrial (**req 8-10**), national (**req 11-16**) and global (**req 17-19**) focus on agreements between actors within a level to determine e.g. trust, sharing knowledge and transparency.
4. Strategic planning & tactics	**Req 10, 11, 12 and 19** show how defining goals on a joint platform and determining pooled resources and inventory of capabilities can help stating what direction (inter)national parties across sectors and borders should work towards. However, we see that for individual, organisations and industries – the approach is still determined by individual choices.
5. Further exploration into own sector	Unfortunately, theory often promotes using existing methods and/or making do with what is available. An improvement would be to enable sectors to work with each other in order to improve their current standards by jointly sharing – the model provides initial steps such as **req 7** (intermediate players help beginners) and establish a platform – but encouraging further exploration could be a consequence of pooling resources (**req 10**) and determining strategy (**req 12**).

Empirical requirements (Chapter 4; pg 66-67)	*Literature requirements (Chapter 3; pg 50-52)*
6. Decide effective governance methods	**Req 9** (mutually agreed guidelines) and **14** (jointly agree on tasks and actions) enables on industrial and national (basically cross-sector) to determine by allowing members to opt on how to move jointly forward. Which can be followed up on by **req 12** (strategy).
7. Provide valuable collaboration across sectors	Here the agreements made on a global level are important, as this is the platform where parties come together to work. Thus reqs such as **15** (trust) and **17** (one platform) enable various actors to partake in joint action on a formal agreements that could otherwise only be achieved through various informal contact.

Differences that are not mentioned are requirements from literature that are emphasised on each level focusing on different activities. On the other hand empirical requirement data focuses on common goals, which could be achieved for each level. This can be noted in the different activities undertaken by each level, e.g. individual: focus on education, awareness and tooling. These measures are further highlighted in our model by defining different activities, roles and responsibilities for each layer to ensure no overlap takes place. The overlap that occurs due to interaction with other stakeholder groups is considered as an exception to this rule.

In the next table, we evaluate whether these basic recommendations from practice (7 from chapter 4; page 67-68) complement the 19 critical theoretical requirements from chapter 3 (page 50-52). Additionally, it is evaluated if these contain elements from the analytical model. However, if both theory and literature requirements do not cover the area of solutions; this implies that future research must take place to clarify this issue. This research was conducted in order to bridge the gap between both fields. Additionally, it can serve to demonstrate adjustments made to requirements to fit within the scope of our research. It will also provide us with a consistent integrated collaboration framework design, which we hope to achieve.

Literature requirements (→) vs. Empirical requirements (↓)	***Individual level***	***Organisational level***	***Industrial level***	***National (cross-sector) level***	***Global level***
(1) Clear decision making structure	The delegate present within the multi-level governance panel can also oversee activities e.g. educate and empower users in the correct use of IT is not currently in place. As mentioned in req. 1 and 3 in literature, where an *IT education and awareness program* should be put in place for users.	Yes, by implementing specific guidelines and allocating responsibilities provides structure within this level. Companies are able to dictate their direction and structure (combining different opportunities); meeting theoretical req 4 *freedom of implementation.*	Yes, req. 8 makes it possible for each industry to have a committee to consult for clarity on individual role and responsibility within group (also on governance, resolving issues, standards etc.)	Yes, req. 14 focuses on representatives as well; by determining the main activities can a proper governance structure for multiple parties be placed for actors to work together depending on their own roles and responsibilities.	Yes, the multi-level governance panel helps meet req. 18 from literature too. It provides the highest level on a global scale to follow objectives and meet their roles and responsibilities.
(2) Use of trends from other sectors	Aggregation of user interests could result in a variety of topics, as each individual has unique set of knowledge. The model implements this by naming generic and specific guidelines for users.	Yes, internally through choosing specific standards (**req. 5 and 6** would require prior knowledge on methods before harmonizing and/or tailoring; **req 7** would help ask other experts in order to focus on different topics)	Yes, req. 8 and 10 are also met because interaction within and outside stakeholder groups will compel to look at sharing existing knowledge and work together on discovering new trends.	Yes, req. 11 will focus on internal inventory (what is available, being looked at) and 12 will allow different industrial committees to share their information on the joint platform with the multi-level governance panel.	Yes, req. 17 focuses on creating awareness for all nations as a whole, which shall take place after combining international reports (obtained from subsequent req. 18) to create awareness.

Literature requirements (→) vs. Empirical requirements (↓)	*Individual level*	*Organisational level*	*Industrial level*	*National (cross-sector) level*	*Global level*
(3) Peer-benchmarking, focus on reporting, whistleblowing options.	On individual level – activities do include reporting to (inter)national level. Education tests should be proposed to determine and promote general knowledge on risks in cyberspace.	Each governance structure focuses on reporting, shared sectors (industrial, national and global). In turn, by facilitating information sharing all involved parties allows them to go back, and make their own inventory (and implement those changes on organizational level).			
(4) Strategic planning and tactics	Not necessary for individual level (although plans regarding education and awareness could be split into activities that are already carried out and ones that need put in place to expand user's general knowledge on IT).	Yes, meeting req. 6 also states that tailoring should be done to fit own goals and vision (to fulfil roles & responsibilities). Interaction allows organisations to learn from other levels as well.	Yes, enabling flexibility also allows adaptability. Implementing req. 9 shows how the input of each member also contributes to determining what vision the shared standard sees as important developments.	Yes, by adapting rules and regulations periodically can the requirements 8 till 11 be implemented to look at what resources are available and how to distribute the functions within the (regional) industry.	Yes, req. 18 is also met because this level does – to some extent provide a vision of what needs to be done on a global level – by planning for governance to achieve its goals.

	Literature requirements (→) vs. Empirical requirements (↓)	***Individual level***	***Organisational level***	***Industrial level***	***National (cross-sector) level***	***Global level***
(5)	Further exploration into own sector	Shared activities from other levels helps improve whatever knowledge exists within individual actors to improve education (req. 1) and awareness; as well as be in line with the global definition (req. 19).	Yes, by keeping in touch with intermediate players can organisations improve themselves and meet req. 7 to development within their own area of expertise.	Yes, encouraging domain specific and generic requirements helps meet req. 9 and 10 as well – combining internal knowledge with external participation to create new methods.	Yes, by gaining input from other stakeholders can effectivity be measured correctly and req. 13 be met; which focuses on how the nation's needs for security can be met effectively, while delegating efforts for innovation to its partners.	No, as cross-sector collaboration (national and global) encourages sharing, this could also inspire its parties to create something new. Req. 19 could be met by organising an analysis of international trends; which can be seen as further exploration on a global level.
(6)	Decide on what is relevant for effective measures and governance	No, motion to allow suggestions from public at regional, national level where regulation between and across sectors is determined	Yes, the flexible outline given in activities and req. 4 allows (internal) feedback to adjust and change plans.	Yes, self-contribution from members (req. 9) does allow changes to be reflected in industry standards	Yes, req. 16 focuses on whether rules and regulations are met and/or adjusts accordingly.	Yes, while req. 17 is for conflict resolution, it should also provide a platform for members to express their concern in terms of effective measure. Req. 18 initiates a process for the feedback, delivered to fulfil req. 19 (request for a public document).

	Literature requirements (→) vs. Empirical requirements (↓)	***Individual level***	***Organisational level***	***Industrial level***	***National (cross-sector) level***	***Global level***
(7)	Provide valuable collaboration initiatives across sectors	More awareness and communication during events. Additional requirement (i) allows cross-level reporting to take place too.	Not considered necessary for this level, as the focus on individual institution's development.	Yes, this is done internally, within a given industry.	Yes, this is present within different industries of a nation; meeting req. 12, 14 and 16 to jointly use input from all actors on this level to determine the course of cross-sector collaboration.	Yes, noted as the joint contribution of the various international committees on one platform (req. 17) and one definition on what needs to be done by all actors (req. 19).

5.4 Answering (sub) research question 4

In this chapter, we aim to answer: *How would we design an analytical model for cyber security collaboration? And what activities, roles and responsibilities are there between the different levels and/or cyber domains in our model?*

We firstly note that there are differences in levels, from definition (InfoSec vs. CySec) to model structuring. This is due to the complexities of having many actors involved, who each have their own approach and method to tackle cyber security. On the one hand, there is literature. This allows for stakeholder separation, whilst these stakeholders are in dire need of new and different structure that enables all actors to use their own method of risk management. On the other hand, there is practice. Practice suggests that in existing methods these issues do overlap. Thus our main challenge was to present an approach where the basics for each type of stakeholder remains general. Additionally, each stakeholder is represented as the same from the outer layer within our collaboration model. However when we focus within the layer, subgroups are enabled autonomy to still apply and manage risks according to their own idea of implementation.

This same logic should be used for structuring requirements: the general governing committee allows "level" check for common rules, while individuals (firms, group of stakeholders) within the level still have the autonomy to structure their own approach and contribute to joint efforts.

The pyramid structure for our model is used to illustrate the combination of various roles and responsibilities from each of the different cyber domains. It features each stakeholder and shows what (inter)action is needed and applied. This differs for all five groups, because

- citizens need to focus on education and raising awareness on security; while
- organisation looks to integrate technology and business with security;
- industry looks mainly at methods to collaborate with domain partners/experts and get a more sector specific help on security issues;
- while the national level aims to provide cross-sector help on security.

Our ultimate goal is to provide a base for a global level, where one multi-level governance panel can oversee developments and address critical issues. Currently from our analysis in chapters 2, 3 and 4 we see that there is insufficient means and reference from the scientific body of knowledge to determine how the global structure is to be placed. Yet, by taking examples from experts, these gaps can be filled as to why each level differs and has a different type of interaction with superiors and underlings. Superiors are classified as a level with more network influence and organisational capacity. Underlings depend on the height of the level of the existing structure which is being investigated.

Our model offers an overview of how various stakeholder groups could work within a network setting. Due to its suggestive nature, we do not focus on finalising the implementation or complexities with regard to organisational science or governance of groups. Instead we simply offer an initial example of dividing roles and responsibilities within the various actors in cyber space. Additionally, we explain that due to this diversity of stakeholders, it might be a good idea to have a multi-level governance panel in place to oversee all activities in the joint cyber ecosystem. This ecosystem could take actions if the actors do not adhere to the rules of engagement. This approach effectively safeguards international interests and ensures that the governance panel will intervene when matters cross geographical or physical borders. Moreover, this type of regulatory body could help to prioritize the severity of an incident, by framing the problem accordingly. This would be in order to be taken seriously by influential actors; while providing transparency across national borders to handle conflicts of a socio-technical nature.

Additionally, this analytical model for collaboration allows each group of stakeholders to determine how to use the flexible internal network structure to fit their own approach. This approach focuses on dealing with specific risks in their own manner; enabling them to each come to an independent decision regarding the overall approach to cyber security. This is done by allowing each internal level access to freely determine how to structure their tasks in order to meet their role and responsibilities to protect cyber space. For example, this approach used by individuals to secure their actions in cyber space differs vastly from the approach used by national institutions. The former aims to secure their own individual interests and its perspective is limited as certain interests and consequences are visible for a given person. The latter faces risks and consequences for the whole society that are much more complex. This is especially when individuals, organisations and/or industries are not able to adhere their responsibilities in cyber space according to their designated roles.

In summary, the key features of this collaboration model are:

- Roles and activities of various stakeholders, varying from individual users to global players;
- Multilevel governance panel to safeguard the alleviation of systemic risks. This could for example be done by prioritizing severity of cross border incidents and assigning sub-activities to different actors from each level within the collaboration model;
- Flexible internal network structure to allow individual stakeholders freedom of action in dealing with specific internal risks;
- Overview of interactions between levels and with other stakeholder groups in order to jointly resolve an incident; such as enabling premature escalation and warn all stakeholders who could be affected. This is in order to jointly deal with a problem before it turns into a major incident.

The following chapter uses existing case studies to highlight use and application of the various subsections. Additionally, it provides detailed explanation on (inter)action, showing how our model tackles issues such as collaboration. Finally, it demonstrates how better addressing roles and responsibilities could be tackled.

Chapter 6 – Model applicability

In order to affirm the proposed properties of our model from Chapter 5, this section conducts a thought experiment by looking into a key example of a high impact cyber incident. The case is used to illustrate how our suggested collaboration model can contribute to making differences that current methodologies are unable to resolve. Additionally, our model can help ease barriers between levels of communication, albeit in a theoretical setting. This section concludes by answering the following sub-research questions in the final section:

What common issues are found in a high impact cyber incident case study, and how can results from using the model (not) cover the existing gap? Additionally, how can this case study analysis improve our model?

6.1 Model validation through case study analysis

This particular case study has been chosen, because of the impact caused in the Dutch environment, which was also observed in the media. In turn, the case also emphasizes the need to set up important measures, all of which are either recommended by literature or practice in our framework. As each case is not able to address all levels of our framework, the following helps identify the wide scope of risks and consequences of actions. This scope needs to be considered when securing cyber space.

6.1.1. Case analysis from literature

Four years ago, at the beginning of June 2010, a hacker attempted to gain access to the systems of a Dutch commercial certificate authority Diginotar. The perpetrator succeeded a month later and began issuing rogue certificates. This is when this company, which was part of VASCO Data Security International, started to issue fraudulent certificates which were published online. As soon as this occurred, other parties used these vulnerabilities to engage in cybercrime activities. What was even worse, was that the company itself only published the incident in August 2011. This was after the Dutch governmental computer emergency response team (CERT) known as GOVCERT.NL was notified by the German GERT. Only then were they able to revoke Diginotar's rights and products. This heavily affected both public and private clients, who relied on this trusted certification element. (Prins, 2011).

The main reason for the company was eventually declared unfit to practice by its peers, was due to the time it took before reporting the attack to the (government) authorities and the citizens. This also emphasizes the importance of incident management, as this very company was audited yearly against the ETSI standards for certificate authorities (or CAs). In addition, Fox-IT also revealed that it took an entire month before hackers completely compromised the CA server and published the data online (Leyden, 2011; Fisher, 2012). Another company from New Jersey (USA), called Comodo had also been hacked by the same perpetrator (Roberts, 2011; Fisher, 2012). However, as this organisation revealed its shortcomings within mere hours, it bad reputation was advertised to serve as an example. This limited the damage to their reputation, so that thereafter they could still continue to do business.

To summarize, details on breaches and/or problems occurred on:

- individual level: very little communication between individuals using IT led to citizens no longer trusting the "Verisign" on webpages,
- organisational (certificate company) and industrial (effects of wrong security certification) level,
- regional industries discovered gap in certification and needed to change industry standards to become stricter. This is in order to prevent such security gaps from general certification,
- Dutch national government had to step in and take control of situation by removing Diginotar from its job, providing security,
- global companies were also duped because some of their products and/or services were cloned (which then exploited users) and were affected by distrust.

6.1.2 Analysis using our model

The model offers a way of analysing actors and their roles and responsibilities for this security breach, as communication and collaboration needed to take on different levels. This involved the individual, firm, industry and national level, which to some extent need to be aware of the problems caused by this incident. In turn, to resolve the problem through *reporting*, it would have been possible to shorten the time needed to send a *technical investigation team* to analyse and resolve the situation.

Because this breach was felt (inter)nationally, authorities had to stop operations immediately and are entrusted to quarantine the affected areas. Funds, education, tools (maintenance) and compliance to rules for public institutions acting, on their behalf, as well as citizens should be made by this group. This in turn is to create trust in regional authorities who can handle such situations. Yet, awareness between all parties can help reduce the panic and confusion created between parties during crisis.

The awareness of risks and consequences between each layer of actors could be handled better in this case. Our framework emphasizes the need for interaction between and within levels by providing the first start through illustrating specific and generic guidelines. Additionally, actions and interactions between stakeholders on various levels are illustrated in order to fulfil the third and fifth recommendation by experts. Regarding joint efforts, Diginotar and FoxIT could have joined hands earlier through earlier contact and reporting. This could also have been done by investing in tools that look into and pursue problems regarding internet security; enabling further research into understanding of cyber space. This research could have been conducted within borders, as done on an industry level; and across, as done on a global level.

More importantly, this situation shows exactly why a hierarchical model with a national and global level is needed to coordinate actions on behalf of all cyber space users. This is mainly because these users all have to deal with the same problem. In times of global crisis in cyber space, when there are no boundaries like in the physical plane, having one authority who could hypothetically communicate with national institutions would help raise awareness on this problem. It would also aid in creating a platform to address local parties who could help resolve the problem quickly. Because of the added functionality of each layer, responsibilities also differ per layer. An institution has a different focus and different resources available to spread awareness. Examples of such resources are many sources of individually finding and reporting bugs, and offering advice and tutorials. It can also be used for collaboration, such as funding for further tool development. This also shows how the proposed elements from the highest (global) to the lowest (users) tier play an important role in connecting individual users with higher authorities and organisations. It ultimately leads to aid in jointly protecting each other across cyber space.

6.2 Reflecting on the contribution of our research

This analytical model provides a significant scientific contribution. This is that each level of stakeholders (individual or organisations) can contribute on each level. Thus, it provides an immense contribution to collaboration. The following sections aim to answer what the common issues are, which are found in a high impact cyber incident case study. Additionally it answers how the results from using the model can (not) cover the existing gap. Furthermore it answers, how this case study analysis can improve our model. This could for example be on the transparency of incidents for national, global authorities. By finding requirements, obtained from theory and practice, we get a better idea about the bigger picture of interaction between industries in cyberspace. Most cyber security efforts until now have only concentrated on one level, and limited their collaborative efforts to focus on only reaching their own goal. They do not addressing systemic risk of cyber space. This is seen when individual firms work together, but also when a separate nation proposes to follow a certain national cyber security strategy. This is represented by regional activity. By allowing cross-sector as well as industry collaboration, two types of integrative frameworks emerge. These two types can help protect a certain domain, as well as care for national security through a self-sustaining organisation. This organisation will function solely on member contribution, which will add incentive to improve developments so that a higher maturity level can be reached.

In turn, the analytical nature of this collaboration framework also provides insight on how interaction could be improved. For example, this framework illustrates for different cases how top-level reporting can help support organisations to find their place in the network as well as create public awareness. This top-level reporting can range from global, to national and industrial developments. While governments largely focus on providing a national set of rules and regulations, our model uses theoretical and empirical data to illustrate how other parties can also contribute in taking initiative. Additionally, this data is also used for sponsoring research and developments by improving on their own fields of interest through interacting with other parties. These activities could help other sectors prosper as well. For example, one national cyber security centre (NCSC) can observe and connect data from various industries. This data can sketch a picture for a given region, which can help in finding comparative analyses that could help explain or combat problems in another sector. The ultimate aim would be to encourage more parties to work together.

This is also quite unique as it is the first framework to introduce citizens to share responsibility in securing cyberspace. By incorporating parts from both theoretical and empirical analyses, this framework sketches the importance of raising awareness and the need to properly educate users. This framework then allows these users to understand what kind of risks there are before venturing into cyber space. Subsequently, by carefully considering a number of possible scenarios where sharing information with the public is important, the framework shows how interaction helps entrust institutions with citizen's cooperation. This cooperation is used in dealing with matters, such as waving privacy if it will benefit in apprehending a cyber-criminal. Thus this interaction allows clarity into how the situation is handled and what the consequences of such incidents could be.

Additionally, research has keenly focused on activities undertaken by commercial and government institutions. Yet, our model also sees the importance of educating and empowering the public to understand and take action on such issues. By promoting global and national reporting on trends and events, a healthy ecosystem could be maintained. This could, for instance, be done by also starting campaigns that illustrate the right precautions before venturing into cyber space. This gives citizens social responsibility to ensure their own security.

As mentioned at the start of the research, not all the information on risks is actually shared by each stakeholder group in cyber space. Thus the proposal of the research is to look further into each level of the integrated framework for case studies. This allows us to get more out of the expert interviews, than just theoretical models. Additionally, it allows for a better understanding of insight needed to understand developments of different fields. Furthermore, it ensures that there are environments for integrating multiple perspectives into one hybrid cyber security collaboration framework.

Chapter 7 – Concluding remarks

This last chapter presents a summary of this research in the first paragraph. It does this by answering the question whether this research has designed a proper multi-actor cooperation model. We conclude the report in the second section by pointing out what directions are available for future research.

7.1 Results of our study

At the start of the research, we established the goal of building an analytical model for structuring cooperation between actors. This enables interactions between different layers of actors to function with each other to provide cyber security. From our historical analysis we see that each of the three main domains responsible for various levels of IT security have their own approach. For example, companies had their own approach to perceive today's information security landscape. This was then used to manage IT, where IT was seen as the main component that responded with technological solutions. However, these companies do make a selection of existing IT security models. These models are for example available in the form of international standards, theoretical frameworks, and best practices. In turn, industries built their own guidelines to compare organisations within their domains by deciding certain norms and criteria. This was in order to establish a baseline that can be objectively checked. Additionally, national institutions constructed their own models for technology security by looking at how rules and regulations for all institutions and industries were applied. This all could help narrow the scope of IT and define how the technology is to be managed. In all previous events, we noticed that it is society that comes up with measures that are technology-centred.

Today, we note a greater importance of what consequences are brought into our society. These consequences can be brought in by interconnected users, institutions, domains, governments and global operators. All these actors operate in a joint ecosystem we see as cyberspace. All actors intend on using and developing internal models through creation and application of a security model. This model is determined through various combinations using standards, frameworks, guidelines, tools and techniques. It is thus that one wonders whether all these methods cover the systemic risks of cyber space. This is because it is difficult to determine who is responsible for fulfilling a certain role within cyber space. In turn, these separate developments make us wonder whether one joint initiative would help resolve governing issues regarding the security of critical information infrastructure. An example of such governing is the European Central Bank, which oversees the financial activities undertaken by all member states using the Euro. The idea of a collaboration model is thus seen as attractive, as it would help various industries use one guideline for collaborating parties. For example, this guideline could state that activities should start securing from a national level.

How did we achieve it?

As mentioned earlier, the current body of knowledge focuses on a single actor. It also focuses on how they can employ specific models tailored to suit their benefit. Our model contributes to the current scientific body of knowledge by offering an analytical perspective. It does this by showing how roles and responsibilities for various cyber space stakeholders can be divided in order to work within a network setting. By predetermining what each actor can and cannot do in cyber space (see chapter 3 of this report), we first start understanding the actions and the limitations for each stakeholder group.

Our modelling approach stresses the need for a central coordination on a global level, which is suggested or found in literature or real life. This is why we suggest a multi-level governance panel, which is in touch with representatives on other levels and shares their findings. By interacting with their governance peers, this panel can oversee all the various stakeholder activities in the joint cyber ecosystem and take appropriate actions if consequences are breached. This approach in turn also effectively safeguards international interests. Additionally, it ensures that the objective committee steps in when matters cross borders, e.g. geographically or physically. Moreover, this regulatory body also boosts the severity of an incident in order for it to be taken seriously. Yet, it provides enough transparency across national borders to handle conflicts of a socio-technical nature.

Moreover, the model also makes use of an internal network structure for stakeholders to use their own approach in dealing with specific risks in their own manner. This is done by allowing each internal level access to freely determine how to structure their tasks. This is meant in order to meet their role and responsibilities to protect cyber space. For example, the approach used by individuals to secure their actions in cyber space differs vastly from the approach used by national institutions. On an individual level, a user aims to secure their own individual interests and his or her perspective is limited as only certain interests and consequences are visible for this person. On a national cross-sector level, risks and consequences occur that involve the whole society. These risks and consequences are much more complex; especially when individuals, organisations and/or industries are not able to adhere to their responsibilities in cyber space. These responsibilities are set up according to their designated roles.

By analysing a case study in the sixth chapter through a thought experiment setting, we note that our collaboration model provides insight on how the actions of each stakeholder affect the consequences of the incident. This is done by looking at interactions between the parties during the incident. Additionally, roles and responsibilities are viewed, which could have been in place in order to detect, respond and prevent future disasters.

The theoretical implications of our research mean that there are still plenty of topics to explore when it comes to combining various stakeholder perspectives and exploring issues briefly addressed with experts. Examples of the latter topic are pooling resources and combining cross-sector analyses to improve security methods within a specific organisation. These examples show that some topics are still very active in practice but have to be further explored in literature studies. As research does not look into such methods yet, new topics for exploring into cyber security cannot yet be defined.

Similarly the consequences of our analyses for practice means that there is a small stepping stone to integrate conflicting views on a global level. It is also of interest to further explore see how improving interactions between could have ideally prevented high impact incidents from taking place in the first place. This is due to cyber security being a cross-border issue, which could be addressed as a *tragedy of commons*. Additionally, while preventing these incidents, another avenue to explore is what an added value there could be for multiple parties. Consequentially, the scientific contribution of this thesis lies in providing an initial outline of how collaboration between five complex stakeholders could take place. It also and provides input for further studies.

7.2 Future research

As mentioned in the introduction to this research, several factors were not considered because they lie outside of our predefined scope. Taking these factors into mind, we explore how expanding the scope could contribute to enriching the knowledge and data of this research. Future research could expand on:

1. *Compare unfamiliar models with existing case studies.* The theoretical information during our exploration of this topic implied that popular methods can often be complimented by looking at unfamiliar methods. This search could be performed by smaller researchers who tend to delve into more expert knowledge, such as incident response with detailed case studies. Some experts showed interest in exploring political science and/or methods from other sectors that can be tested in case studies. This could be explored to investigate what is previously known and how tested methods can be improved. The key to this is also to see whether there is any overlap in effectiveness.
2. *Different levels for empiric data.* Detailed examination of what is currently used within sectors will help us to understand much more about how IT methods are used. The general outlook of this thesis shows that more detailed knowledge could help pinpoint where the problem in collaboration between different stakeholder perspectives lies.
3. *Look into application of actively involving citizens in security*. Currently not much information is found on general collaboration with citizens other than campaigns, forums and media to alert the public. This thesis provided small steps by giving an analysis to envision how this group could aid cyber security. Closely studying how stakeholders act and behave within the ecosystem could vastly improve the current body of knowledge.
4. *Conduct a study into how harmonisation applies in real life.* From our historical analysis of information security methods we observed that standards such as the ISO27k family and CobiT have often added new chapters to their models, but are these are being used and termed as effective. We feel that in-depth study into the application of these models could help expand today's knowledge much more than providing general applications. This is mainly because these general applications could (not) be used every now and then by select stakeholders.
5. *Employ trial and error to merge various existing (inter)national research into one framework.* Current research focuses on important improvements and research into current operations. It would however be far more interesting to test various approaches by fitting them into case study analysis and to see whether integrating certain perspectives could help put together a new model. It would also prove useful to test a global outlook that can effectively regulate various stakeholder parties and govern various international activities in cyber security.

Further studies could look into initiatives within each level to find more details e.g. roles and responsibilities. Additionally, actions that could help collaboration could be investigated by seeking out the effectiveness of interaction within every level. Additionally, national and governmental institutions could be approached to look at the viability of the proposed model. This is because so far, only theory and practice have briefly broached by the discussion through case studies and general interviews.

Ultimately, the researcher's understanding is that in the near future, more parties would be looking into practical viability. Additionally implementation of integrating different views could be done to understand more about how collaboration of various actors fits in real life cyber security.

References

A. Daneels, W. S., 1999. *What is SCADA?.* Trieste, Italy, s.n., pp. 339-343.

Adam Hahn, G. M., December 2011. Cyber Attack Exposure Evaluation Framework for the Smart Grid. *IEE Transactions on Smart Grid,* pp. 835-843.

Alberts, C. J. & Dorofee, A. J., 2002. *Managing Information Security Risks: The OCTAVE Approach.* [Online]
Available at:
http://books.google.nl/books?hl=nl&lr=&id=EGInzsKcG_8C&oi=fnd&pg=PR15&dq=define+information+security&ots=qDbV_zFly8&sig=BHMeeA12j72iJOiM1KOUB_zI_DA#v=onepage&q=define%20information%20security&f=false
[Accessed 5 April 2013].

Anderson, J. M., 2003. Why we need a new definition of information security. *Computers & Security,* pp. 308-313.

ANSI, A. N. S. I., 2013. *Introduction to ANSI.* [Online]
Available at: http://www.ansi.org/about_ansi/introduction/introduction.aspx?menuid=1
[Accessed 30 August 2013].

Armstrong, C. J. & Armstrong, H. L., 2007. Mapping information security curricula to professional accreditation standards. *Proceedings of the 2007 IEEE Workshop on Information Assurance,* p. 30=35.

Atherton, K. D., 2013. *The Biggest DDoS Cyber Attack In History Just Happened, And I Feel Fine.* [Online]
Available at: http://www.popsci.com/technology/article/2013-03/biggest-cyber-attack-history-just-happened-and-i-feel-fine
[Accessed 20 August 2013].

Atos Nederland, 2013. *Cyber security (Dutch site - cyber beveiliging).* [Online]
Available at: http://nl.atos.net/nl-nl/home/your-business/defensie-en-veiligheid/cyber-security.html
[Accessed February 2013].

Axelos, 2014. *What is ITIL.* [Online]
Available at: https://www.axelos.com/what-is-itil
[Accessed 1 September 2014].

BBC, B. B. C. N., 2014. *Edward Snowden: Leaks that exposed US spy programme.* [Online]
Available at: http://www.bbc.com/news/world-us-canada-23123964

Bellis, M., 2013. *The history of computers.* [Online]
Available at: http://inventors.about.com/library/blcoindex.htm
[Accessed 25 March 2013].

Bencsáth, B., Pék, G., Buttyán, L. & Félegyházi, M., 2012. The Cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet,* pp. 971-1003.

Berkowitz, B. & Hahn, R. W., 2003. *Cyber Security - Who's Watching The Store.* [Online]
Available at: http://regulation2point0.org/wp-content/uploads/downloads/2010/04/phpe4.pdf
[Accessed 29 July 2013].

Bernroider, E. W., Pilkington, A. & Cordoba, J.-R., 2013. Research in information systems: a study of diversity and inter-disciplinary discourse in the AIS basket journals between 1995 and 2011. *Journal of Information Technology,* pp. 8, 74–89.

Bosch-Rekveldt, M. et al., 2011. Grasping project complexity in large engineering projects: The TOE (Technical, Organizational and Environmental) framework. *International Journal of Project Management*, August, 29(6), pp. 728-739.

Brancheau, J. C. & Wetherbe, J. C., 1987. Key Issues in Information Systems Management. *MIS Quarterly,* pp. 23-85.

Brehmer, B., 2005. *The dynamic OODA loop: Amalgamating Boyd's OODA loop and the cybernetic approach to command and control.* Stockholm, Sweden, Department of War Studies, Swedish National Defence College, pp. 1-15.

Brynjolfsson, E., 1993. The productivity paradox of information technology. *Communications of the ACM,* pp. 66-77.

C. Alcarez, I. A. D. N. J. L., 2011. *Managing incidents in smart grids à la cloud.* s.l., IEEE Society, p. 5.

Cai, N., Wang, J. & Yu, X., 2008. SCADA System Security: Complexity, History and New Developments. *The IEEE International Conference on Industrial Informatics (INDIN),* pp. 569-574.

Campbell-Kelly, M. & Garcia-Swartz, D. D., 2005. The History of the Internet: The Missing Narratives. *Journal of Information Technology,* pp. 18-33.

Canal, V. A., 2008. Usefullness of an Information Security Management Maturity Model. *Information Systems Control Journal Vol. 2,* pp. 1-4.

Chee-Wooi Ten, G. M. C.-C. L., 2010. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. *IEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans,* pp. 853-865.

Choo, K.-K. R., 2011. The cyber threat landscape: challenges and future research directions. *Computers & Security,* pp. 719-751.

Chou, D. C. & Chou, A. Y., 2006. A Guide to the Internet Revolution in Banking. *Information Systems Management,* pp. 47-53.

Clemente, D., 2013. *Cyber Security and Global Interdependence - What Is Critical?,* London, United Kingdom: Chatham House.

Cockshott, J., 2005. Probability Bow-Ties: A Transparent Risk Management Tool. *Process Safety And Environmental Protection,* pp. 307-316.

Commerce, U. D. o., 2009. *NIST Information Security.* [Online]
Available at: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
[Accessed 12 November 2012].

Copeland, D. G. & McKenney, J. L., 1988. Airline Reservations Systems: Lessons from History. *Management Information Systems Quarterly,* September, 12(3), pp. 353-370.

CSRC, C. S. R. C., 2013. *Early Computer Scurity Papers, Part 1.* [Online]
Available at: http://csrc.nist.gov/publications/history/#paperlist
[Accessed 30 July 2013].

Davidson, N. & Sillence, E., 2010. It won't happen to me: promoting secure behaviour between internet users. *Computers in Human Behaviour,* pp. 1739-1747.

Deloitte and the National Association of State Chief Information Officers, 2012. *State governments at risk: a call for collaboration and compliance,* Lexington, Kentucky (USA): Deloitte Development LLC..

Denning, D., 2003. *Cyber-security as an emergent infrastructure,* The New Press: The Emerging Relationship between IT and Security (Robert Latham ed.).

DHS, U. D. o. H. S., 2013. *Cyber security.* [Online]
Available at: http://www.dhs.gov/topic/cybersecurity
[Accessed 18 August 2013].

DHS, U. D. o. H. S., 2013. *http://www.dhs.gov/national-cyber-security-awareness-month.* [Online]
Available at: http://www.dhs.gov/national-cyber-security-awareness-month
[Accessed 2 September 2013].

Directory, I. 2., 2008. *Introduction To ISO 27002.* [Online]
Available at: http://www.27000.org/iso-27002.htm
[Accessed 12 November 2012].

Duncan, R. J., 1995. There are some cracks in the cornerstone of information security. *Computers & Security,* pp. 675-680.

Dutta, A. & McCrohan, K., 2002. Management's role in information security in a cyber economy. *California Management Review,* pp. 67-87.

Economist, T., 2012. *Cyber-warfare: Hype and fear.* [Online]
Available at: http://www.economist.com/news/international/21567886-america-leading-way-developing-doctrines-cyber-warfare-other-countries-may

ENISA, E. N. a. I. S. A., 2012. *Resilience & Critical Information Infrastructure Protection (CIIP) Section.* [Online]
Available at: https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards
[Accessed 4 March 2013].

ENISA, E. N. a. I. S. A., 2012. *Shortlisting network and information standards and good practices,* Heraklion, Greece: ENISA.

ENISA, E. N. a. I. S. A., 2013. *Auditing Security Measures,* Athens, Greece: ENISA.

ENISA, E. N. a. i. S. A., 2013. *ENISA Activities.* [Online]
Available at: http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process
[Accessed 9 July 2013].

ENISA, T. E. N. a. I. S. A., 2013. *About ENISA.* [Online]
Available at: http://www.enisa.europa.eu/about-enisa
[Accessed 17 Maart 2013].

Ericsson, G. N., July 2009. Information Security for Electric Power Utilities (EPUs) - CIGRÉ Developments and Frameworks, Risk Assessment and Technology. *IEE Transactions on Power Delivery,* pp. 1174-1180.

Falliere, N., Murchu, L. O. & Chien, E., 2011. *W32. Struxnet Dossier,* Cupertino, California (USA): Symantec (Security Response).

Fisher, D., 2012. *Final report on DigiNotar hack shows total compromise of CA servers.* [Online]
Available at: http://www.theregister.co.uk/2011/09/06/diginotar_audit_damning_fail/
[Accessed 18 August 2013].

Forum, I. S., 2007. *Information for Non-ISF Members on The Standard of Good Practice.* [Online]
Available at: https://www.securityforum.org/userfiles/public/SOGP.pdf
[Accessed 30 August 2013].

Forum, I. S., 2011. *SF's Cyber Security Strategies: Achieving Cyber Resilience Executive Summary.* [Online]
Available at: https://www.securityforum.org/userfiles/public/download-research/cybersecuritystrategies/cyber-security-strategies_executive-summary_non-members.pdf
[Accessed 30 August 2013].

Forum, I. S., 2013. *ISF's Standard of Good Practice 2013 Executive Summary.* [Online]
Available at: https://www.securityforum.org/userfiles/public/sogp2013/isf_the-2013-standard-of-good-practice-for-information-security_executive-summary.pdf
[Accessed 7 September 2013].

Furnell, S., Bryant, P. & Phippen, A., 2007. Assessing the security perceptions of personal Internet users. *Computers and Security,* pp. 410-417.

Gebauer, M., 2012. *NATO Faced with Rising Flood of Cyberattacks (Warfare with Malware).* [Online]
Available at: http://www.spiegel.de/international/world/nato-concerned-about-increasing-numbers-of-cyberattacks-a-829908.html
[Accessed 30 October 2012].

Grubb, B., 2014. *Heartbleed disclosure timeline: who knew what and when.* [Online]
Available at: http://www.smh.com.au/it-pro/security-it/heartbleed-disclosure-timeline-who-knew-what-and-when-20140415-zqurk.html

Hafner, K. & Lyon, M., 1998. *Where Wizards Stay Up Late (The Origins of the Internet).* New York: Touchstone.

Halink, S., 2013. *Improving cybersecurity.* [Online]
Available at: https://www.bof.nl/2013/01/02/improving-cybersecurity/
[Accessed 28 August 2013].

Hammerli, B., 2005. *C(I)IP task description and a proposal for a substitute of national C(I)IP policies.* Acris GmbH, Switzerland, IEEE, p. 11.

Heasuk, J., Seungjoo, K. & Dongho, W., 2010. A Study on Comparative Analysis of the Information Security Management Systems. *Computational Science and Its Applications – ICCSA*, pp. 510-519.

Hermans, J. & Schreurs, G., 2013. *Vijf denkfouten over cybersecurity,* Amstelveen, The Netherlands: KPMG Advisory N.V..

Herzog, S., 2011. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security,* IV(2), pp. 49-60.

Highsmith, J. & Cockburn, 2001. Agile software development: the business of innovation. *Computer,* September.pp. 120-122.

Hirst, A. R., Escuder, B., Miravet, J. F. & Smith, D. K., 2008. High-Tech Applications of Self-Assembling Supramolecular Nanostructured Gel-Phase Materials: From Regernative Medicine To Electronic Devices. *Angewandte Chemi International Edition,* pp. 8002-8018.

Hohlbaum, F., Braendle, M. & Alvarez, F., 2010. *Cybersecurity - Practical considerations for implementing IEC 62351.* [Online]
Available at:
http://www05.abb.com/global/scot/scot387.nsf/veritydisplay/b3427a5374a35468c1257a93002d8df5/$file/1MRG006973_en_Cyber_Security_-_Practical_considerations_for_implementing_IEC_62351.pdf
[Accessed 12 November 2012].

Höne, K. & Eloff, J., 2002. Information security policy — what do international information security standards say?. *Computers & Security*, October, pp. 402-409.

Hope, C., 2013. *When was the first computer invented?.* [Online]
Available at: http://www.computerhope.com/issues/ch000984.htm
[Accessed 25 March 2013].

Hubbard, D. W., 2009. *The Failure of Risk Management: Why It's Broken and How To Fix It.* [Online]
Available at: http://books.google.nl/books?id=u2AceU1L95EC
[Accessed 1 June 2013].

Humphreys, E., 2008. Information security management standards: Compliance, governance and risk management. *Information Security Technical Report,* pp. 247-255.

Hunker, J., 2002. Policy changes in building dependability in global infrastructures. *Computers & Security,* pp. 705-711.

IEEE, 2007. *IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities.* [Online]
Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4453853
[Accessed 12 November 2012].

ISA, 2012. *ISA99, Industrial Automation and Control Systems Security.* [Online]
Available at: http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821
[Accessed 12 November 2012].

ISACA, I. S. A. a. C. A., 2008. *Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit ,* United Kingdom: ITGI.

ISO, I. O. f. S., 2013. *Benefits of International Standards.* [Online]
Available at: http://www.iso.org/iso/home/standards/benefitsofstandards.htm
[Accessed 30 August 2013].

J. Stamp, P. C. J. D. J. D. W. Y., 2003. *Sustainable Security for Infrastructure SCADA.* Albuquerque, NM, Sandia National Laboritories, p. 6.

Jones, A. & Ashenden, D., 2005. About risk management. In: *Risk management for computer security - protecting your network and information assets.* s.l.:Butterworth-Heinemann, p. 296.

Kjaerland, M., October 2006. A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers & Security, Volume 25, Issue 7,* pp. 522-538.

Klimberg, A., 2010. *International cyber incidents, legal considerations,* Tallinn, Estonia: CCDCOE, cooperative cyber defence centre of excellence.

Klimburg, A., 2012. *National Cyber Security Framework Manual.* [Online]
Available at: http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf
[Accessed 3 June 2013].

Klöpping, A., 2012. *Whole of KPN was possibly endagered (Mogelijk was heel KPN in gevaar).* [Online]
Available at: http://www.alexanderklopping.nl/post/17430814643/mogelijk-was-heel-kpn-in-gevaar-een-overzicht-van-een

Koppenjan, J. & Groenewegen, J., 2005. *Institutional design for complex technological systems.* s.l.:International journal of technology, policy and management.

Krebs, B., 2011. *FBI: $20M in Fraudulent Wire Transfers to China.* [Online]
Available at: http://krebsonsecurity.com/2011/04/fbi-20m-in-fraudulent-wire-transfers-to-china/
[Accessed 18 August 2013].

Lamb, R. J. & Yu, S., 2011. *Cyber operations maturity framework,* McLean, Virginia: Booz Allen Hamilton.

Lee, T. B., 2014. *The Heartbleed Bug, explained.* [Online]
Available at: http://www.vox.com/2014/4/8/5593654/heartbleed-explainer-big-new-web-security-flaw-compromise-privacy

Leiner, B. M. et al., 1997. The Past and Future History of the Internet. *Commun. ACM,* 40(2), pp. 102-108.

Leyden, J., 2011. *Inside 'Operation Black Tulip': DigiNotar hack analysed.* [Online]
Available at: http://www.theregister.co.uk/2011/09/06/diginotar_audit_damning_fail/
[Accessed 18 August 2013].

Limited, I., 2007. *Standard of Good Practice.* [Online]
Available at: https://www.securityforum.org/userfiles/public/2007_sogp_pub.pdf
[Accessed 12 November 2012].

Limited, I., 2012. *Tools & Methodologies.* [Online]
Available at: https://www.securityforum.org/whatwedo/publictools/
[Accessed 12 November 2012].

Limited, I. S., 2012. *ISO27k Timeline.* [Online]
Available at: http://www.iso27001security.com/html/timeline.html
[Accessed 31 August 2013].

LLC, PricewaterhouseCooper, 2013. *Key findings from The Global State of Information Security® Survey 2014.* [Online]
Available at: http://www.pwc.com/us/en/cfodirect/issues/risk-management/global-state-information-security-survey-2014.jhtml

Ltd., C., 2014. *The Heartbleed Bug.* [Online]
Available at: http://heartbleed.com/

Ltd, I., 2013. *ISO/IEC 27002:2013.* [Online]
Available at: http://www.iso27001security.com/html/27002.html#StructureAndFormatOfISO17799
[Accessed 31 August 2013].

M.T.O. Amanulla, A. K. A. Z., 2005. *Network Security Vulnerabilities in SCADA and EMS.* Dalian, China, IEEE/PES, p. 6.

MacDermott, S., 2013. *From Brussels to Talinn: NATO's new relevance.* [Online]
Available at: http://blogs.avg.com/public-policy/nato%E2%80%99s-new-relevance/
[Accessed 30 June 2013].

Manuel Cheminod, L. D. A. V., 2013. Review of Security Issues in Industrial Networks. *IEEE Transactions on Industrial Informatics,* pp. 277-293.

MOD, M. o. S. a. D., 2012. *English Translation of Dutch Cyber Defense Strategy.* [Online]
Available at: http://www.infosecisland.com/blogview/21953-English-Translation-of-the-Dutch-Defense-Cyber-Strategy.html
[Accessed 29 August 2013].

Naughton, J., 2010. *The internet: everything you ever need to know.* [Online]
Available at: http://www.theguardian.com/technology/2010/jun/20/internet -everything-need-to -know

NCSC, D. N. C. S. C., 2014. *Frequently Asked Questions.* [Online]
Available at: https://www.ncsc.nl/english/current-topics/frequently-asked-questions.html

NCSC, N. C. S. C., 2013. *Cybersecuritybeeld Nederland,* Den Haag: Directie Cyber Security van de Nationaal Coordinator Terrorismebestrijding en Veiligheid (NCTV).

NCTV, N. C. T. e. V., 2014. *Over Alert Online.* [Online]
Available at: https://www.alertonline.nl/over_alert_online/

NERC, 2004. *NERC 1300 - Cyber security.* [Online]
Available at:
http://www.nerc.com/docs/standards/sar/Draft_Version_1_Cyber_Security_Standard_1300_091504.pdf
[Accessed 12 November 2012].

Newsdesk, 2012. *Georgia Tech releases cyber threats forecast for 2013 (Cybersecurity).* [Online]
Available at: http://www.homelandsecuritynewswire.com/dr20121115-georgia-tech-releases-cyber-

threats-forecast-for-2013
[Accessed 18 November 2012].

Nicolas Falliere, L. O. M. E. C., February 2011. *W32. Struxnet Dossier,* s.l.: Symantec (Security Response).

NIST, N. I. o. S. a. T., 2012. *Computer Security Resource Center.* [Online]
Available at: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
[Accessed 9 July 2013].

OECD, C., 2012. *Cybersecurity policy making at a turning point.* [Online]
Available at: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf
[Accessed 3 June 2013].

Office of the Law Revision Counsel, U. S. o. A., 2013. *Cornell University Law School - Legal Information Institute.* [Online]
Available at: http://www.law.cornell.edu/uscode/text/44/3542
[Accessed 15 March 2012].

Opstelten, I. & Verhagen, M., 2012. *File 26643 (ICT), Nr 225 (KPN breach).* [Online]
Available at: https://zoek.officielebekendmakingen.nl/dossier/26643/kst-26643-225?resultIndex=191&sorttype=1&sortorder=4

Ostrom, E., 1990. *Governing the commons - the evolution of institutions for collective action.* 2003 ed. Cambridge: Cambridge University Press.

Ouzounis, D. V., 2013. *Resilience of Networks and Services and Critical Information Infrastructure Protection.* [Online]
Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP
[Accessed 17 March 2013].

Paulk, M., Curtis, B., Chrissis, M. & Weber, C., 1993. *Capability maturity model, version 1.1,* Pittsburgh (Pennsylvania, USA): IEEE Software.

Prins, J., 2011. *Interim Report DigiNotar Certificate Authority breach "Operation Black Tulip".* [Online]
Available at: http://www.rijksoverheid.nl/ministeries/bzk/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html
[Accessed 12 August 2013].

Quigley, K., 2013. *"Man plans, God laughs": Canada's national strategy for protecting critical infrastructure,* Toronto, Canada: The Institute of Public Administration of Canada.

Quora, 2013. *How Does Cyber Warfare Work?.* [Online]
Available at: http://www.forbes.com/sites/quora/2013/07/18/how-does-cyber-warfare-work/

R. Chandia, J. G. S. S. M. P. T. K., 2010. Security strategies for SCADA networks. In: *International Federation for Information Processing Digital Library, Critical Infrastructure Protection.* s.l.:Springer, pp. 119-131.

Rajab, M., Zarfoss, Z., Monrose, F. & Terzis, A., 2006. *A Multifaceted approach to understanding the botnet phenomenon.* New York, USA, ACM, pp. 41-52.

Rinaldi, S., Peerenboom, J. & Kelly, T., 2001. Identifying, understanding and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine,* pp. 11-25.

Rising, L. & Janoff, N., 2001. The Scrum software development process for small teams. *Computer,* July-August, 34(9), pp. 26-32.

Robert Dawson, C. B. E. D. J. M. G. N., 2006. *SKMA: a key management architecture for SCADA systems.* Hobart, Tasmania, Australia, s.n., p. 10.

Roberts, P., 2011. *Phony SSL Certificates issued for Google, Yahoo, Skype, Others.* [Online]
Available at: http://threatpost.com/phony-ssl-certificates-issued-google-yahoo-skype-others-032311
[Accessed 18 August 2013].

Rowe, B. R. & Gallaher, M. P., 2006. *Private Sector Cyber Security Investment Strategies: An Empirical Analysis.* [Online]
Available at: http://www.weis2006.econinfosec.org/docs/18.pdf
[Accessed 30 September 2013].

Rowe, D. C. & Lunt, B., 2012. *Mapping the cyber security terrain in a research context.* New York, NY, USA, Calgary, Alberta (Canada), pp. 7-12.

Rowe, D. C., Lunt, B. M. & Ekstrom, J. J., 2011. *The role of cyber-security in information technology education.* West Point, New York, USA, ACM, pp. 113-122.

Samani, R. & Paget, F. (. I., 2013. *Cybercrime Exposed.* [Online]
Available at: http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-exposed.pdf
[Accessed 22 July 2013].

Schmitt, D. S. &. E., 2012. *Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure.* [Online]
Available at: http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html?_r=0
[Accessed 30 October 2012].

Security, U. D. o. H., 2013. *Critical Infrastructure Sectors.* [Online]
Available at: http://www.dhs.gov/critical-infrastructure-sectors
[Accessed 15 March 2013].

Security, U. D. o. H., 2013. *Secure Cyber Networks.* [Online]
Available at: http://www.dhs.gov/secure-cyber-networks
[Accessed 16 March 2013].

Security, U. D. o. H., n.d. *DHS.gov.* [Online]
Available at: http://www.dhs.gov/what-critical-infrastructure
[Accessed 20 June 2013].

Shaw, W. T., 2006. *Cybersecurity for SCADA systems.* Tulsa, Oklahoma: PennWell Corporation.

Simona, 2012. *KPN confirms digital burglary (KPN bevestigt digitale inbraak).* [Online]
Available at: http://forum.kpn.com/t5/News-stream/KPN-bevestigt-digitale-inbraak/ba-p/16669

Siponen, M. & Willison, R., 2000. Information security management standards: Problems and solutions. *Information & Management,* pp. 267-270.

Sources, V. W., 2013. *Timeline of computer security hacker history.* [Online]
Available at: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history
[Accessed 10 October 2013].

Strous, L., 1994. Security Evaluation Criteria. *Computers & Security*, 13, pp. 379-394.

Syalim, A., Hori, Y. & Sakurai, K., 2009. Comparison of Risk Analysis Methods: Mehari, Margarit, NIST800-30 & Microsoft's Security Management Guide. *International Conference on Availibility, Reliability & Security*, pp. 726-731.

Theoharidou, M., Kokolakis, S., Karyda, M. & Kioutouzis, E., 2005. The insider threat to information systems and effectiveness of ISO17799. *Computers & Security,* pp. 472-484.

Townsend, A., 2001. The Internet and the rise of the new network cities, 1969-1999. *Environment & Planning B: Planning and Design,* pp. 39-58.

University, C. M., 2014. *Vendor Information for VU#720951 (Heartbleed Bug).* [Online]
Available at:
http://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=720951&SearchOrder=4

Unknown, 2013. *Probleem banken door cyberaanval (Banks face problems after cyber attack).* [Online]
Available at: http://nos.nl/artikel/492603-geslaagde-cyberaanval-op-banken.html
[Accessed 18 August 2013].

Various, 2012. *Wikipedia.org.* [Online]
Available at: http://en.wikipedia.org/wiki/Risk_IT
[Accessed 10 July 2013].

Various, 2013. *American Express joins the ranks of US banks attacked by al-Qassam group.* [Online]
Available at: http://www.infosecurity-magazine.com/view/31563/american-express-joins-the-ranks-of-us-banks-attacked-by-alqassam-group/
[Accessed 18 August 2013].

Various, 2013. *Cyberbunker.* [Online]
Available at: http://en.wikipedia.org/wiki/CyberBunker
[Accessed 20 August 2013].

Various, 2013. *DigiNotar.* [Online]
Available at: http://en.wikipedia.org/wiki/DigiNotar
[Accessed 20 August 2013].

Various, 2013. *Politie.nl kort plat na DDoS-aanval (Dutch police website shortly offline after DDoS attack).* [Online]
Available at: http://nos.nl/artikel/535826-politiewebsite-onbereikbaar-na-hack.html
[Accessed 18 August 2013].

Various, 2013. *Spamhaus.* [Online]
Available at: http://en.wikipedia.org/wiki/Spamhaus
[Accessed 20 August 2013].

Various, 2013. *Wikipedia.org.* [Online]
Available at: http://en.wikipedia.org/wiki/ISO/IEC_17799
[Accessed 9 July 2013].

Various, 2014. *Cyber-warfare: Is the risk of cyber-warfare overrated?.* [Online]
Available at: http://www.economist.com/debate/debates/overview/256

von Solms, B., 2005. Information Security - The Fourth Wave. *Computer Security,* Volume 25, pp. 165-168.

von Solms, B. & von Solms, R., 2005. From information security to...business security?. *Computer Science & Society,* Volume 24, pp. 271-273.

von Solms, R., 1997. Information security management: why standards are important. *Information Management & Computer Security,* 7(1), pp. 50-57.

von Solms, R., 1998. Information security management (3): the Code of Practice for Information Security Management (BS 7799). *Information Management & Computer Security ,* 6(5), pp. 224-225.

von Solms, R. & van Niekerk, J., 2013. From information security to cyber security. *Computers and security,* pp. 97-102.

von Solms, S. (., 2000. Information Security - The Third Wave?. *Computers & Security,* pp. 615-620.

von Solms, S. (., 2010. The 5 Waves of Information Security – From Kristian Beckman to the Present. In: *Security & Privacy - Silver Linings In The Cloud.* Brisbane, Australia: Springer Berlin Heidelberg, pp. 1-8.

Wamala, D. F. C., 2011. *The ITU National Cybersecurity Strategy Guide.* [Online]
Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
[Accessed 3 June 2013].

Whitman, M. E. & Mattford, H. J., 2011. *Principles of Information Security.* [Online]
Available at: http://books.google.nl/books?hl=nl&lr=&id=L3LtJAxcsmMC&oi=fnd&pg=PR9&dq=define+information+security&ots=6UH3RWeQwP&sig=G0fdlneVryRqKpquclgDBI-VnXw#v=onepage&q=define%20information%20security&f=false
[Accessed 5 April 2013].

Zhang, D. & Zhou, L., 2004. Discovering Golden Nuggets: Data Mining In Financial Application. *IEEE Transactions on Systems, Man and Cybernetics - Part C: Applications & Reviews,* pp. 513-522.