Cyber security: a risky business

Broadening the perspective on cyber security risk

Master thesis for the Executive Master Cyber Security

Cyber Security Academy

Linda Durand

First supervisor: prof. B. van den Berg (Leiden University)

Second supervisor: S. Boeke (Leiden University)

18 January 2018

Abstract

This thesis identifies two conceptions of risk - the realist and social constructivist conception - and investigates how both conceptions shape the way in which the risks related to cyber security are framed and how this framing informs government responses. By means of a conceptual analysis, the research reveals that from a historical perspective the realist conception has become the most common theoretical perspective on risk. The realist perspective considers risks as real events that can be objectively calculated, measured, and mitigated through risk management. Many different risk management methodologies have been designed to address the risks related to cyber security. However, the value of risk management in the field of cyber security is limited. The social constructivist perspective on risk offers an alternative view on risk. The analysis shows that from this perspective the current cyber security threat discourse, which constitutes hypothetical cyber-doom scenarios, can be considered as a social construct and is subject to the political process of securitization. Due to increased social and political pressures to mitigate risks in society, governments resort to risk management to deal with risks. A case study on the government of the Netherlands shows that risk management regarding cyber security is considered a fundamental principle. Yet, the government also recognizes that the true magnitude of the risks related to cyber security remains uncertain as risk management regarding cyber security has its limits. From the social constructivist perspective, three alternative responses for governments are explored in this thesis and concern precaution, trust, and resilience.

Contents

1. Introduction

We are living in a digital world where computers and the internet have become central to our daily lives and everyone and everything is increasingly connected (Singer & Friedman, 2009: 1-2). Ever since the first electronic mail was sent in 1971, the digital landscape has transformed enormously. The internet is no longer merely a place to send messages and look up information, it now extends to include our critical infrastructures, our economy, our healthcare, and even our coffeemakers and toys. Due to this increasing connectedness, it is becoming difficult to define where the physical world ends and the digital world begins (Singer & Friedman, 2009: 1-2). This is due to the fact that the digital domain cannot merely be defined by the technology it consists of. Instead, what is now called cyberspace has become a complex realm where technology and humans interact and where new activities and applications are being deployed constantly (Singer & Friedman, 2009: 1-2; van den Berg et al., 2014: 2; Deibert, 2017: 172).

As a result of the widespread application of these new opportunities, society as a whole has become reliant on the undisrupted functioning of the information and communication technology (ICT) systems that form the foundation of cyberspace (Deibert, 2017: 172). As has become evident over the years, this reliance is vulnerable. Not only are these ICT-systems prone to technical malfunctions due to the constant operation and maintenance of, and interaction with these systems, they are also targeted by malicious actors (Deibert, 2017: 172). A diverse set of actors, including professional criminals, state actors, terrorists, cyber vandals and script kiddies, hacktivists, internal actors, and private organizations are looking to purposefully disrupt ICT-systems, steal or manipulate information, or conduct digital espionage for instance (Deibert, 2017: 172; National Cyber Security Centre, 2017: 8).

Even though there is no complete and reliable data available on the exact number of cyber-attacks or cyber-malfunctions, the threat level in the digital domain is considered very high by experts all across the board (Dlamini, Eloff & Eloff, 2009: 4; Deibert, 2017: 172; Singer & Friedman, 2009: 3). For example, it is estimated that in the US alone there is an average of $300 billion in economic and intellectual property loss, which constitutes over 1 percent of the US' GDP. Studies in other countries show similar percentages (Hathaway, Demchak, Kerben, McArdle & Spidalieri, 2015: 3). The extent of the threat in cyberspace is often illustrated by referring to highly visible incidents, to highlight but a few: the sophisticated Stuxnet attack on a nuclear plant in Iran in 2010, the disclosures of Edward Snowdon on the widespread NSA cyber espionage and monitoring in 2013, the attack on the electricity grid of the Ukraine in 2015, the e-mail leak of the Democratic National Committee in the run-up to the US elections in 2016, and the worldwide ransomware attack Wannacry in May 2017 resulting in hospitals closing down in the UK (Singer & Friedman, 2009: 2; Deibert, 2017: 172; Inkster, 2016: 23-24; Sullivan & Kamensky, 2017: 30; Mattei, 2017: 972). What is more, the news media is also waking up to these incidents adding to the growing attention to the

dangers of cyberspace (Lawson, 2011: 1). In response, public, private and international organizations are currently creating cyber security strategies and allocating funds to address the risks related to cyber security (Luiijf, Besseling & De Graaf, 2013; Singer & Friedman, 2009: 3; Deibert, 2017: 172-173).

Nevertheless, not everyone is as convinced of the gravity of the cyber threat. As mentioned by Brito & Watkins (2011), the cyber security phenomenon may very well be subject to threat inflation. Threat inflation is understood to be the attempt to create more concern and urgency over a certain threat than can be substantiated through objective research (Brito & Watkins, 2011: 40-41). The authors claim that even though threats in cyberspace do exist, the concerns for so-called "cyber-doom scenarios" remain as yet unsupported by evidence that is available to the general public[1] (Brito & Watkins, 2011: 40). These cyber-doom scenarios are hypothetical stories that typically involve multiple critical infrastructure systems failing at the same time, leading to serious or total destruction of the economy and society (Lawson, 2011: 4; Dunn Cavelty, 2016: 414). It is argued that even though we are witnessing cyber-incidents that at times cause major inconveniences, we have not seen anything close to these cyber-doom scenarios and it is questioned whether they will ever happen at all (Dunn Cavelty, 2016: 414; Lawson, 2011: 5-7).

This begs the question: how real are the risks regarding cyber security? What are these risks exactly, and what constitutes an appropriate response? Finding answers to these questions occupies governments, businesses, and researchers alike, as evidenced by an increasing amount of research conducted. Despite these efforts, addressing the risks effectively, while simultaneously stimulating the economic potential of cyberspace and securing rights and freedoms of people online, remains challenging for most governments (Hathaway et al., 2015: 3). The aim of this thesis is not to add to the existing research efforts of investigating the cyber security risks themselves. Instead, the aim is to examine how we are currently going about the exercise of identifying and addressing the risks concerning cyber security. This is done by drawing from different theories and conceptions of risk.

Dealing with risk is an unavoidable part of life (Berg, 2010: 79). On a global scale, dealing with risk concerns issues such as climate change or nuclear safety. On an individual level, risk involves deciding if it is safe to cross the street for instance. Focusing on risk is about finding ways to cope with an uncertain future and trying to prevent or minimize possible losses (Zinn, 2009: 2; Berg, 2010: 79). The assumption that underlies this idea is that we can influence future outcomes and keep ourselves safe by taking appropriate measures. This assumption poses many questions though. For instance, do we need to protect ourselves against every conceivable risk, and what is the acceptable price we are willing to pay to guard ourselves against these risks? How do we determine what acceptable risk levels are, and how do we

[1] Government officials often refer to classified information to support the claims for the threats in cyberspace (Brito & Watkins, 2011: 49, 56).

deal with residual risks? Moreover, it leads to the question of how we can determine risk in the first place (Zinn, 2009: 1-2; Berg, 2009: 85-86; Lupton, 1999: 17-18).

According to Bernstein (1999), at the heart of the debate over the best way to determine risk is an as yet unresolved tension regarding the extent to which the past can be used to determine the future (Bernstein, 1996: 6). There are some that find that risks can best be defined by looking at quantification. This entails measuring the past in order to make predictions about the future. This idea forms the foundation of modern day risk management (Bernstein, 1996: 6; Zinn: 2009: 4-5; Berg, 2010: 79; Lupton, 1999: 17-18). There are others that find that the value of calculating the past is limited, as calculation only goes so far when confronted by the struggles and ambiguity of daily reality (Bernstein, 1996: 6-7). These two perspectives on risk are referred to as the realist perspective, and the social constructivist perspective respectively (Zinn, 2009: 5-7; Lupton, 1999: 17).

According to the realist perspective, risks are real events or hazards that exist in the world and which can be determined objectively (Zinn, 2009: 4-6). Lupton (1999) ads that according to this perspective, risks "are pre-existing in nature and in principle are able to be identified through scientific measurement and calculation and controlled using this knowledge" (Lupton, 1999: 18). It is within this realist perspective that modern day risk management can be understood. Risk management entails the process of objectively calculating and quantifying the likelihood and impact of events (Berg, 2010: 79). As such, risk management is a systematic approach to establish the best course of action to deal with uncertain events, by identifying, assessing, prioritizing, and mitigating risks (Berg, 2010: 79-81). The first studies on risk management, as we know it today, were conducted after World War II. It was during this period that technological risk management models were starting to be designed in response to the industrialization of society and because of ensuing concerns for the environment, and public health and safety (Dionne, 2013: 147; Berg, 2010: 80; Kasperson et al., 1988: 177). Thus, risk management was originally developed to create safe technological systems (Berg, 2010: 80,82; Zinn, 2009: 4-5). Within this context, risks are considered non-intentional accidents, meaning they do not entail human agency (Hessami, 2004: 99-100; Reniers & Cozzani, 2013: 6).

The social constructivist perspective on the other hand holds that risks cannot merely be determined by an objective calculation or measurement of the probability and impact of an event. Instead, a risk is seen as a complex construct that is created by cultural or social values that are applied to it (Kasperson et al., 1988: 177-178; Renn, 1992: 54-55). Thus, what constitutes risk is influenced by human interaction, involving social and cultural processes, that steers the appreciation and determination of risk (Zinn, 2009: 6-8). It is within this perspective that a more security focused idea of risk applies. This entails the notion that the determination of risk should take into account the intentional character of human agency that leads to risk. As opposed to the realist view on risk, calculating probabilities in terms of

security is much more difficult as human behavior is not static and the capabilities of malicious human actors is often unknown (Hessami, 2004: 99-100; Reniers & Cozzani, 2013: 6).

The rationale behind studying scientific theories is that they can help make sense of the world around us. Moreover, scientific theories can provide us with a deeper understanding of certain issues and help us make decisions on whether or not to act, and if so, in what manner (Zinn, 2009: 2). This thesis makes use of theories of risk in order to gain a deeper understanding of the way in which cyber security is perceived. More specifically, this thesis investigates how the realist and social constructivist conceptions of risk shape the way in which we are currently framing cyber security.

What is more, based on this frame, it is possible to identify and evaluate how we respond to the risks concerning cyber security. More specifically, the responses from the perspective of governments are investigated. The governmental perspective is interesting as political pressures constitute an increased call on governments to address and mitigate risks through various ways of risk management (Power, 2004: 9). A case study of the Netherlands is provided to illustrate this notion. Yet, despite these efforts, risks can never be completely mitigated, and failures, incidents, and crises do happen (Power, 2004: 10). Consequently, the social constructivist perspective is called upon to highlight examples of alternative approaches for responding to the risks related to cyber security. As a result, the main question of this thesis is: *how do conceptions of risk shape the framing of cyber security and how does this framing inform government responses?*

Structure of the thesis

The next chapter, chapter two, contains the research methodology and scope of the research. The remainder of this thesis consists of three parts. The first part consists of two chapters and constitutes the theoretical framework of this thesis. Chapter three elaborates on what exactly constitutes risk by looking at the meaning, definitions and the historical context of the notion of risk. Chapter four zooms in on the realist and social constructivist perspectives of risk. The second part of this thesis analyzes how both conceptions of risk frame the shaping of cyber security in chapter five. The third part of this research investigates what the framing of cyber security means for the responses of governments in chapter six. In chapter seven conclusions are drawn and reflections provided.

2. Research methodology and scope

This chapter first describes the research methodology that is used in this thesis. Then, the limitations to the study are provided in the second part of this chapter.

2.1 Research methodology

The main question of this thesis concerns how different conceptions of risk shape the framing of cyber security and how this framing informs government responses. In order to find answers to the research question, this thesis is descriptive in nature and constitutes a conceptual analysis of different risk theories and their application to the field of cyber security. The thesis consists of three parts. The first part provides the theoretical framework concerning risk by explaining the different conceptions of risk. Based on this theoretical framework, the second part of the research examines how these conceptions currently shape the way in which cyber security is being framed. The third part elaborates on the way in which this framing informs government responses to cyber security risk. This is elaborated upon below.

Part one

Part one of the study consists of two chapters which are both conducted by means of desk research. The first chapter starts by describing how the notion of risk can be defined and understood. Risk as a concept is very diffuse and can mean different things to different people (Hansson, 2005: 7-8). What is more, a brief overview of the origins of the concept of risk is provided in order to understand how the concept has evolved over time. The second chapter elaborates on the different conceptions of risk, the realist perspective and social constructivist perspective.

Part one is based on four main literary sources. Hansson (2005) provides an overview of five ways in which the conceptual meaning of the notion risk can be explained. Bernstein (1996) extensively writes about the history of risk and the scholars that contributed to the development of the notion of risk throughout history. Even though it is beyond the scope of this thesis to extensively review the entire book, the most noteworthy observation that is borrowed from Bernstein includes the idea that without the introduction of our present-day numerical system the entire venture of risk management would not have come to pass. The third and fourth works are offered by Lupton (1999) and Zinn (2009). Both authors place the realist conception of risk in relation to the social constructivist conception and extensively write about the different theoretical approaches that are placed within the social constructivist conception. It should be added that the chapters draw upon the works of additional scholars to complete and enrich the analysis.

Part two

The second part of this thesis, which constitutes chapter five, concerns the analysis of the way in which both the realist and social constructivist conception of risk shape the framing of cyber security. The analysis is based on desk research and draws on a variety of different literary sources including scientific books and articles in scientific journals.

Chapter five consists of three parts. The first part focuses on how the realist perspective shapes the framing of cyber security. This is done by looking at the origins of cyber security under the header of information security, and how risk management is applied to the field of cyber security. The second section of the chapter focusses on the limitations of making use of risk management in the field of cyber security. The third part investigates how the social constructivist perspective shapes the framing of cyber security. More specifically, this section provides three examples of discussions that currently exist within literature and that fit in with the social constructivist perspective rather than the realist perspective. The aim is not to provide an exhaustive overview of all social constructivist discussions that exist. Instead, the discussions illustrate that social constructivist thinking in the field of cyber security is taking place and offer different insights regarding cyber security risks than looking at them from the realist perspective.

Part three

The third part of the research focusses on the manner in which the framing of cyber security, as discussed in the second part of the research, informs government responses. In the first section of chapter six, the notion of the 'risk management of everything' offered by Power (2004) is quoted to illustrate how there is increased political pressure on governments to address and mitigate risks through various ways of risk management.

The second part of the chapter exemplifies this idea by providing a case study of the government of the Netherlands. More specifically, three examples are offered that show how risk management related to cyber security is regarded as a fundamental principle within the cyber security policy of the Netherlands. The case study draws upon a number of policy documents, most notably: the Dutch National Security Strategy, the National Security Profile, the National Cyber Security Strategy, the Cyber Security Assessment of the Netherlands, and the Baseline Information Security.

The last section of chapter six investigates what insights the social constructivist perspective could offer governments in response to risks related to cyber security. Three government responses are investigated: precaution, trust and resilience. Again, it should be added that these are not the only policy responses that could be contrived from the perspective of social constructivism. The purpose of this section is to illustrate that the social constructivist perspective offers different insights than the realist perspective with regard to possible government responses. Based on the writings of Beck (2006) the precautionary principle is

investigated as an additional policy response, and Giddens (1999) offers the notion of trust. A number of different scholars argue that resilience could serve as an appropriate strategy in light of the complex, and inevitable nature of the risks related to cyber security (Power, 2004; Dunn Cavelty & Giroux, 2015; Lawson, 2011). The literary works of a number of different scholars are used to illustrate the applicability of these three possible government responses to the field of cyber security. It should be added that this part of the chapter does not specifically focus on the Netherlands, even though the Netherlands is used as an example of a government that has actively adopted a policy regarding trust.

2.2 Scope

2.2.1 Risk classification and the psychometric perspective

Risk is studied within a variety of different scientific disciplines and consequently there is a vast amount of theoretical writing available on the subject (Zinn, 2009: 3; Luhmann, 1993: 1). In order to compare and contrast the different theoretical contributions, classifications of risk theories have been created (Renn, 1992: 55-56). It should be noted that different authors classify risk conceptions in different ways (Renn, 1992: 55-56; Lupton, 1999: 17; Zinn, 2009: 8). Overall, it can be stated that the two overarching conceptions are the realist and social constructivist perspectives (Lupton, 1999: 17; Zinn, 2009: 8). Nevertheless, it should be added that a third perspective can be identified that fits in between both the realist and social constructivist perspective: the psychometric perspective, which constitutes the study of risk perception (Zinn, 2009: 5-6, 8).

The psychometric perspective is derived from the field of psychology. It concerns the objective study of the perception of risk (Zinn, 2009: 6). Within this field of study, psychological models of human behavior are used to find out which risks people worry about and how much they worry (Lupton, 1999: 19; Zinn, 2009: 6). The way in which this is investigated, is through standardized questionnaires to establish general patterns of behavior and causality. Psychometric research has shown how certain aspects of risk, for example the scale, dreadfulness, and likelihood of risk, influences how people perceive them (Zinn, 2009: 6).

Literature classifies the psychometric perspective as a realist approach and, as such, it recognizes that risks can be objectively identified. Nevertheless, while risks can be objectively identified, the perspective also holds that the interpretation of risks by people is subjectively biased (Zinn, 2009: 5; Lupton, 1999: 19). Zinn (2009) states that “this means that although we can objectively find out what the best response to a risk would be, the observable subjective judgements and perceptions deviate systematically” (Zinn, 2009: 5). It should be added that risk perception is discussed and valued by both realists and social constructivists in different ways. Realists hold the efforts made by experts, who calculate and quantify risks, in higher esteem than the subjective interpretation of lay-people. From this perspective, the knowledge of experts is considered neutral and unbiased (Lupton, 1999: 19). Social constructivists, on the

other hand, argue that the identification of risk and the perception of risk are very much intertwined and can hardly be seen separately. In line with this perspective, the knowledge of experts and lay-people both constitute what is considered to be a risk. What is more, the endeavors of experts in calculating risks are equally prone to the implicit social and cultural biases as the judgements of lay-people (Zinn, 2009: 25-26; Lupton, 1999: 29).

Despite a vast amount of literature and research on risk perception, the application of risk perception in the field of cyber security is still very limited and there are no comprehensive psychometric studies regarding cyber security yet (Huang, Rau & Salvendy, 2007: 907). What is more, studies that are conducted into the cyber security awareness of lay-people shows that the risk perception is quite low (Blanksma Çeta & Konings, 2017: 4-5). As a result, it can be derived that the responses to the risks regarding cyber security are primarily informed by the knowledge of experts rather than public risk perception. Moreover, vastly different risk perceptions exist within society, and incorporating them into policy is notoriously difficult for policy-makers (Power, 2004: 19-20). As this thesis focusses on the framing of the risks related to cyber security and the way in which government responses are informed by this framing, it can be derived that this frame is mostly based on insights provided by experts. Thus, a discussion on the risk perception of cyber security is out of scope in this thesis. Instead, expert knowledge is focused on and constitutes both the realist and social constructivist perspectives.

2.2.2 Scope of the theoretical framework

Realist perspective

With regard to the description of the realist perspective in chapter four, it should be noted that an extensive amount of literature is available on what constitutes risk management. Providing an all-encompassing examination of the risk management process and all its facets extends beyond the scope of this thesis. Instead, the first part of chapter four offers an overview of the core elements of risk management with the aim of contrasting the realist perspective with the social constructivist perspective in the second part of the chapter.

Social constructivist approaches

A full account of what constitutes the social constructivist perspective would require an extensive review of a number of different approaches, including: risk society and reflexive modernization, securitization, governmentality, risk and culture, systems theory, and edgework (Zinn, 2009: 15-16; Lupton, 1999: 24-28; Vuori, 2017: 64). Even though these approaches are all similar in the sense that they consider the notion of risk to be socially constructed in some way, they differ in terms of epistemological background and focus area (Lupton, 1999: 24-28).

The scope of this thesis is limited to an overall description of the main characteristics of the social constructivist perspective in chapter four, and a specific focus on two social constructivist approaches: risks society and reflexive modernization, and securitization. Risk society and reflexive modernization is argued to be the most influential approach. Lupton (1999) states that the specific insights regarding the structural and political nature of risk throughout the process of modernization accounts for the popularity of the risk society and reflexive modernization approach (Lupton, 1999: 82-83). Securitization theory is highlighted in this thesis because of its specific focus on how issues are socially and politically constructed as security issues (Vuori, 2017: 64-65). What is more, the securitization approach is explicitly applied to the field of cyber security by a number of different scholars (Dunn Cavelty, 2013: 106).

Even though a review of the edgework approach is thus beyond the scope of this thesis, it deserves a note of attention. As elaborated upon in chapter three, in contemporary society, risk primarily has a negative connotation meaning danger or fear. Yet, it should not be disregarded that risk can also have a more positive association. In the field of economics, speculative risk entails the situation in which the outcome can result in both gains and losses (Williams, 1966: 577; Halek & Eisenhauer, 2001: 4). In popular culture, risk-taking involves the voluntary pursuit of experiencing dangerous activities, like extreme sports, for purposes of pleasure and excitement, or breaking with everyday routine and boredom (Lupton, 1999: 149-150; Zinn, 2009: 106-107). This is referred to as the edgework approach. Edgework "takes place around cultural boundaries: such as those between life and death, consciousness and unconsciousness, sanity and insanity and an ordered sense of self and environment" (Lupton, 1999: 151). It is possible to argue that hacking could involve an element of thrill seeking for some actors, for instance in the case of script kiddies (National Cyber Security Centre, 2017: 19). However, investigating this element extends beyond the purpose of this thesis.

The next part of the thesis first investigates the concept of risk in further detail and offers the theoretical framework. The different conceptual meanings of risk are discussed, followed by a brief historical overview of how the notion of risk evolved over time. Then, the realist and social constructivist perspectives on risk are elaborated upon in chapter four.

Part 1

3. What is risk?

The term risk does not have one well-defined meaning. As a consequence, confusion and misunderstanding has oftentimes characterized (public) debate over issues concerning risk. This can have far reaching consequences as it can influence policy debates, policy making and the allocation of resources (Fischhoff, Watson & Hope, 1984: 123-124; Renn, 1992: 54). This chapter focuses on the different conceptual meanings of the term risk. What is more, history shaped the way in which we consider the notion of risk today. Therefore, the second section of this chapter places the concept of risk in a historical context to show how the meaning of risk has changed over time.

3.1 Defining risk

Defining the term risk is no straightforward task. From a conceptual perspective, different definitions and meanings are ascribed to the concept. Hansson (2005) identifies five different meanings of the term risk. First, he notes that risk can mean an *unwanted event*, which may or may not take place (Hansson, 2005: 7). Second, risk is also often thought of as *the cause* of a potential unwanted event. To add to the complexity, risk is frequently used interchangeably with notions such as hazard, threat, loss, and damage (Hansson, 2005: 7-8).

The third way of understanding risk concerns risk calculation. This entails thinking of risk as the *probability* that an unwanted event may or may not take place. Building on this meaning of risk, the fourth way to explain risk is considered the most common way to express risk from a technical perspective, namely risk defined as the *statistical expectation value* of a possible unwanted future event. In this context, risk is not only understood by looking at the probability that a future event might occur, it also entails identifying and calculating the *consequences* of the event, the expectation value (Hansson, 2005: 7-8). Combining the probability and consequences of a possible future event is the basis of technical risk management which is explained further in chapter four.

Hansson derives the fifth way of looking at risk from decision theory. According to this theory, there is a distinction between decisions made *under risk* and decisions made *under uncertainty*. The difference being that for decisions made under risk, the probabilities that a possible future event will take place are known to the decision maker whereas for decisions made under uncertainty, the probabilities are unknown (Hansson, 2005: 8).

The above meanings of risk all refer to a negative or undesired outcome. It should be added though, that risk can also be used to include positive outcomes. In the context of *risk taking*, the result of taking certain action can be both positive and negative (Zinn, 2009: 4). In insurance theory, this is referred to as *pure risk* and *speculative risk*. Pure risk can be understood as referring to an outcome where there is no chance to gain anything and the only

result is either loss or status quo. Speculative risk, on the other hand, refers to a situation in which the outcome can constitute of both gains and losses (Williams, 1966: 577; Halek & Eisenhauer, 2001: 4).

As the above illustrates, the common denominator of all interpretations and meanings of risk, is the idea that risk has to do with the concept of uncertainty. How mankind has dealt with this uncertainty has differed throughout history. Consequently, the meaning of risk has changed considerably over time. The next section describes the historical context of risk in more detail.

3.2 A short historical overview of risk

There is no clear origin of the word risk (Luhmann, 1993: 9). The term risk can be traced back to the Latin term riscum which was used during the Renaissance period (Lupton, 1999: 5). In Europe, mention of the term risk appeared in Germany, Risiko, in the mid sixteenth century and became part of everyday language in the early eighteenth century (Zinn, 2009: 8; Lupton, 1999: 5). Moreover, the Oxford English Dictionary traces the term risk back to the mid seventeenth century to the French Risque and the Italian Risco meaning danger (Zinn, 2009: 7).

According to Bernstein (1996), there are two interrelated aspects that are at the heart of the development of thinking in terms of risk. The first concerns the introduction of the present-day numerical system as the foundation for the development of methodologies for calculating probabilities and odds. The second aspect involves humankind realizing that the uncertainty of the future could in fact be influenced and managed by humans (Bernstein, 1996: 1-2, 23, 35). Both aspects are elaborated upon below.

In order to create meaningful calculations of probabilities and odds of possible future events, the introduction of the modern day numerical system was essential (Bernstein, 1996: 22-23). Before the introduction of numbers, and most notably the invention of zero, numbers were expressed by means of letters (Bernstein, 1996: 29, 32). The Greeks developed such a letter-number system in 450 BC, followed by the Hebrews and Romans. Even though these systems were helpful to some degree, they were not suitable for even simple calculations like adding and subtracting (Bernstein, 1996: 29-30). The Hindus created the numerical system in 500 A.D. and the Arabs encountered and adopted this numbering system when they swept through India. From here, the system eventually spread to the rest of Europe as well and the field of mathematics developed considerably (Bernstein, 1996: 23-28, 31). Nevertheless, the introduction of the numerical system and the development of mathematics hereafter was not enough to spark the thinking of risk (Bernstein, 1996: 35).

This has to do with the second aspect that forms the foundation of thinking about risk. Humankind needed to gain the idea that the uncertainty of the future could somehow be influenced and managed by people (Bernstein, 1996: 1-2, 28, 35). Bernstein (1996) argues that is was not until the Renaissance that humankind started to think of the future as manageable (Bernstein, 1996: 18). Before that time, risks were considered natural events, acts of God, and matters of fate and luck that humans had no influence on (Bernstein, 1996: 18; Lupton, 1999: 5). A notable development in the change of this belief was the emergence of maritime trading in the 1500s and 1600s (Lupton, 1999: 5; Bernstein, 1996: 21). Confronted with the dangers and challenges of oversea travels, traders and seafarers needed to start thinking in terms of business forecasting (Bernstein, 1996: 21, 95). As a result, an early form of insurance to protect their business ventures against possible losses arose (Zinn, 2009: 9).

The notion of risk developed further as society transitioned towards modernity (Lupton, 1999: 5). The process of modernity started in post-feudal Europe and is understood as the transition towards an industrialized world. At the foundation of the idea of modernization is the idea "that the key to human progress and social order is objective knowledge of the world through scientific exploration and rational thinking. It assumes that the social and natural worlds follow laws that may be measured, calculated and therefore predicted" (Lupton, 1999: 6). It was during the eighteenth and nineteenth century, the Industrial Revolution, that the science and mathematics of statistics and probabilities was developed further. Through these processes, uncertain and unpredictable futures were considered to be brought under control. What is more, the meaning of the term risk expanded to include the idea that human agency influences uncertain future events and the control of such events (Lupton, 1999: 6-7).

Within this context, the distinction between risk and uncertainty, as mentioned in the previous section, was developed. Thus, risk in its technical context is understood as the condition in which the probabilities of possible future events are considered knowable. Alternatively, uncertainty is considered the situation in which the probabilities of possible future events are unknown (Hansson, 2005: 8; Lupton, 1999: 7).

The difference between pure risk and speculative risk in insurance theory, as mentioned in section 3.1, also results from the process of modernization. It is even argued by some scholars that a so-called *insurance society* advanced resulting in the notion that everything can be insured (Zinn, 2009: 9). The difference between 'good' and 'bad' risks dominated until the beginning of the nineteenth century. It is argued, however, that at the end of the twentieth century this differentiation has diminished. While the more positive notion of speculative risk is still used in terms of insurance and economic speculation, in everyday language the term risk is generally considered as negative and equivalent to danger, threat, or hazard (Lupton, 1999: 8-9).

In contemporary western society, the concept of risk is strongly incorporated into the research practices of experts that operate in diverse fields of science. As Lupton (1999) argues,

> "An apparatus of expert research, knowledge and advice has developed around the concept of risk: risk analysis, risk assessment, risk communication and risk management are all major fields of research and practice, used to measure and control risk in areas as far-ranching as medicine and public health, finance, the law, and business and industry." (Lupton, 1999: 9).

Not only has the subject of risk proliferated in academic research, it is also increasingly referred to in the news media in the context of a danger, threat, or hazard (Furedi, 2006: 8; Zinn, 2009: 4). A number of factors are offered to account for this increasing use of the term risk. First, the progress made regarding probability research and computer technologies made it possible to create complex statistical analysis that were not possible before. Second, it is claimed that such statistical research has gained in importance as it now forms the foundation of what society regards as certainty (Lupton, 1999: 10). Third, it is argued that in the transition towards contemporary western society a large number of changes took place after the second World War, examples include the end of the Cold War, the introduction of communication technology, the feminist movement, and the process of secularization. This subsequently resulted in the questioning and breakdown of previously held norms and traditions. As a result, it is argued that the individual in contemporary society is confronted with higher levels of uncertainty, complexity, a sense of disorder, and distrust of institutions and authorities. What is more, the individual has gained greater levels of risk awareness (Furedi, 2006: 8-9). Some writers even claim that individuals in contemporary society experience constant low-levels of fear. It is argued by some scholars that risk now represents feelings of fear, anxiety, and uncertainty in society. Paradoxically, all the strategies and studies conducted aiming to address and mitigate risk only increase the general anxiety about risk (Beck, 2006: 332).

Summary

The conceptual meaning of the word risk differs greatly which can result in misunderstandings when trying to address risk. Overall, it can be stated that risk has to do with uncertainty. This is an important notion, as throughout history mankind has progressively tried to bring the uncertain future under control. At the foundation of this endeavor are two factors: the introduction of our present-day numerical system, and the realization of humankind that the future can be predicted and influenced by human intervention. In the process of modernization, the idea that objective knowledge is necessary to address and predict future risks was increasingly valued. In response to this, and because of further technological developments, the mathematics of statistics and probabilities was developed and now forms the basis of the way in which we address risk. In contemporary society, risk is increasingly present, and risk management practices are strongly incorporated into many different research areas. This results in greater risk awareness within society and a general feeling that

risks need to be mitigated. It is argued however, that all the efforts to study and address risk only increase the general apprehension of risk in contemporary society.

4. The realist and social constructivist perspectives on risk

Different theoretical perspectives on risk exist. This chapter investigates the realist and social constructivist perspectives in further detail. As a result, a theoretical framework is presented that forms the basis for further study in chapters five and six.

4.1 The realist perspective

As elaborated upon in the previous chapter, the transition of society towards modernity brought forth the notion that risk can be understood and addressed by means of objective knowledge and through statistical and probabilistic analysis. It is within this context that the realist perspective can be understood. According to Lupton (1999) the realist perspective is the most common perspective towards risk (Lupton, 1999: 17). The realist perspective holds that risks are real and physical events or hazards that can be objectively observed and determined. As the realist notion implies, risks are considered real not only in their consequences, but also as objective events and facts (Zinn, 2009: 4-6; Renn, 1992: 55). Lupton (1999) ads that according to this perspective, risks "are pre-existing in nature and in principle are able to be identified through scientific measurement and calculation and controlled using this knowledge" (Lupton, 1999: 18). It is within this realist perspective that modern day risk management can be understood (Zinn, 2009: 7-8).

4.1.1 Risk management

The first studies on risk management as we know it today were conducted after World War II (Dionne, 2013: 147). It was during this period that technological risk management models were starting to be designed in response to the industrialization of society and because of ensuing concerns for the environment, and public health and safety (Dionne, 2013: 147; Berg, 2010: 80; Kasperson et al., 1988: 177). Risks to the environment and public health and safety were seen as direct results of progress made in the fields of science, technology and industry (Lupton, 1999: 18). Risk management therefore originated in fields such as engineering, statistics, actuarialism, toxicological and epidemiological research, and probabilistic risk management (Lupton, 1999: 17; Zinn, 2009: 5).

In this context, risk is considered a safety issue, meaning that risks are unintentional and do not entail human agency (Hessami, 2004: 99-100; Reniers & Cozzani, 2013: 6). As described above, risk management originated in response to industrialization. So, initially risk management was designed for technical and mechanical environments, and closed industrial systems (Kriaa, Pietre-Cambacedes, Bouissou & Halgand, 2015: 157). The causes of risks in these systems are internal and stem from component failures or human errors. The risks are thus considered accidental in nature, and the frequency of these accidents occurring is generally very low (Abdo, Kaouk, Flaus & Masse, 2017: 2). This focus on risk as a safety issue is in contrast to what is understood as the security paradigm which considers risks as

intentional acts caused by human actors (Hessami, 2004: 100). The security paradigm is elaborated upon in section 4.2.

As elaborated upon in chapter three, the most common way to express risk from a technical perspective is by calculating the probabilities and potential consequences of unwanted future events (Abdo, Kaouk, Flaus & Masse, 2017: 2). To conduct these calculations, researchers look at past events in order to make predictions about the future. In order to be successful and create reliable calculations, there should be enough statistical data available, and future conditions need to be comparable to the past situation that was measured. What is more, this process only applies in conditions with limited complexity and not too many variables (Bernstein, 1996: 6; Zinn, 2009: 5; Renn, 1992: 58). Also, should there be limits to the calculability of risks, realists consider this as a situation that can be resolved by doing further research and creating better analysis (Zinn, 2009: 5).

So, the essence of risk management is to calculate the likelihood and consequences of potential unwanted events. Yet different definitions exist of what exactly constitutes risk management (Berg, 2010: 80). Certain definitions consider risk management as solely a decision-making process that does not include the identification and assessment of risks. There are other definitions that consider risk management as a more integrated process that does include identification, assessment and decision-making processes (Berg, 2010: 80-81). In line with the more integrated approach to risk management, a generally accepted definition of risk management is provided by Berg (2010) and explains risk management as “a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues.” (Berg, 2010: 80). Figure 1 provides a schematic overview of these elements. The rationale behind integrated risk management is that organizations are dealing with increasingly diverse (operational) processes, which result in complex and interrelated risks. Consequently, responses need to be designed in a coordinated and systematic manner in order to achieve the overall strategic objectives of the organization (Berg, 2010: 81).

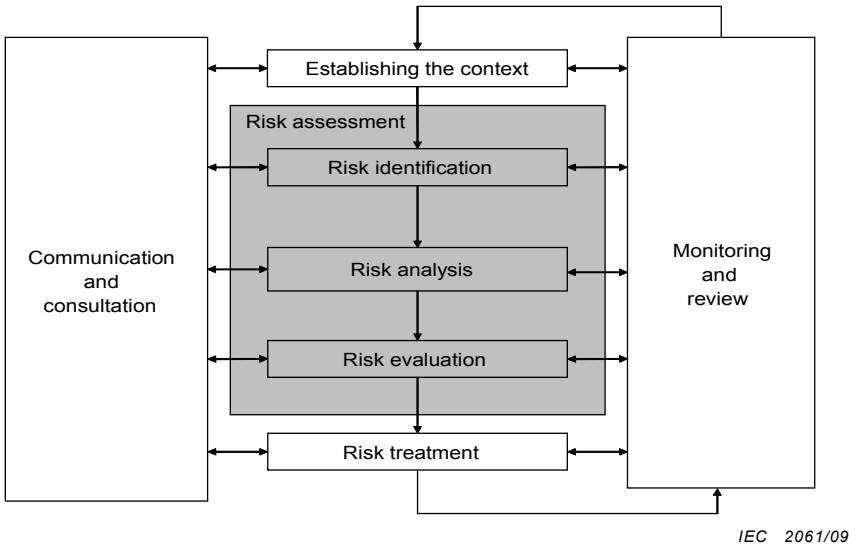

Figure 1 – Risk management process (ISO/IEC 31010, 2009: 11).

As mentioned above, risk management works best in situations where there is enough statistical data, where there is limited complexity in terms of variables, and where past conditions are comparable to future conditions (Berg, 2010: 80,82; Zinn, 2009: 4-5; Kasperson et al., 1988: 178). This is illustrated by looking at the different methods of risk management that are used within different disciplines. Three methods of risk management can be identified, the actuarial approach, the toxicological and epidemiological approach, and the probabilistic approach (Renn, 1992: 57, 59). All three risk management methodologies aim to predict physical harm to human beings or systems, establish averages of the events causing this physical harm over time and space, and make use of frequencies to establish likelihood. They differ in the technique that is used to make these calculations and are explained below (Renn, 1992: 59).

The actuarial approach employs a mathematical and statistical analysis aimed at establishing the relative frequencies of certain events over time. It is an approach that originates in the field of insurance. An example of this method is trying to predict the number of traffic fatalities for the coming year by looking at the number of traffic fatalities, which is referred to as the expected value, of the previous year (Renn, 1992: 58). The toxicological and epidemiological approach is used to establish health and environmental risks. This is done by determining and quantifying causal relations between sources of potential physical harm and effects of these sources on living organisms or environmental systems. The third approach, the probabilistic approach, is applied in the field of safety engineering. It entails a so-called fault-tree or event-tree analysis to calculate failure probabilities of the separate components that exist within a complex technological system. As a result of the analysis, it is possible to establish the failure rate of the technological system as a whole (Renn, 1992: 59).

4.1.2 Responses to risk

The result of the different risk management methods is calculating risk levels. The purpose of creating risk levels is to make informed decisions about the required course of action, or risk treatment, that is to be taken (Abdo, Kaouk, Flaus & Masse, 2017: 1-2). Different types of risk treatment exist; it is possible to accept, avoid, reduce or mitigate, and transfer risks (Berg, 2010: 86). In order to decide on the appropriate measure, it is necessary to establish acceptable risk levels. Deciding whether a risk is acceptable or not depends on a cost-benefit analysis (Arunraj & Maiti, 2007: 653). A risk can be acceptable if it is considered sufficiently low as not to result in considerable benefits should a measure be taken to address the risk (Berg, 2010: 81). It is also possible that there are no treatments available for a specific risk. It should be added that it is never possible to completely eliminate risk. Residual risks remain and it is difficult to address risks that we do not yet know of (Berg, 2010: 86). As a consequence, risk management can be considered a mechanism that is to reduce risk to acceptable levels (Abdo, Kaouk, Flaus & Masse, 2017: 1-2; Ionita, 2013: 12).

4.2 The social constructivist perspective

As the notion implies, social constructivism considers risk as a socially constructed concept that is determined in specific social and cultural contexts and is the result of the social and cultural processes that apply to these contexts. Risks are determined by social interaction where meaning and values are applied to the concept of risk (Lupton, 1999: 29; Zinn, 2009: 6-8). Consequently, according to this perspective, risk is contingent in nature (Lupton, 1999; 25). So, within social constructivist perspective, risk is seen as a complex construct where human interaction steers the appreciation and determination of risk (Zinn, 2009: 6-8).

As opposed to the realist perspective, the social constructivist perspective holds that risks cannot (merely) be determined by objective calculation and measurement. Even though most realists would acknowledge that objective risk management is never completely possible, as human bias and values can never be fully eliminated from the process, the results of risk management calculations tend to be presented as facts and absolute truths (Lupton, 1999, 18). Social constructivists challenge this notion and state that the determination of risk is an outcome of cultural and social values that influence the entire process of establishing risk (Kasperson et al., 1988: 177-178; Renn, 1992: 54-55). An example of determining risks through social interaction is by means of ‘discourse’. It is through discourse, including the formation of strategies, practices, and institutions that risks can be brought into being and can be addressed through action or intervention (Lupton, 1999: 84-85). Thus words – the discourses – are used to describe, classify, characterize, and explain problems as being risky (Zinn, 2009: 56).

In contrast to the realist perspective, it is within the social constructivist perspective that a more security focused idea of risk applies. This entails the notion that risks arise due to intentional acts involving human actors. As a result, it is the responsibility of humans to control these risks. However, as opposed to the realist view on risk, calculating the probabilities of security risks is much more difficult because determining human behavior is not static (Hessami, 2004: 99-100; Reniers & Cozzani, 2013: 6; Beck, 2006: 329; Lupton, 1999: 64-65). What is more, in this context the malicious actors and their capabilities are often unknown which makes the determination of the risks stemming from these actors an elaborate endeavor involving the assessment of an extremely wide variety of different possible scenarios (Kriaa, Pietre-Cambacedes, Bouissou & Halgand, 2015: 159).

As mentioned in chapter two, different approaches can be placed under the social constructivist perspective (Zinn, 2009: 6-8; Lupton, 1999: 16). What they have in common is that all approaches tend to focus on characteristics of risk within contemporary western societies. What is more, it is argued that within these societies risk has become a central and omnipresent feature of culture and politics. As a result, risk is used to organize, monitor and regulate individuals, societal groups and institutions. Additionally, risk is considered something that can be contained and controlled by means of human intervention. Consequently, risk has come to be directly related to concepts like choice, responsibility and blame (Lupton, 1999: 25).

Despite these similarities, the approaches differ in terms of how strongly they consider risks to be socially constructed. Some approaches are considered as weak social constructivist and some are regarded as strong social constructivist approaches. Weak social constructivist approaches recognize, like the realist perspective, that risks are real dangers or hazards that can objectively be determined. Yet, they also acknowledge that there is a difference between a risk itself and the perception of it (Lupton, 1999: 59-62). Strong social constructivists, in contrast, pose that risks do not exist unless we choose to define and recognize an issue as a risk. As such, risks result as products of social processes that are strategically used in the public domain to fix attention on one type of risk and not another (Zinn, 2009: 6-7).

These notions are further highlighted below by looking at two social constructivist approaches in more detail. The first entails the risk society and reflexive modernization approach. The second is the securitization approach, which is a social constructivist approach that was developed with a specific focus on how security issues are brought into being.

4.2.1 Risk society and reflexive modernization

The notion of risk society was first published by the German author Ulrich Beck in 1986 (Zinn, 2009: 18). Beck differentiates the way in which western society regards the notion of risk by comparing pre-modern and early modern societies with late, also referred to as contemporary or modern society (Lupton, 1999: 62). The author argues that as a result of the modernization

of society, and accompanying technological and economic progress, the focus of society has shifted from a primary concern over the establishment of wealth to a concern over the prevention of risks (Beck, 2006: 332; Zinn, 2009: 20). He refers to this as the creation of the so-called risk society. As a consequence, debates over risk govern the political domain and extend to the concern of individuals resulting in a greater consciousness and apprehension of risk (Beck, 2006: 332-333). The writings of Beck are considered weak social constructivism. On the one hand, he considers the realist practices of calculating and measuring risks to be useful. On the other hand, he states that these objectively calculated risks are subsequently interpreted in cultural and political processes (Lupton, 1999: 60).

Beck goes on to mention three characteristics of risks within the context of the risk society. First, risks have become global in contemporary society (Beck, 2006: 333-334). Where risks tended to be more personal in nature and experienced on a local scale or bound by borders of the nation state in pre-modern and early-modern society, risks in late modern society can result in global impact. Beck takes a rather apocalyptic view towards these global risks, and describes them as irreversible with the potential to destroy humanity and other living beings as a whole (Lupton, 1999: 59-61). Examples mentioned by Beck include environmental and nuclear risks. As such, risks have become de-localized. As a result of this globalization of risk, risks are becoming increasingly difficult to quantify, prevent and resolve, which makes them more enduring as well (Beck, 2006: 333-334).

This leads to the second characteristic of the risk society: risks are becoming more difficult to calculate (Beck, 2006: 334). As mentioned in chapter three, in pre-modern society, risks were considered incalculable because they were seen as acts of God that humans had little control over. As statistical and probabilistic calculation developed in early modernity, uncertain and unpredictable futures were considered to be brought under control, and thus the idea of the calculability of risk was established. Beck argues that the global nature of risk in late modernity has again made risks incalculable as their effect and impact are no longer contained in space and time (Beck, 2006: 334). Added to the difficulty of calculating risk in contemporary society is the notion that risks and their effects are becoming more complex and often unobservable. This also makes it more difficult to assign blame and responsibility should things go wrong as cause and effect can no longer be clearly related (Beck, 2006: 334).

Building on the second characteristic of incalculability of risk, the third characteristic that Beck mentions is the non-compensatibility of risk. This notion entails the idea that technological progress in early modernity made it possible not only to calculate risk, it also became possible to mitigate and control these risks by designing interventions. However, risks in late modernity are considered irreversible in nature, meaning that once the damage is done, there is no going back. Examples mentioned by Beck are the effects of climate change and terrorists gaining access to weapons of mass destruction. This means that instead of focusing on mitigation and control, the focus shifts to precaution by means of prevention. This is referred to as the

precautionary principle (Beck, 2006: 335, 337). What is more, Beck argues that as a result of focusing on prevention, society is increasingly trying to anticipate risks that are not even proven to exist yet (Beck, 2006: 333-334). This idea also poses challenges for politics, as politicians are tasked to provide security even though they might not know the true extent of certain risks. Consequently, political action could result in overreaction as the political cost of not acting is higher than the political cost of overreacting (Beck, 2006: 335-336).

It is within this setting that Beck offers the idea of reflexive modernization (Beck, 2006: 338). He uses this term in order to describe how early modernity, the period of industrialization in the early twentieth century, automatically transitioned into late modernity established in the late twentieth century. As a result of this transition, risks in late modernity arise as a result of the process of modernization itself and consequently become globalized in nature. In response to this transition, and the creation of the subsequent risk society, it becomes necessary to respond to risk on an international level. This means that international institutions, alliances, and actions are needed to address risks at a global level. As a result, the notion of the risk society transforms into a notion of a 'world risk society' (Beck, 2006: 333, 338). The term reflexive modernization is thus used in the sense that society is confronted by the effects of the process of modernization itself and as a result must reflect on this process resulting in increased awareness of the consequences. As a result, people now face a constant struggle over what constitutes risk and thus, risks have become highly political (Beck, 2006: 336).

It is not only Ulrich Beck who has written about the twenty-first century risk society and reflexive modernization. His work is complemented by the work of Anthony Giddens who portrays similar views in his writings in the 1990s (Giddens, 1999). Like Beck, Giddens takes a weak social constructivist approach identifying risks as hazards or dangers that objectively exist in the world and can be brought under control by means of risk management, yet he recognizes that this cannot be done in precise manner. He also recognizes that risks are socially constructed (Giddens, 1999: 3-4). What is more, in line with the notion of reflexive modernization, Giddens agrees that the process of modernization and human progress resulted in a less utopian future than imagined. As a result, society now faces greater uncertainty than before and it is the responsibility of humankind to address this (Giddens, 1999: 6). The authors differ in the sense that they take a different view regarding the nature of this idea of greater uncertainty. Where Beck considers greater uncertainty as the result of in fact a greater number of risks posed towards society due to the process of modernization, Giddens claims that society does not face a greater number of risks. Instead, society has become less tolerant of risks (Giddens, 1999: 3).

What is more, Giddens differs from Beck by including the notion of trust in his writings. He argues that, with the introduction of modernity, society has introduced abstract expert systems, for example our monetary system, that requires trust in the system to work. As a

result, he argues, people become reliant on systems that are often invisible but directly affect our lives. Should these systems fail the repercussions can be enormous and have effects on a global level. He states that by instating trust in expert knowledge and systems, people create a protective cocoon to guard themselves against risk and uncertainty (Giddens, 1990: 35-36).

4.2.2 Securitization

Building on the notion that risks are very much political is another social constructivist approach, that of securitization (Vuori, 2017: 64). Even though different definitions of securitization exist, there is a general logic that scholars use to explain what securitization involves (Bourbeau, 2015: 395). According to this logic, securitization is understood as the socio-political process of labeling a phenomenon as a security issue by means of speech acts (Vuori, 2017: 64-65; Bourbeau, 2015: 396). The speech acts are used to position the phenomenon as an existential security threat. As a result of this process, the phenomenon becomes the highest priority on the political agenda which allows for the introduction of exceptional emergency measures and policies to address the issue (Vuori, 2017: 65; Bourbeau, 2015: 396).

Securitization was introduced in the 1990s when discussions on the scope of security studies arose. Those in favor of the traditional view argued that the field concerns the study of the phenomenon of war and the role of state therein, also stipulated as the study of national security (Vultee, 2010: 34, Nissenbaum, 2005: 66). Opposing this idea were those scholars who claimed that the perspective should be widened to include issues besides war and the traditional role of the state (Vultee, 2010: 34). In response, scholars at the Copenhagen School introduced the notion of securitization that allows for a broadening of the scope to other issues besides national security while at the same time holding on to the traditional focus on the role of the state (Vultee, 2010: 34).

Thus, securitization constitutes the process in which intentional action is taken with the specific goal of convincing an audience of that a specific issue constitutes a security threat, and moving this threat up on the political agenda (Vuori, 2017: 65). In the process of securitization, an issue starts out as being non-politicized meaning that the issue is not part of the public debate, nor does the state deal with it. As the issue subsequently becomes politicized, it becomes part of public debate and the state needs to start making decisions on the subject and allocate recourses to address it. In the transition from politicized to securitized, the issue becomes the highest item on the agenda and "is no longer debated as a political question, but dealt with at an accelerated pace and in ways that may violate normal legal and social rules" (Hansen & Nissenbaum, 2009: 1158-1159).

The process of securitization does not only need to be portrayed as an existential security threat as described above. What is also required is a threatened referent object and a securitizing actor. Referent objects are (collective) goods that are threatened by the issue that

is being securitized (Vuori, 2017: 65). An example of a referent object is the security or functioning of the nation-state itself, but it can also be the environment, religion, culture, or the economy for instance (Nissenbaum, 2005: 66). Another important aspect of the process of securitization is that of agency. In other words, who is capable of securitizing? Most often securitizing actors are high-ranking government officials or politicians. Yet, it is possible for other actors to securitize. Examples include media actors, highly visible lobbyists or pressure groups (Nissenbaum, 2005: 66-67).

Establishing whether or not a speech act has successfully securitized an issue is a contested principle within securitization literature. Some argue that successful securitization involves gathering enough potential support for security measures, others claim that these security measures need to be implemented before an issue is successfully securitized (Vuori, 2017: 67). In general, successful securitization depends on the power and capability of a person, or persons, to socially and politically construct an issue as a security threat and have it accepted as such by the audience (Vultee, 2010: 34). This is not to say that an entire audience needs to be completely convinced of the urgency. What is more, this process does not have to happen overnight, it can be gradual process as well (Nissenbaum, 2005: 69-70).

The securitization process can have far-reaching consequences. If successful, securitization can break the rules that normally restrict certain behavior and certain policies. If society is confronted by an existential security threat, this allows for the introduction of exceptional emergency measures. The rationale behind this seems logical at first. If society is faced with an imminent and dire security threat, as the securitization discourse implies, it is logical that efforts are taken to try and stop it before something happens (Nissenbaum, 2005: 71). However, in the case of securitization this often includes measures to reduce restraints on government power, changes to normal democratic procedures and civil liberties, and increased funding for security agencies and infrastructure. The most evident example of this process is perhaps the introduction of the Patriot Act in the United States in response to the terrorist threat. It is therefore argued that the process of securitization needs to be carefully scrutinized (Nissenbaum, 2005: 70).

Summary

This chapter investigates two conceptions of risk in more detail. The realist perspective is considered to be the most common theoretical perspective on risk. Realists view risks as real and physical events or hazards that can be objectively observed and determined through risk management. Risk management originated in response to industrialization and ensuing concerns over public health and safety, and the environment. Within the fields of natural-science, technology and engineering, risk management developed to address component failures and human errors in closed industrial systems and mechanical environments. From this perspective, risk is considered a safety issue, and risks result from unintentional accidents. The foundation of risk management is the calculation of risk levels, most commonly conducted

by multiplying the likelihood and impact of unwanted events based on statistical and probabilistic data. Risk management requires statistical data and works best in closed environments with limited complexity and variables.

In contrast, the social constructivist perspective considers risk as a complex social construct, which is determined by social and political processes, interaction, values, and discourses. It is within this perspective that human agency is a central element, both in terms of causing risk and in containing it. Two approaches within this perspective are highlighted. First, the risk society and reflexive modernization approach, offered by Ulrich Beck and Anthony Giddens, states that as a result of the process of modernization, risks have become a central and omnipresent feature of culture and politics. Risks have become global, incalculable, complex, political, and potentially catastrophic resulting in a risk society in which there is a greater apprehension of risk. Second, the securitization approach constitutes the socio-political process in which an issue is framed as an existential threat and labeled as a security issue. The intention is to convince an audience of the catastrophic nature, and make it the most urgent matter on the political agenda. Securitizing an issue often results in exceptional emergency measures being taken and the process should therefore be carefully scrutinized. In the next chapter, both conceptions of risk are used to investigate how they frame the way in which the issue of cyber security is perceived.

Part 2

5. How do the conceptions of risk shape the framing of cyber security?

The theoretical framework presented in the previous chapter describes both the realist and social constructivist conceptions of risk. Based on this framework, this chapter illustrates how the realist and social constructivist conceptions of risk shape the way in which cyber security is framed and consists of three parts. In the first part of this chapter it is examined how the risks regarding cyber security can be portrayed from the realist perspective. This includes taking a closer look at what constitutes cyber security, how cyber security can be regarded from a technical point of view, and how the risks related to cyber security are addressed via risk management practices. The second part of this chapter takes a closer look at the limitations of risk management in the field of cyber security. The third part provides a number of examples of social constructivist discussions regarding cyber security. The aim is to illustrate how social constructivist thinking offers different insights regarding the risks related to cyber security than looking at them from the realist perspective.

5.1 Cyber security from a realist perspective

As indicated in chapter four, the realist perspective views risks from a technical, natural science, and engineering outlook. In this context, risks are considered real, objective dangers or hazards that can be identified through risk management practices. This section investigates how the risks regarding cyber security are viewed from the realist perspective. What is more, it is examined how the risks regarding cyber security are addressed by means of risk management practices.

5.1.1 From information security to cyber security: a short overview

In order to find out how cyber security fits in with the realist conception of risk, it is necessary to look at the origins of cyber security. The term cyber security as such did not exist when computers and the internet first came into existence. What did exist was the notion of 'information security'. Concerns over information security started as soon as humankind started to write messages and develop the need to keep what was written secret. Over the course of history, information security was applied to information that was sent through telegrams, the telephone, and through computers. Thus, the origins of information security primarily focused on keeping transmitted information and data confidential (Dlamini, Eloff & Eloff, 2009: 2).

However, computers developed from stand-alone units requiring data to be physically transferred between them in the 1940s up to the 1950s, to multi-user and time-sharing mini computers that were connected through networks in the 1960s up to the 1970s, and to the creation and adoption of personal computers and the development of the internet starting

from the 1980s up to the late 1990s. As ICT-systems and their application became more advanced, the challenges with regard to information security changed along the way (Dlamini, Eloff & Eloff, 2009: 2-3). Information and data were quite safe in the stand-alone computer of the 1940s and 1950s. Viruses and worms were developed during the 1980s and spread through the use of floppy disks but were considered minor annoyances at first. However, nowadays they can infect thousands of systems in a matter of seconds (Dlamini, Eloff & Eloff, 2009: 2-3). Therefore, information security needed not only concern itself with safeguarding the confidentiality of information, it became necessary to focus on the integrity and availability of information as well; this came to be known as the CIA triad for information security (Dlamini, Eloff & Eloff, 2009: 2-3; van den Berg et al., 2014: 2).

There are variations with regard to the definition of information security. In general, it can be understood to mean "the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information" (Whitman & Mattord, 2011, 8). This is to be accomplished by ensuring the confidentiality, integrity, and availability of information. It should be emphasized that, as the above-mentioned definition suggests, information security does not only focus on securing the information itself but also the systems that are used to process the information. Consequently, information security includes data, computer, and network security as well. This is sometimes referred to separately as information and communication technology (ICT) security[2] (Von Solms & Van Niekerk, 2013: 98-99).

Up until the early 1990s, information security was almost entirely considered a technological issue existing in the realm of computer sciences and engineering (van den Berg et al., 2014: 2; Dlamini, Eloff & Eloff, 2009: 7; Humphreys, 2008: 247; Wood, 2004: 16). As mentioned above, the continuous development of new technologies to improve computers and networks resulted in the development of new security risks as well. In turn, these security risks were addressed by developing new technological solutions (Humphreys, 2008: 247; Dlamini, Eloff & Eloff, 2009: 7). Providing security measures with regard to the CIA triad was in the hands of technical experts (van den Berg & Keymolen, 2017: 190). For example, as early as the 1970s the first encryption standard was developed, the Data Encryption Standard, by the American National Bureau of Standards the forerunner of the National Institute of Standards and Technology (NIST) that we know it today (Dlamini, Eloff & Eloff, 2009: 3, 7).

It was not until the 1990s that this technical perspective started to broaden (Humphreys, 2008: 247). This was due to the fact that as a result of the technological progress made, ICT-systems were increasingly used for diverse applications involving human interaction. As a result, what is now referred to as cyberspace was created. Cyberspace is considered the realm where technology, including hardware, software, and information systems, interact with

[2] In the remainder of this thesis, when information security is mentioned, it includes ICT security as well.

people (van den Berg et al., 2014: 1-2; Klimburg, 2012: 8). As a result, the focus on technical information security alone is somewhat diminished. Accordingly, the CIA triad is considered too limited as well, resulting in additions such as authenticity and accountability as well (Von Solms & Van Niekerk, 2013: 98; Stallings, 1982: 5). In line with these developments, it is now increasingly recognized that addressing the risks in cyberspace requires a broader, more strategic, and multi-disciplinary approach (van den Berg et al., 2014: 1-4; Dlamini, Eloff & Eloff, 2009: 7; Wood, 2014: 16-17; Humphreys, 2008: 247).

It is this transition from a purely technical focus to a multi-disciplinary approach that constitutes the shift from information security to the idea of cyber security (Von Solms & Van Niekerk, 2013: 100; van den Berg et al., 2014: 1). This is not to say that the technical aspects are considered less important, it is to indicate that the scope of what constitutes security and risk in cyberspace has extended (Dlamini, Eloff & Eloff, 2009: 7). As such, cyber security is considered to encompass the same notions as information security but includes issues that are not necessarily technical as well. This includes the security of people, processes, and organizations (Dlamini, Eloff & Eloff, 2009: 7; Von Solms & Van Niekerk, 2013: 98, 101; Humphreys, 2008: 247).

Van den Berg et al. (2014) endeavor to capture this transition by offering a conceptualization of cyberspace. This conceptualization of cyberspace asserts the necessity of looking beyond the primary focus on technology whilst analyzing cyberspace in order to understand the opportunities and risks this domain holds. The conceptualization stresses the need to look at the socio-technical layer, which has been created on top of the technical layer, and has enabled the many cyber activities that we are currently able to perform. These cyber activities consist of the multifaceted interaction between people and the ICT systems. The authors provide a third layer to their model, the governance layer, which consists of a large number of human actors and organizations that govern both the technical and socio-technical layers (van den Berg et al., 2014: 2).

It should be noted that there is no widespread consensus of what defines and constitutes cyber security exactly. Many countries around the world now have cyber security strategies including their own definitions of cyber security, which may lead to confusion when the risks regarding cyber security are discussed (Klimburg, 2012: 12; Luiijf, Besseling & De Graaf, 2013: 5). What is more, it is argued that the broadened meaning of cyber security is primarily used by those concerned with policy making and governance, whereas the technical community prefers to hold on to the notion of information security (Van der Meulen, 2015: 10-11).

5.1.2 Cyber security risk management

Against this historical background, risk management methodologies were developed and adopted for information security starting in the 1980s. Over the years, a vast amount of different risk management methodologies including standards, frameworks, regulations and

tools have been created to address the risks related to information security and cyber security (Ionita, 2013: 115). Unfortunately, there is no comprehensive information available on the history, usage, and popularity of all the different methodologies (Harpes et al., 2014: 3; Soo Hoo, 2000: 6, 9). Nevertheless, studies that aim to create non-exhaustive overviews of the different risk management methods can easily include up to 46 different methodologies (Ionita, 2013: 115; Harpes et al., 2014: iii-iv).

The different methodologies that exist today all differ in terms of aim, scope, applicability, protection requirements, and usability (Ionita, 2013: 115). What is more, they all include a conceptual model of risk, yet the way in which risk is defined, operationalized and measured differs greatly between the different methodologies. Nevertheless, central to almost all risk management methodologies is the determination of risk levels by calculating the likelihood and impact of events (Ionita, 2013: 116; Soo Hoo, 2000: 4). Overall, it can be stated that the different risk management methodologies are closely related to the traditional risk management methodologies that were originally developed outside the field of information security or cyber security, as described in section 4.1.1 (Ionita, 2013: 116).

One particular framework is considered to be most widely used and accepted nowadays. That is the international ISO/IEC set of Information Security standards (Ionita, 2013: 115; Humphreys, 2008: 248). This framework includes standards[3] with regard to general ICT security and management issues, specifications on the implementation and maintenance of an information security management system, and information on how to conduct risk assessments (Ionita, 2013: 115). What is more, most other risk management methodologies make use of the ISO/IEC framework as the basis for their own methodology or at least refer or comply with the framework (Ionita, 2013: 116).

It should be added that the ISO/IEC framework is considered abstract and high-level, aiming to create a comprehensive risk management system instead of focusing on specific technical requirements. Even though the framework does not refer to cyber security as such, it is considered to be a multi-disciplinary framework aiming at reducing risk at all levels of an organization including requirements for managing people, information, processes, services, IT and physical assets (Ionita, 2013: 116; Humphreys, 2008: 248).

5.2 Limitations of cyber security risk management

As mentioned above, unfortunately there is no comprehensive data available regarding the usage and popularity of risk management methodologies in the field of cyber security. Nevertheless, the sheer number of different risk management methodologies that have been developed could serve as an indication of their application in the field. As stated in chapter

[3] The most relevant ISO/IEC standards regarding information security and risk management include: ISO/IEC 13335-1, ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27005 (Ionita, 2013: 115).

four, risk management was originally designed for closed technological environments. As such, successful risk management requires conditions with limited complexity and variables, enough statistical data, and future conditions that are comparable to past conditions. However, it was also mentioned in chapter four that in the world risk society, risks have become global and de-localized resulting in risks becoming incalculable, complex and unobservable. The next paragraphs illustrate that meeting the requirements for successful risk management proves challenging in the field of cyber security as the risks pertaining to this field are global, complex and dynamic.

5.2.1 Complexity

The cyber security domain is complex in a number of ways. First, in order to perform calculations of impact and likelihood, the risk management process involves detailed analysis of a number of different categories[4], including: threats, vulnerabilities, controls, losses, and incidents (Soo Hoo, 2000: 5; Blakley, McDermott & Geer, 2001: 99-100). A major problem with these calculations in the field of cyber security is that they quickly become too complex as many different variables can be identified for each category (Soo Hoo, 2000: 7). To illustrate this point, over a thousand different vulnerabilities were reported to the Common Vulnerabilities and Exposures (CVE) website for the month December 2017 alone (Common Vulnerabilities and Exposures, 2017).

Second, the complexity of risks in the field of cyber security can be explained by looking at the interconnected nature of cyberspace. The digital and physical domain have become strongly interconnected. Due to developments such as office automation, process automation, data storage including cloud services, and network dependencies, cyber-incidents can start in many different locations and spread through systems and networks quickly. As a result, the vulnerabilities in one system can cause major problems for many other systems and are not necessarily bound by space and time (Rijksinstituut voor Volksgezondheid en Milieu [RIVM], 2016: 127).

Third, in terms of responding to cyber-incidents the field is also rather complex. A large number of public and private organizations are responsible for different parts of the digital domain. What is more, it is often difficult and time consuming to investigate the exact nature and impact of cyber-incidents, even for the system administrators responsible for the systems (RIVM, 2016: 127).

5.2.2 Lack of statistical data

Adding to the problem of complexity is the enduring lack of comprehensive, statistical data regarding threats, vulnerabilities, controls, losses and incidents (Soo Hoo, 2000: 8-9). Despite many different efforts to create such statistical data, there is still no complete and reliable

[4] The terminology for the different categories differs depending on the risk management methodology chosen (Ionita, 2013: 116).

data available (Dlamini, Eloff & Eloff, 2009: 4-5; Blakley, McDermott & Geer, 2001: 99-100). This is due to a number of different reasons.

With regard to threats and controls, not only do attackers benefit from keeping their activities secret, often, cyber security defenders also prefer to keep their activities behind closed doors. Cyber security is a realm characterized by secrecy (Libicki, Ablon & Webb, 2015: xi, 1). The nature of cyberspace makes it possible for malicious actors to hide their identities, capabilities, and attacks. As a result, many incidents go undetected and attribution is very difficult (Dunn Cavelty, 2007, 20: Singer & Friedman, 2009: 149-150). Defenders, therefore, argue that in order to keep the upper hand in this context, very little information can be made public with regard to the controls that are implemented to keep systems safe (Libicki, Ablon & Webb, 2015: 1, 13).

Many efforts are currently being deployed to create extensive overviews of vulnerabilities. The previously mentioned Common Vulnerabilities and Exposures website serves as an example. Nevertheless, vulnerabilities often go undetected. The software that makes up cyberspace consists of massive amounts of code which is constantly changing as new networks, products, and applications are developed and connected. It is estimated that the number of bugs found in software typically range from three to twenty bugs per thousand lines of code before the software is tested. A vulnerability constitutes a software bug that can result in a security weakness in the design, implementation, or operation of a computer system. If these vulnerabilities are found, patches can be deployed. However, sometimes these vulnerabilities go undetected, resulting in so-called 'zero-day vulnerabilities' (Singer & Friedman, 2009: 148; Libicki, Ablon & Webb, 2015: 41-44).

What is more, as far as losses are concerned, security incidents go unreported as organizations lack incentives to report, or compile statistics of incidents (Soo Hoo, 2000: 8-9). This can be due to fears for legal liability, damaging customer confidence, or overall damage to the reputation of the organization (Dlamini, Eloff & Eloff, 2009: 4-5; Soo Hoo, 2000: 8-9). There are efforts to stimulate the reporting of cyber security incidents. For example, in the European Union, the Council Directive 2016/1148/EC concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1 was adopted, which includes the provision for organizations to report cyber security breaches to authorities. This could contribute to gaining more data on incidents. However, the breach notification provision is limited to organizations that operate in specific sectors. In the case of the EU directive these sectors constitute organizations that deliver essential services, also regarded as critical infrastructures, and digital service providers including search engines, online marketplaces, and cloud computing services (Council Directive 2016/1148/EC).

Besides lacking incentives for collecting statistical data, current research efforts have not yet contributed to the establishment of comprehensive statistical data either. Many studies focus

on specific regions, mostly concentrating on the situation in the United States and the United Kingdom. Aggregated data on the state of affairs on a global level is not yet available (Dlamini, Eloff & Eloff, 2009: 4-5). What is more, many studies into the risks in cyberspace are conducted by security vendors. It can be in their best interest to exaggerate the risks in order to sell their security products (Dlamini, Eloff & Eloff, 2009: 4-5).

5.2.3 Safety versus security

Besides the complex nature of cyberspace and the lack of statistical data, risk management in the field of cyber security is difficult as future conditions are often incomparable to past conditions. This is not only due to the fact that cyberspace itself is constantly changing and evolving, the threats are also constantly in motion (Dlamini, Eloff & Eloff, 2009: 1-4). The main focus of cyber security is on threats stemming from intentional human actors (Dunn Cavelty, 2016: 402). As already discussed above, as ICT-systems became more sophisticated, so too did the efforts of malicious actors to poke holes in these systems and look for ways to gain unauthorized access or disrupt their functioning (Dlamini, Eloff & Eloff, 2009: 1-4). As stated by Libicki, Ablon & Webb (2015), "attackers and defenders are locked in an interminable innovation struggle" (Libicki, Ablon & Webb, 2015: 34).

Therefore, addressing the risks related to cyber security constitutes a security issue rather than a safety issue as it is considered to involve intentional acts. Nevertheless, as illustrated in the previous section, the risk management methodologies developed for cyber security are based on the methodologies that were originally designed to address unintentional safety risks in closed and static environments. As mentioned in chapter four, calculating the probabilities of security risks is much more difficult because determining human behavior is not static and the capabilities of malicious actors are often unknown (Hessami, 2004: 99-100; Reniers & Cozzani, 2013: 6; Beck, 2006: 329; Lupton, 1999: 64-65). It is therefore argued that applying risk management to the risks concerning cyber security inevitably fails as risk management methodologies are not designed and equipped to address dynamic and unpredictable intentional risks (Dunn Cavelty & Giroux, 2015: 215; Abdo, Kaouk, Flaus, & Masse, 2017: 2-3). What is more, with a primary focus within the field of cyber security on intentional risks, it is argued that the accidental safety risks remain underexposed (Abdo, Kaouk, Flaus, & Masse, 2017: 3).

5.3 Cyber security from a social constructivist perspective

This section investigates how the social constructivist perspective on risk shapes the way in which cyber security is perceived. As such, an overview of social constructivist thinking in the field of cyber security is provided. The aim is to offer examples of discussions that are currently ongoing and that fit in with the social constructivist perspective of risk rather than the realist perspective. The discussions highlighted in this section by no means form an exhaustive overview of all the discussions that currently exist. Instead, the discussions serve to illustrate

that social constructivist thinking in the field of cyber security exists and can offer different insights regarding cyber security risks than looking at them from the realist perspective.

5.3.1 Cyber security risk discourse

As noted in section 4.2.1, one of the notions of the risk society and reflexive modernization approach is that in the process of modernization, the primary focus of society now concerns the prevention of risk, resulting in a risk society. Whether this is due to the idea that society is confronted by a larger number of risks or that society has become less tolerant of risk in general is debated. However, in light of the argument of the risk society, the extensive focus on addressing cyber security risks through diverse practices of risk management, as illustrated in the first part of this chapter, can be explained (Power, 2004: 38). Yet, the previous section also illustrates the difficulties that are currently experienced regarding cyber security risk management due to the complex, interconnected, and incalculable nature of cyberspace. The risk society and reflexive modernization approach ads notions of globalization and a catastrophic nature to what constitutes contemporary risk. This section investigates how these notions are influencing the cyber security risk discourse.

Dunn Cavelty and Giroux (2015) argue that the cyber security risk discourse is currently revolving around the notion of catastrophic cyber-attacks aimed at societies' critical infrastructure (Dunn Cavelty & Giroux, 2015: 210). Some scholars refer to this as the constitution of so-called cyber-doom scenarios. Cyber-doom scenarios are considered hypothetical stories that typically involve multiple critical infrastructure systems failing at the same time, leading to serious, long-term, or total destruction of the economy and society. In this context, cyber-attacks are sometimes compared to have similar destructive force as weapons of mass destruction (Lawson, 2011: 5-7; Brito & Watkins, 2011: 40, 50; Dunn Cavelty, 2016: 414). Critical infrastructures are considered of vital interest to the functioning of society. Consequently, disruptions are pictured to cause major crises both in terms of the functioning of society and economic losses (Dunn Cavelty & Giroux, 2015: 210).

What is more, Dunn Cavelty and Giroux (2015) state that by linking cyber security to critical infrastructure protection, and thereby national security, the functioning of society has in itself become a critical infrastructure (Dunn Cavelty & Giroux, 2015: 214). This is notable as it is claimed that this has allowed for the perception that contemporary society is faced with a growing number of potentially catastrophic risks, which can be deliberately exploited by malicious actors (Dunn Cavelty & Giroux, 2015: 214).

As such, the risk discourse is both inward-looking and outward-looking. The inward-looking narrative holds that the increased interconnectedness of critical infrastructures has made them more complex and vulnerable to major disasters as it is argued that one catastrophic event can spread through entire systems quickly and easily (Abdo, Kaouk, Flaus, & Masse, 2017: 2). The outward-looking narrative concerns the increased readiness of malicious actors

to exploit these systems (Dunn Cavelty & Giroux, 2015: 215). However, as critical infrastructures are connected to cyberspace, these malicious actors are no longer bound to space and time, so the argument goes. As a result, the very nature of space and time is altered and thus the security that space and time used to offer is changed as there is no place to hide and the treat has become global and omnipresent (Dunn Cavelty & Giroux, 2015: 215). Furthermore, it is concluded that "the threat is networked and complex—and the threat *is* the network and *is* complexity" (Dunn Cavelty & Giroux, 2015: 215).

However, this framing of cyber security as an existential security risk constitutes a social construct as factual evidence to justify such framing is not yet available (Brito & Watkins, 2011: 40, 46). This is elaborated upon in the following section.

5.3.2 Securitization and threat inflation

As discussed in section 4.2.2, securitization theory constitutes the political, discursive process of portraying the issue as a security issue by means of speech acts. The speech acts are used to position an issue as an existential security threat. As a result of this process, the issue becomes the highest priority on the political agenda which allows for the introduction of exceptional emergency measures and policies to address the issue. A limited number of scholars have investigated how securitization theory applies to the field of cyber security (Dunn Cavelty, 2013: 106).

Nissenbaum (2005) for example, identifies two ways in which securitizing moves can be acknowledged within the field of cyber security. First, it is argued that cyberspace itself poses a threat as it is used by terrorist groups to facilitate their endeavors. More concretely, it is stated that, through cyberspace, terrorists are able to secretly communicate with each other, formulate plans, raise funds, and spread terrorist propaganda (Nissenbaum, 2005: 67). Second, as mentioned above, through cyberspace it is claimed that catastrophic cyber-attacks can take place aimed at the destruction of societies' critical infrastructure and thus threaten national security. These scenarios are often also used to position cyberspace itself as the next battlefield for warfare (Rid, 2012: 6). Positioning the threat of cyber warfare in this regard is also considered a securitizing move. Nisssenbaum, goes on to mention a number of speech acts that not only include government officials as securitizing actors, but also include actors in the private sector, and the media (Nissenbaum, 2005, 68).

As mentioned in section 4.2.2, it is often difficult to establish whether an issue has been successfully securitized. The scholars of the Copenhagen School have argued that the securitization of cyber security has merely been an attempt at securitization (Hansen & Nissenbaum, 2009: 1156). Yet, other scholars argue that, at the least, securitizing moves in the realm of cyber security are underway (Dunn Cavelty, 2013: 106). Therefore, it is perhaps more useful to look at the implications of these securitizing moves regarding cyber security.

It was stated in the previous chapter that securitization can break the rules that normally restrict certain behavior and policies and allow for the introduction of exceptional emergency measures. In the case of the securitization of cyber security, these extraordinary measures could include the limitation of privacy online, increased surveillance by national security agencies, and increased funding of these national security agencies to combat cyber security threats (Nissenbaum, 2005: 71-72; Lawson, 2012).

With regard to the notion of privacy online, an example constitutes the elaborate, and ongoing, public debate over the use of encryption and back doors. For example, after the terrorist attacks in Paris in November 2015 many US and European officials stated that encryption played a role in the planning of the attacks (Thielman, 2015). Furthermore, the most noticeable example of increased surveillance by national security agencies became evident in the United States as a result of the Snowdon revelations on the surveillance practices of the NSA in 2013 (Deibert, 2017: 172). With regard to increased funding of national security agencies, it is argued that as a result of the cyber warfare discourse, an extensive and powerful military-industrial complex is arising. To illustrate, in 2016 the US Cyber Command, part of the Department of Defense, had a budget of $466 million and this budget is expected to rise over the coming years (Hathaway, Demchak, Kerben, McArdle & Spidalieri, 2016: 26).

Threat inflation

As illustrated above, the process of securitization can have far-reaching implications and should therefore be carefully scrutinized (Nissenbaum, 2005: 72). In this respect, there are scholars that argue that the discourse on the threats related to cyber security is subject to threat inflation (Brito & Watkins, 2011: 39; Dunn Cavelty, 2016: 414). Threat inflation is understood to be the attempt to create more concern and urgency over a threat than can be substantiated through verifiable evidence (Brito & Watkins, 2011: 40-41). There are a number of scholars that argue that even though it is recognized that threats regarding cyber security exist and can cause major inconveniences, we have not yet witnessed incidents that pose existential threats to society and it is questioned whether this will happen at all (Dunn Cavelty, 2016: 414; Lawson, 2011: 5-7; Brito & Watkins, 2011: 40). What is more, the evidence that is to account for these kind of cyber-doom scenarios is often classified, which makes the scrutiny of this evidence impossible (Brito & Watkins, 2011: 40).

What is more, not everyone is convinced of the threat stemming from the cyber warfare scenario (Rid, 2012: 5). In his well-known book and article *Cyber war will not take place*, Thomas Rid argues that cyber war has not, is not, and will not take place (Rid, 2012: 5). Rid argues that if we look at the way in which the concept of war is conceptualized, we have not yet seen an act of cyber war to date. War constitutes three elements according to Rid: (1) an act of force, (2) it needs to be instrumental meaning that there needs to be a means to an end, and (3) it is always political (Rid, 2012: 7-8). Rid argues that there has not been any cyber offense to date that meets all three requirements (Rid, 2012: 6).

5.3.3 Actor-network theory and cyber security

Another avenue of research regarding cyber security that fits in with the social constructivist perspective rather than the realist perspective, involves the idea of Actor-Network Theory (ANT) applied to the field of cyber security. Founded by Bruno Latour and Michel Callon, ANT is a theory that includes a diverse set of different ideas and is therefore difficult to define precisely (Munro, 2009: 125). Overall, it can be stated that ANT rejects the idea of humanism which states that humans are the central force of everything (Munro, 2009: 125). The major insight that ANT brings to the table is the idea that not only humans are actors but also non-humans, or objects. In order to limit confusion, actors, both human and non-humans, are referred to as *actants* (Roby, 2014: 1).

What is more, the theory can be used to define and describe the *relations and connections* between these actants that exist together within networks and can form, if placed together, a new entity (Roby, 2014: 1). To illustrate this concept, Latour (1999) offers the example of what constitutes a gunman. Placing a man and a gun together creates a new entity: a gunman. The rationale followed in this example is that a man needs a gun in order to shoot, and a gun does not shoot on its own. Thus, only if put together the new entity, the gunman, is created and has a particular agency in itself (Latour, 1999, 179-180). Consequently, the idea of ANT is that both human and non-human actants play an equal role in the network they create and have equal agency (Roby, 2014: 1). An actor-network is thus understood as a macro level phenomenon that can be explained by looking at the actants that it consists of and how they are related to each other (Roby, 2014: 1).

Balzacq and Dunn Cavelty (2016) show how notions of ANT can be applied on the realm of cyber security. The scholars argue that even though cyber-incidents are discussed at length in policy debate and literature, it is not investigated how cyber-incidents can be understood as active drivers of political responses and interventions (Balzacq & Cavelty, 2016: 3, 5). In order to understand the agency of cyber-incidents in shaping political responses and processes, it is first necessary to understand what they do and how they work (Balzacq & Cavelty, 2016: 5).

According to ANT, the security of a network is dependent on keeping all the actants that constitute the network in place. If there are objects that threaten the coherent nature of the network, then the network could break down, this is referred to as depunctualization. Should this happen, then all relations between actants become variable and fluid (Balzacq & Cavelty, 2016: 11). The authors apply these notions to cyber-security, stating that cyber security incidents constitute the depunctualization of the cyber security network, the example they use is that of malware (Balzacq & Cavelty, 2016: 10). The authors note that malware is a particularly interesting actant as it can move through cyberspace independently from the person who originally wrote the malware and it directly affects how cyberspace functions and operates. The authors derive that if different actants can create different networks, then there

is not one universal cyberspace and thus, cyberspace cannot be understood by merely looking at the threats it consists of (Balzacq & Cavelty, 2016: 10).

With regard to cyber security, the major insight of ANT is that computers and software are active, not passive, entities that have agency of their own. It follows then that the way in which we study the risks related to cyber security could be studied as the result of interrelated actants (Balzacq and Dunn Cavelty, 2016: 21). In line with the discussion in the beginning of this chapter, it helps to understand the realm of cyberspace as a context wherein both humans and technologies interact. It can contribute to further specified analysis of the way in which these actants interact and influence the very nature of cyberspace (Balzacq and Dunn Cavelty, 2016: 22).

Summary

Addressing the risks related to computer and network technologies started out under the header of 'information security'. Originally, this was almost entirely considered to be a technical endeavor aimed at establishing the confidentially, integrity, and availability of these technologies. This started to change around the 1990s when these technologies were increasingly used for diverse applications involving human interaction, and cyberspace was created. It is now increasingly recognized that addressing the risks in cyberspace requires a broader, more strategic, and multi-disciplinary approach. The transition from a purely technical focus to a multi-disciplinary approach is what constitutes the shift from information security to cyber security. Many different risk management methodologies are developed to address the risks regarding information security and subsequently cyber security. Unfortunately, there is no comprehensive data available regarding the usage and popularity of the risk management methodologies in the field of cyber security. Nevertheless, the sheer number of different risk management methodologies could serve as an indication of their application in the field. However, risk management was originally designed to address accidental safety risks in closed and static technological systems. The risks related to cyber security, in contrast, are considered complex, dynamic and unpredictable. Moreover, the main focus of cyber security is on threats stemming from intentional human actors which are not static and often unknown. Also, there is an enduring absence of sound statistical data that is needed to conduct successful risk management. Therefore, it is argued that the value of risk management in the field of cyber security is limited.

From a social constructivist perspective, this chapter illustrates how the cyber security risk discourse is currently revolving around the notion of catastrophic cyber-attacks aimed at societies' critical infrastructure. This cyber security risk discourse is part of the political process of securitization. Securitization can have far-reaching consequences and should therefore be carefully scrutinized. In this regard, it is argued that factual evidence to justify the cyber security risk discourse is not yet available, the discourse therefore constitutes a social construct. Another avenue of research within the social constructivist perspective concerns

Actor Network Theory (ANT). The main insight that ANT brings to the table is the idea that non-human actors, like computers and software, have agency of their own. This realization could contribute to the further study and understanding of cyber security incidents.

Part 3

6 How does the framing of cyber security inform government responses?

This chapter investigates how governments respond to the framing of cyber security through both the realist and social constructivist perspective. The chapter consists of three parts. In the first part, it is argued that there is an increased pressure on governments to address risks through risk management practices. The second part illustrates this notion by taking a closer look at how risk management is incorporated as a fundamental practice within the government of the Netherlands. By means of a case study, three examples are provided. The third part offers examples of government responses when looking at cyber security risks from the social constructivist perspective.

6.1 The risk management of everything – government responses

As already discussed in chapter three, the notion of risk is all around us in contemporary society, permeating scientific research efforts and news media attention. Moreover, this results in greater risk awareness within society and a general feeling that risks need to be mitigated. From the social constructivist perspective, Beck ads that we are now living in a risk society which is characterized by a greater apprehension of risk. On top of that, Power (2004) argues that "more and more events and things are being seen and described in terms of 'risk', even though the concept remains elusive, contested and 'inherently controversial'" (Power, 2004: 13-14). What is more, there is an increased call on all kinds of organizations, including governments, to address and mitigate risks through various ways of risk management. Power refers to this as the 'risk management of everything' (Power, 2004: 9-10).

Within the context of the risk management of everything, governments are faced with increased political pressures to use risk management practices with the aim of making risks more controllable and governable (Power, 2004: 10). As a result, risk management has become a central endeavor of government practice, and is an essential part of governments' primary function of public service delivery (Power, 2004: 11). In this context, risk is even explained as the driver for quality control in the absence of real markets (Power, 2004: 19). What is more, risk management has become linked with accountability. As a result, governments are increasingly held accountable for their decisions and thus become increasingly occupied with addressing secondary risks to their reputation as well (Power, 2004: 14-15, 20).

Within this context it is not strange that governments turn to risk management for dealing with cyber security risks. The next section provides a case study of risk management practices related to cyber security by the government of the Netherlands. In the context of the risk management of everything, the case study illustrates how the Dutch governments' responses to cyber security risks can be explained in practice.

6.2 Cyber security risk management in the Netherlands – a case study

This section provides examples of risk management practices regarding cyber security by the government of the Netherlands. In the Netherlands, the policy responsibilities for cyber security are decentralized (Boeke, 2016: 7). This means that many different governmental organizations are responsible for a part of the cyber security policy. Investigating the risk management dimension of every governmental organization is beyond the scope of this thesis. Instead, the examples included below illustrate how risk management constitutes a fundamental principle for the responses of the government of the Netherlands when dealing with the risks related to cyber security. First, risk management in relation to cyber security is described in the context of the National Security Strategy. Then, risk management specifically related to cyber security is provided. The last example includes the risk management requirements related to information security.

6.2.1 Cyber security risk management in the context of national security

In the Netherlands, cyber security risk management is part of an all-hazards approach to risk management that finds its basis in the Dutch National Security Strategy (NSS). The NSS of the Netherlands was one of the first national security strategies to specifically adopt a risk management methodology as the foundation of its strategy (Klimburg, 2012: 26). The NSS was adopted in 2007 and aims to provide a whole of government approach to national security. The purpose of the national security strategy is to examine in an integral, systematic and periodical manner which disasters or crises may occur and what impact they may have on society. It contributes to the determination of priorities by the Dutch Cabinet with regard to the deployment of people and resources (Nationaal Coordinator Terrorismebestrijding and Veiligheid [NCTV], 2007: 7-8, 16; Klimburg, 2012: 26).

The process for risk management, as described in the NSS, constitutes an annual evaluation and assessment of the risks concerning national security. The process set forth in the NSS follows three steps: (1) the analysis of threats and risk assessment involving the assessment of likelihood and impact, and the identification of priorities (2) strategic planning, including an analysis of required resources, and (3) implementation, including the formulation of policy and regulation (NCTV, 2007: 13). This process was adjusted over the years and now constitutes a risk assessment every four years which is published in the so-called 'National Security Profile' (NSP). The four-year timeframe was established in order to do justice to the complexity of the risks included in the NSP and to have sufficient time to develop and implement resilience-enhancing measures (Opstelten, 2013: 5; NCTV, 2017a).

Despite adjustments to the process, risk management as a fundamental principle has remained intact in the NSS. The latest NSP, published in 2016, recognizes the contested nature of the concept of risk. What is more, even though the profile investigates notions like impact

and probability, it states that the quantitative calculation of both notions is excluded from the report. The authors argue that restricting the risks in the report to a quantitative interpretation alone does not do justice to the risks that are described (RIVM, 2016: 27).

Even though the NSS recognizes the threat stemming from ICT-failure, at the time of adoption, it did not yet recognize cyberspace as a critical asset for the safeguarding of national security. Nevertheless, this changed quickly and in the annual Cabinet letter on the progress of the NSS in 2009 the risks stemming from ICT-failure regarding critical infrastructures was recognized as an area of future investment (ter Horst, 2009: 2).

The NSP 2016 illustrates this ambition and provides a chapter on cyber security risks. It acknowledges that, due to the complex and novel nature of cyberspace, the likelihood, impact, and nature of large-scale cyber security risks are highly uncertain (RIVM, 2016: 117). The NSP includes a risk analysis of three imaginable cyber security scenarios: (1) disruption of the internet, (2) disruption of critical infrastructure due to cyber-attack, and (3) cyber espionage towards the Dutch government. The study concludes that the likelihood of physical damage of cyber-incidents is limited, whereas the impact due to social unrest and economic damage can be considerable (see figure 2). What is more, it is argued that cyber espionage could potentially cause major damage to the position of the Netherlands but is difficult to quantify. Damage due to cybercrime has already proven to cause inconvenience to citizens and companies, but until now has not yet have disruptive consequences for society. The report further states that even though cyber-doom scenarios regarding the attack on critical infrastructures are speculated upon, in reality, these types of scenarios hardly come to pass (RIVM, 2016: 132).

Figure 2 – Risk diagram of cyber threats (RIVM, 2016: 133)

6.2.2 Cyber security risk management

As stated above, the risks pertaining to cyber security are deemed quite uncertain according to the NSP 2016. Nevertheless, much is being done to address the risks. A complete review of all cyber security (policy) efforts of the Dutch government is beyond the scope of this thesis[5]. This section includes a description of how the notion of risk management is addressed in two guiding documents on cyber security: the Dutch National Cyber Security Strategy (NCSS) and the Cyber Security Assessment the Netherlands (CSAN).

The first NCSS of the Netherlands was adopted in 2011. The strategy adopts a number of principles with regard to cyber security in the Netherlands. One of these principles is that the measures and policies regarding cyber security need to be proportional. While it is recognized that complete security regarding the realm of cyber security is not possible, it states that choices with regard to policy measures should be based on risk assessment (Ministerie van Justitie en Veiligheid, 2011: 4). Moreover, the strategy contains a work plan including six points of action. One point of action concerns the requirement for developing threat and risk assessments. The NCSS is placed in the context of the overarching National Security Strategy and thus the effort of creating risk assessments for cyber security is to be integrated into the national effort of creating periodical risk assessments (Ministerie van Justitie en Veiligheid, 2011: 5-6). What is more, it is specifically noted that the National Cyber Security Centre (NCSC) is to establish one integrated assessment of all risks regarding ICT, and the Dutch secret service and military secret service are called upon to provide the NCSC with information for this purpose (Ministerie van Justitie en Veiligheid, 2011: 5-6).

The NCSS was revised and updated in 2013. The second NCSS maintains that an overall risk-based approach is needed to be able to achieve a balance between the overall levels of risk in cyberspace, the protective measures that need to be taken, and accepted risk levels that need to be established (NCTV, 2013: 8). The main difference between the first NCSS and the second strategy is that risk management is explicitly placed in the context of the protection of critical infrastructures in the second strategy (NCTV, 2013: 9). One of the objectives of the NCSS is to establish an approach for the risk assessment and identification of the risks related to critical ICT-dependent systems, services and processes. Based on this risk assessment, a program is to be established that should develop the basic security requirements that need to be followed (NCTV, 2013: 9, 23). Two specific points of action are taken up in the strategy, including the risk assessment of legacy systems, and the general strengthening of the research

[5] For an in-dept review: see Boeke, S. (2016). *First Responder or Last Resort? The role of the Ministry of Defence in national cyber crisis management in four European countries*, and Hathaway, M & Spidalieri, F. (2017). *The Netherlands. Cyber readiness at a glance*.

and analysis capabilities of Dutch security agencies in order for them to conduct risk assessments in the digital domain (NCTV, 2013: 28-29).

Both cyber security strategies include the provision for a periodical, overarching cyber security risk assessment. This risk assessment is indeed created annually and is known as the Cyber Security Assessment the Netherlands (CSAN). The findings of the CSAN constitute an important basis for the risk-based approach of cyber security and the design of policy measures (NCTV, 2013: 15; Dijkhoff, 2015: 1). The CSAN provides an assessment of the risks in cyberspace on a meta-level. The report provides a qualitative assessment of assets, threats, vulnerabilities, controls, and incidents. What is more, a quantitative valuation of these risk elements is provided in the form of a threat matrix (see figure 3). The underlying calculation or methodology for this threat matrix is not provided in the report. Additionally, even though the threat matrix includes the risk concerning failure of ICT, overall the CSAN mostly investigates the cyber security risks stemming from malicious human actors (NCTV, 2017b: 8).

	Targets		
Source of threat	Governments	Private organisations	Citizens
Professional criminals	Disruption of IT	Disruption of IT	Disruption of IT
	Manipulation of information	Manipulation of information	Manipulation of information ↓
	Theft and publication or selling of information	Theft and publication or selling of information	Theft and publication or selling of information
	IT takeover	IT takeover	IT takeover
State actors	Digital espionage	Digital espionage	Digital espionage
	Offensive cyber capabilities	Offensive cyber capabilities	
	Theft and publication of information	Theft and publication of information	
Terrorists	Disruption/takeover of IT	Disruption/takeover of IT	
Cyber vandals and script kiddies	Theft of information	Theft of information	Theft and publication of informatio
	Disruption of IT	Disruption of IT	
Hacktivists	Theft and publication of obtained information	Theft and publication of obtained information	
	Defacement ↑	Defacement ↑	
	Disruption of IT	Disruption of IT	
	IT takeover	IT takeover	IT takeover ↑
Internal actors	Theft and publication or selling of obtained information	Theft and publication or selling of obtained information	
	Disruption of IT	Disruption of IT	
Private organisations		Information theft (industrial espionage)	Commercial use/abuse or 'resale' of information
No actor	IT failure	IT failure	IT failure

Relevance legend

Yellow: *No new trends or phenomena are recognised that pose a threat.*
OR (sufficient) measures are available to remove the threat.
OR no appreciable manifestations of the threat occurred during the reporting period.

Orange: *New trends and phenomena are observed that pose a threat.*
OR (limited) measures are available to remove the threat.
OR Incidents have occurred outside the Netherlands and there have been several minor incidents in the Netherlands.

Red: *There are clear developments which make the threat expedient.*
OR Measures have a limited effect, so the threat remains substantial.
OR Incidents have occurred in the Netherlands.

Changes with respect to CSAN 2016:
↑ Threat has increased
↓ Threat has decreased

Figure 3 – CSAN threat matrix (NCTV, 2017: 8)

6.2.3 Risk management in context of information security – Baseline Information Security

Another example of risk management within the government of the Netherlands constitutes the adoption and implementation of the so-called Baseline Information Security (BIS). The BIS was adopted in 2012 and is the mandatory framework for information security within the Dutch government (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties [Ministerie van BZK], 2012: 4). Thus, the Dutch government considers information security as a different concept then cyber security. In the BIS, information security is defined as the process of determining the reliability of information processing in terms of confidentiality, availability and integrity, and the establishment of a coherent package of measures (Ministerie van BZK, 2012: 57). As such, the notion of information security is considered to be in line with the more technical approach as described in chapter five.

The aim of the BIS is to establish a framework for the information security of the entire Dutch government. The framework is mandatory to be implemented by all government services. For the information security of municipalities, a separate baseline applies, but this baseline is derived from the BIS and therefore very similar (Kwaliteitsinstituut Nederlandse Gemeenten, 2013: 3). Within the framework, the primary principle for information security is emphasized to be risk management (Ministerie van BZK, 2012: 4). What is more, the framework is based on the ISO standards ISO 27001:2005 and ISO 27002:2007. As already mentioned in chapter five these ISO standards are currently considered to be the most commonly used and accepted. Just as the ISO/IEC framework is considered abstract and high-level, aiming to create a comprehensive risk management system, so too is the BIR directed at establishing overarching requirements including also for example physical security of buildings and personnel (Ministerie van BZK, 2012: 4, 21, 24). The framework also includes an annual accountability and auditing requirement which is monitored by Dutch Parliament (Ministerie van BZK, 2012: 10).

So, the examples included in this case study illustrate how risk management is regarded as a fundamental principle for dealing with cyber security risks. Cyber security is considered part of national security, and as such, the periodical risk management process that was designed for dealing with national security risks include cyber security risk management as well. What is more, the National Cyber Security Strategy considers risk management the foundation for addressing the risks related to cyber security. As a result, a separate risk assessment for cyber security is conducted each year which mostly focusses on intentional threats. Besides risk management for cyber security specifically, the Dutch government has developed an overarching mandatory risk management framework that concerns information security specifically. Thus, the Netherlands considers the technical risk management of information security as separate from cyber security. Yet, risk management is considered essential for both concepts. Nevertheless, the limitations of risk management in the field of cyber security are also recognized and the severity of the risks related to cyber security is considered uncertain. The next section investigates how insights offered by the social constructivist perspective

could inform government responses regarding cyber security risks beyond a focus on risk management.

6.3 What insights does the social constructivist perspective offer governments?

Despite efforts to eliminate risks, they can never be completely mitigated and failures, incidents, and crises do happen (Power, 2004: 10). It is paradoxical then, that the increased efforts of governing risk through risk management, and the subsequent failure of being able to is "suggesting a world which is out of control and where failure may be endemic, and in which the organizational interdependencies are so intricate that no single locus of control has a grasp on them" (Power, 2004: 10). So, focusing on risk management alone could have the adverse effect that, if things go wrong and incidents occur, this could result in an increase in the perception of risk. The following part provides examples of government responses to the risks related to cyber security from the social constructivist perspective.

6.3.1 Precautionary principle

As mentioned in chapter four, in response to the non-compensatibility and catastrophic nature of risk in the risk society, the primary focus of dealing with risk shifts to a strategy of precaution. This is known as the precautionary principle (Beck, 2006: 335, 337). Originally, the precautionary principle was applied to the field of environmental protection. Nowadays, the principle is discussed and applied to many other fields as well (Feintuck, 2005: 371). The general idea of the precautionary principle is the rationale that "nothing is safe as long as it has not been proven harmless" (Beck, 2006: 337). This is in contrast to the opposing idea of laissez-faire which holds that everything is safe as long as it is not proven that it is dangerous (Beck, 2006: 337). Thus, the precautionary principle is considered especially applicable to fields where risks pose irreversible harm (Feintuck, 2005: 371-372).

The most notable example of how the precautionary principle is applied to the field of cyber security constitutes privacy and data protection. As Thierer (2014) states, the internet is designed in a distributed and decentralized way allowing information to flow freely. This pertains to all information that is provided online, also privacy sensitive and personal data. It is argued that it is really difficult to keep information confidential. What is more, once information is publically available on the internet, in most cases it is impossible to get it back. Adding to the problem is the observation that people voluntarily share their personal data through various applications. The extent to which this is happening nowadays is argued to be unparalleled (Thierer, 2014: 469- 470).

In response, privacy and data protection laws and regulations are being designed to safeguard privacy and personal data. A noteworthy example of such legislation is the General Data Protection Regulation (GDPR) adopted in the EU. The GDPR will come into effect in May 2018 and includes provisions such as increased territorial scope, meaning that no matter where an

organization resides as long as personal data of European citizens is processed the GDPR applies. What is more, the GDPR regulates increased penalties in case of non-compliance, a stronger focus on clear and intelligible consent for data processing, a breach notification, privacy by design, data portability, right to access, and the right to be forgotten (EUGDPR.org, 2017).

However, precautionary legislation in the field of privacy and data protection is also criticized. It is argued that this type of legislation stifles technological innovation, eventually limiting economic growth. What is more, it is sometimes claimed that it is too paternalistic limiting individuals' right to choose (Thierer, 2014: 470- 471).

What is more, as stated in chapter four, as a result of focusing on prevention, society is increasingly trying to anticipate risks that are not even proven to exist yet (Beck, 2006: 333-334). This idea also poses challenges for governments. In line with Power's notion of the risk management of everything, governments are tasked with providing security even though the true extent of certain risks is unknown. Consequently, political action could result in overreaction as the political cost of not acting is higher than the political cost of overreacting (Beck, 2006: 335-336). In this context, it has already been stated in chapter five that the cyber security risk discourse currently revolves around the hypothetical cyber doom-scenarios involving potentially disastrous attacks on societies' critical infrastructures. However, factual evidence for these type of events is not yet offered.

Nevertheless, governments are increasingly taking measures to prevent these type of cyber-doom scenarios from happening. The examples provided in chapter five include the limitation of privacy online, increased surveillance by national security agencies, and increased funding of these national security agencies to combat cyber security threats (Nissenbaum, 2005: 71-72; Lawson, 2012). Even though these efforts are explainable when faced with a potential existential threat, there are downsides to these strategies as well. As argued by Deibert (2009), surveillance and filtering is currently being deployed by a number of governments in varying degrees. However, there are strong concerns with regard to accountability and control resulting in for example 'mission creep', meaning that surveillance and filtering mechanisms are being used for other purposed than originally instated (Deibert, 2009: 327). It is also argued that these practices have the paradoxical effect of creating more insecurity than they offer security (Deibert, 2010: 24).

What is more, in response to worries over the use of encryption by terrorists, some governments argue that they need access to encrypted systems and that back doors need to be built into certain encryption protocols or applications (Soghoian, 2010: 400). However, it is also argued that building in back doors only enhances insecurity as currently it is not possible to weaken encryption in a general sense without compromising the security of digital systems

that make use of encryption as a whole. This latter position has been taken up by the government of the Netherlands (van der Steur & Kamp, 2016: 4).

Based on the above paragraphs it can be concluded that looking at the precautionary principle when faced with potentially catastrophic risks could constitute a logical response but can also have serious adverse effects. The examples provided in the realm of cyber security show that as a result of the precautionary principle, innovation and economic growth can be stifled, and increased surveillance and the creation of back doors could actually result in less security in cyberspace. This leads to the question, what can be done alternatively? The next paragraphs zoom in on two examples of alternative policy responses: trust and resilience.

6.3.2 Trust

As mentioned in chapter four, Giddens introduces the notion of trust as a strategy of dealing with uncertainty. He states that in contemporary society people are reliant on systems that are often invisible to them but can directly affect their lives. Should these systems fail, the impact can be disastrous. Trust is a way of dealing with risk in the sense that it does not diminish uncertainty but it is a strategy to accept uncertainty (Nissenbaum, 2001: 106).

Even though trust cannot be a primary policy strategy, there are a few facets of trust that are interesting if applied to the field of cyber security (van den Berg & Keymolen, 2017: 195). The most often heard rationale involving the notion of trust in relation to cyber security is that trust is needed in cyberspace in order for it to thrive (Nissenbaum, 2001: 103). Van den Berg & Keymolen (2017) investigate how trust can function as a strategy for creating cyber security as well. One example provided by the authors constitutes security reward programs. These programs place trust in outsiders to provide information about vulnerabilities in their ICT-systems. It is stated that “this trust-based approach may fill a blank in the cybersecurity strategy of a company, as it would be too time-consuming or costly to keep these matters in their own hands” (van den Berg & Keymolen, 2017: 200-201).

The government of the Netherlands has embraced this idea by adopting a guideline for coordinated vulnerability disclosure. However, not many other governments have moved in to do the same. Often, legislative barriers regarding provisions on hacking limit the adoption of coordinated vulnerability disclosure policies by governments (Falot & Schermer, 2016: 100).

6.3.3 Resilience

As already mentioned above, governments are currently faced with the paradoxical endeavor of increasingly needing to address risks, and at the same time not really being able to mitigate risks completely as it is inevitable that incidents will occur. In response to this, it is argued by some scholars that it is perhaps wiser to accept that incidents will take place and focus on strategies involving resilience (Power, 2004: 22; Dunn Cavelty & Giroux, 2015: 210-211; Lawson, 2011: 27). Power (2004) refers to this as the new ‘politics of uncertainty’, “such a

politics would be premised on the acceptance that failures and accidents are possible in complex environments, even with the most competent, ethical and expert oversight possible" (Power, 2004: 22). Power goes on to mention that some failure is even necessary with regard to innovation and economic growth (Power, 2004: 22).

Thus, it is argued that in the context of complex risks in contemporary society, instead of only focusing on preventing incidents from occurring, we should move to a state in which it is accepted that incidents will occur. As a result, the focus shifts to resilience and making sure that systems are able to quickly and efficiently recover should incidents occur (Dunn Cavelty & Giroux, 2015: 221-223).

Even though there is merit to be found in this idea of adopting notion of acceptance and resilience given the complex nature of the cyber domain, it remains to be seen how far governments can, and are willing to, go with this rationale. The political pressures and concerns over reputation in the current state of the risk management of everything are not easily disregarded by governments (Power, 2004: 22). Further research is required to find out if governments could and would be willing to adopt a politics of uncertainty.

Summary

Resorting to risk management is a logical move for governments given the notion that they are faced with increased political pressures to address risks. As a result, risk management has become a principle strategy for most governments. A case study of government responses in the Netherlands illustrates this point by identifying three examples of risks management concerning cyber security. In the Netherlands, cyber security risk management is a fundamental principle of the overarching National Security Strategy which includes cyber security as a focus area as well. Policy documents focusing specifically on cyber security, including the Dutch National Cyber Security Strategy and the Cyber Security Assessment of the Netherlands, also position risk management as a fundamental principle. The Baseline Information Security, provides a risk management methodology that all governmental organizations are obliged to follow. However, as illustrated in the previous chapter, risk management has its limits in the field of cyber security. What is more, risks can never be fully eliminated. In response, governments could resort to strategies of preventing risks. However, as illustrated, this could have severe adverse effects as well, making cyberspace less safe and stifling innovation and economic opportunities. Alternative responses for governments could be found by looking at trust and resilience. Placing trust in outsiders to help make systems more secure could be one response. Moreover, given the complex nature of the risks related to cyber security, it might be necessary to move on to a 'politics of uncertainty' and a focus on resilience. This requires the acceptance that incidents will take place, and requires building resilient systems that can easily and effectively recover should incidents occur.

7 Conclusion and reflection

Even though there are different conceptual meanings of the notion risk, overall, risk has to do with the concept of uncertainty. Throughout history mankind has progressively tried to bring the uncertainty of the future under control. In pre-modern society, risks were considered natural events, acts of God, and matters of fate and luck that humans had no influence on. However, over time, mankind has progressively tried to bring the uncertainty of the future under control. As society transitioned towards modernity, the idea that objective knowledge is necessary to address and predict risk was increasingly valued. As a result, risks were considered real events that could be calculated, measured, and mitigated through risk management. This realist conception of risk has become the most common theoretical perspective.

Against this backdrop, it is not strange that, as computer and network technologies developed, the technical community resorted to risk management to address the risks stemming from these technologies. A vast amount of risk management methodologies has been created to deal with the risks related to cyber security. However, risk management was originally designed to address accidental safety risks in closed and static technological systems. The risks related to cyber security, in contrast, are considered complex, dynamic and unpredictable. Moreover, the main focus of cyber security is on threats stemming from intentional human actors which are not static and often unknown. Also, there is an enduring absence of sound statistical data that is needed to conduct successful risk management. Therefore, the value of risk management in the field of cyber security is considered limited.

The social constructivist perspective on risk offers an alternative view on risk. From this perspective, risks cannot (merely) be determined by objective calculation and measurement. Instead, risk is a complex social construct, which is determined by social and political processes, interactions, values, and discourses. From this perspective, it is argued that the current cyber security risk discourse, which involves hypothetical cyber-doom scenarios, constitutes a social construct as factual evidence for these type of scenarios is not yet offered. Moreover, the cyber security risk discourse is argued to be subject to the political process of securitization which could have far reaching consequences with regard to online privacy, mass surveillance, and increased governmental funding.

In contemporary society, risk has become an increasingly present concept, resulting in greater risk awareness within society and a general feeling that risks need to be mitigated. From the social constructivist perspective, it is argued that we are now living in a risk society which is characterized by a greater apprehension of risk. As a result, governments are faced with increased political pressures to use risk management practices with the aim of making risks more controllable and governable. A case study of the Netherlands was provided to indicate how risk management has become a fundamental principle for dealing with cyber security

risks. Nevertheless, it is also recognized by the government of the Netherlands that risk management regarding cyber security has its limits and the true extent of the risks related to cyber security remains uncertain.

From a social constructivist perspective, governments could resort to strategies of prevention. However, it was illustrated that this type of response could have severe adverse effects, making cyberspace less safe and stifling innovation and economic opportunities. Alternative responses for governments could be found by looking at trust and resilience. Placing trust in outsiders to help make systems more secure could be one response even though it can never be the sole response. However, it might be necessary to move on to a 'politics of uncertainty'. Given the complex nature of the risks related to cyber security, and the notion that risks can never be completely eliminated, the politics of uncertainty involves the acceptance that incidents will take place and the requirement for building resilient systems that can easily and effectively recover should incidents occur.

Reflection

Reflecting on the conceptual analysis in this thesis, it should be noted that the aim was to make explicit that there is not just one perspective for dealing with risk. Even though historically it is explainable why risk management practices are developed in the field of cyber security, the same history illustrates why the value of risk management is still limited in this field. Nevertheless, it is not implied in this research that risk management should just be discarded completely. That would constitute throwing out the baby with the bathwater. Instead, we should focus on the implications. For example, risk management was originally designed to deal with accidental safety risks. Cyber security efforts seem to only focus on deliberate cyber-attacks. As stated in this thesis, attributing cyber-attacks is impossible most of the time. This raises the question if we should not direct more attention to the accidental cyber security implications as well.

What is more, this thesis shows that there is a lack of empirical research in a number of fields. First, there is no comprehensive data regarding the usage and popularity of the different risk management methodologies. Second, even though there is a lot of research in the field of cyber security from the realist perspective, there is hardly any research regarding cyber security from the perspective of social constructivism. As illustrated in this thesis, looking at the cyber security domain from the social constructivist perspective leads to the questioning of well-established discourses. The example offered in this thesis concerns the cyber-doom scenario discourse that is questioned, as verifiable data is not available. Again, it is not argued in this thesis that these types of scenarios are impossible and could never take place. Instead, it leads to the challenge of finding ways to substantiate these claims in order to create more informed debates regarding their implications.

References

Abdo, H., Kaouk, M., Flaus, J. M., & Masse, F. (2017). *A new approach that considers cyber security within industrial risk analysis using a cyber bow-tie analysis*. Retrieved on 10 January 2018 from: https://hal.archives-ouvertes.fr/hal-01521762/file/elsarticle-template-harv.pdf

Arunraj, N. S., & Maiti, J. (2007). Risk-based maintenance—Techniques and applications. *Journal of hazardous materials*, *142*(3), 653-661.

Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *1*(2), 176-198.

Beck, U. (2006). Living in the world risk society: A Hobhouse Memorial Public Lecture given on Wednesday 15 February 2006 at the London School of Economics. *Economy and society*, *35*(3), 329-345.

Berg, H. P. (2010). Risk management: procedures, methods and experiences. *Risk Management*, *1*(17), 79-95.

van den Berg, B., & Keymolen, E. (2017). Regulating security on the Internet: control versus trust. *International Review of Law, Computers & Technology*, 1-18.

van den Berg, J., van Zoggel, J., Snels, M., van Leeuwen, M., Boeke, S., van de Koppen, L., … de Bos, T. (2014). On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. *Sto-MP-IST-122 – Cyber Security Science and Engineering*.

Bernstein, P. L. (1996). *Against the gods: The remarkable story of risk*. New York, NY: Wiley.

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. *Proceedings of the 2001 workshop on New security paradigms*, 97-104.

Blanksma Çeta, A. & Konings, F. (2017). Nationaal cybersecurity bewustzijnsonderzoek. Retrieved on 8 January 2018 from: https://www.alertonline.nl/media/Nationaal-Cybersecurity-Bewustzijnsonderzoek-2017-DEF4.pdf

Boeke, S. (2016). *First Responder or Last Resort? The role of the Ministry of Defence in national cyber crisis management in four European countries.* Retrieved on 10 January 2018 from:

https://openaccess.leidenuniv.nl/bitstream/handle/1887/46615/Boeke(September2016)FirstRespondersorLastResort.pdf?sequence=1

Bourbeau, P. (2015). Securitization. *International Encyclopedia of the Social & Behavioral Sciences, 21,* 395-399.

Brito, J., & Watkins, T. (2011). Loving the cyber bomb-the dangers of threat inflation in cybersecurity Policy. *Harv. Nat'l Sec. J.*, *3*, 39.

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

Common Vulnerabilities and Exposures. (2017). *CVE Details*. Retrieved on 2 January 2018 from: https://www.cvedetails.com/vulnerability-list.php?vendor_id=0&product_id=0&version_id=0&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=2017&month=12&cweid=0&order=1&trc=1041&sha=c08604f7d6a3b7bce252a7487fd4dcdd38af8f8b

Deibert, R. (2009). The geopolitics of internet control: censorship, sovereignty, and cyberspace. *Routledge handbook of Internet politics*, 323-336.

Deibert, R. (2017). *Cyber-security*. In M.D. Cavelty & T. Balzacq (Eds.). *Routledge handbook of security studies*. New York, NY: Routledge.

Deibert, R. J., & Rohozinski, R. (2010). Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*, *4*(1), 15-32.

Dijkhoff, K. H. D. M. (2015). Beleidsreactie Cyber Security Beeld Nederland 2015. Retrieved on 10 January 2018 from: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-5.html

Dionne, G. (2013). Risk management: History, definition, and critique. *Risk Management and Insurance Review*, *16*(2), 147-166.

Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. *computers & security*, *28*(3), 189-198.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105-122.

Dunn Cavelty, M., & Giroux, J. (2015). The Good, the Bad, and the Sometimes Ugly. *World Politics at the Edge of Chaos: Reflections on Complexity and Global Life*, 209.

Dunn Cavelty, M. (2016). Cyber-security. In A. Collins (Ed.) *Contemporary Security Studies.* Oxford: Oxford University press.

EUGDPR.org. (2017). *GDPR key changes.* Retrieved on 15 January 2018 from: https://www.eugdpr.org/key-changes.html

Falot, N., & Schermer, B. W. (2016). De strafrechtelijke positie van de Nederlandse etisch Hacker. *Computerrecht, 45*, 94-100.

Feintuck, M. (2005). Precautionary maybe, but what's the principle? The precautionary principle, the regulation of risk, and the public domain. *Journal of Law and Society*, *32*(3), 371-398.

Fischhoff, B., Watson, S. R., & Hope, C. (1984). Defining risk. *Policy Sciences*, *17*(2), 123-139.

Furedi, F. (2006). *Culture of fear revisited*. Continuum.

Giddens, A. (2013). *The consequences of modernity*. John Wiley & Sons.

Giddens, A. (1999). Risk and responsibility. *The modern law review*, *62*(1), 1-10.

Halek, M., & Eisenhauer, J. G. (2001). Demography of risk aversion. *Journal of Risk and Insurance*, 1-24.

Hansen, L. & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), 1155-1175.

Hansson, S. O. (2005). Seven myths of risk. *Risk Management*, *7*(2), 7-17.

Harpes, C., Schaff, G., Martins, M., Kordy, B., Trujillo, R., & Ionita, D. (2014). *Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security.* Retrieved on 12 December 2017 from: https://www.trespass-project.eu/Documents

Hathaway, M., Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2015). *Cyber Readiness Index 2.0.*
Retrieved on 4 December 2017 from:
http://www.potomacinstitute.org/images/CRIndex2.0.pdf

Hathaway, M., Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2016). *United States of America cyber readiness at a glance.*
Retrieved on 8 January 2018 from:
http://www.potomacinstitute.org/images/CRI/CRI_US_Profile_Web.pdf

Hessami, A. G. (2004). A systems framework for safety and security: the holistic paradigm. *Systems Engineering*, *7*(2), 99-112.

ter Horst, G. (2009). *Nationale Veiligheid.*
Retrieved on 9 January 2018 from:
https://www.nctv.nl/organisatie/nationale_veiligheid/strategie_nationale_veiligheid/documenten.aspx

Huang, D. L., Rau, P. L. P. & Salvendy, G. (2007). A survey of factors influencing people's perception of information security. *International Conference on Human-Computer Interaction*, *4,* 906-915.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *information security technical report*, *13*(4), 247-255.

Inkster, N. (2016). Information Warfare and the US Presidential Election. *Survival*, *58*(5), 23-32.

Ionita, D. (2013). *Current established risk assessment methodologies and tools*.
Retrieved on 13 December 2017 from:
https://research.utwente.nl/en/publications/current-established-risk-assessment-methodologies-and-tools

ISO/IEC 31010. (2009). Risk Management - Risk Assessment Techniques, *ISO/IEC, Technical report, ISO, Switzerland, 2009*.

Kasperson, R. E., Renn, O., Slovic, P., Brown, H. S., Emel, J., Goble, R., ... & Ratick, S. (1988). The social amplification of risk: A conceptual framework. *Risk analysis*, *8*(2), 177-187.

Klimburg, A. (Ed). (2012) *National cyber security framework manual.* Tallinn: NATO CCD COE Publication.

Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., & Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety, 139*, 156-178.

Kwaliteitsinstituut Nederlandse Gemeenten. (2013). *Voorbeeld informatiebeveiligingsbeleid gemeenten*.
Retrieved on 10 January 2018 from:
https://informatiebeveiliging-gemeenten.nl/download/vooorbeeld-informatiebeveiligingsbeleid/

Latour, B. (1999). *Pandora's hope: essays on the reality of science studies*. Harvard university press.

Lawson, S. (2011). Beyond cyber-doom: Cyberattack Scenarios and the Evidence of History. *Mercatus Center George Mason University Working Paper*, (11-01).

Lawson, S. (2012). Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. *First Monday*, *17*(7).

Libicki, M. C., Ablon, L., & Webb, T. (2015). *The defender's dilemma: Charting a course toward cybersecurity*. Rand Corporation.

Luhmann, N. (1993). *Communication and social order: risk: a sociological theory*. New York, NY: Transaction Publishers.

Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures 6*, *9*(1-2), 3-31.

Lupton, D. (Ed.). (1999). *Risk and sociocultural theory: New directions and perspectives*. New York, NY: Routledge.

Mattei, T. A. (2017). Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack. *World neurosurgery*, *104*, 972-974.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2012). Baseline Informatiebeveiliging Rijksdienst. Tactisch Normenkader (TNK).
Retrieved on 10 January 2018 from:
https://www.nationaleombudsman.nl/system/files/bijlage/BIR_TNK_1_0_definitief.pdf

Ministerie van Justitie en Veiligheid. (2011). *De Nationale Cyber Security Strategie (NCSS). Slagkracht door samenwerking.*
Retrieved on 10 January 2018 from:
https://www.rijksoverheid.nl/documenten/rapporten/2011/02/22/nationale-cyber-security-strategie-slagkracht-door-samenwerking

Munro, R. (2009). Actor-network theory. In S. R. Clegg & M. Haugaard (Eds.). *The SAGE handbook of power.* London: Sage

Van der Meulen, N. (2015). *Investeren in cybersecurity.*
Retrieved on 13 December 2017 from:
https://www.wodc.nl/binaries/2551-volledige-tekst_tcm28-73944.pdf

Nationaal Coördinator Terrorismebestrijding and Veiligheid. (2007). *Strategie nationale veiligheid.*
Retrieved on 9 January 2018 from:
https://www.nctv.nl/organisatie/nationale_veiligheid/strategie_nationale_veiligheid/documenten.aspx

Nationaal Coördinator Terrorismebestrijding and Veiligheid. (2013). *Nationale Cybersecurity Strategie 2. Van bewust naar bekwaam.*
Retrieved on 10 January 2018 from:
https://www.ncsc.nl/organisatie/nationale+cybersecurity+strategie

Nationaal Coördinator Terrorismebestrijding and Veiligheid. (2017a). *Strategie nationale veiligheid.*
Retrieved on 9 January 2018 from:
https://www.nctv.nl/organisatie/nationale_veiligheid/strategie_nationale_veiligheid/index.aspx

Nationaal Coördinator Terrorismebestrijding and Veiligheid. (2017b). *Cyber security assessment Netherlands 2017.*
Retrieved on 10 January 2018 from:
https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2017.html

National Cyber Security Centre. (2017). *Cyber Security Assessment Netherlands 2017.*
Retrieved on 4 December 2017 from:
https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2017.html

Nissenbaum, H. (2001). Securing trust online: Wisdom or oxymoron. *BUL Rev.*, *81*, 635.

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology*, *7*(2), 61-73.

Opstelten, I.W. (2013). *Voortgangsbrief Nationale Veiligheid.* Retrieved on 9 January 2018 from: https://www.nctv.nl/organisatie/nationale_veiligheid/strategie_nationale_veiligheid/documenten.aspx

Power, M. (2004). *The risk management of everything: Rethinking the politics of uncertainty*. London: Demos.

Ralston, P. A., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA transactions*, *46*(4), 583-594.

Reniers, G., & Cozzani, V. (Eds.). (2013). *Domino effects in the process industries: modelling, prevention and managing*. Oxford: Elsevier.

Renn, O. (1992). *Concepts of risk: a classification*. In S. Krimsky & D. Golding (Eds.) *Social Theories of Risk*. Paeger.

Rid, T. (2012). Cyber war will not take place. *Journal of strategic studies*, *35*(1), 5-32.

Rijksinstituut voor Volksgezondheid en Milieu. (2016). *Nationaal Veiligheidsprofiel 2016.* Retrieved on 9 January 2018 from: https://www.nctv.nl/organisatie/nationale_veiligheid/strategie_nationale_veiligheid/documenten.aspx

Roby, H. (2014). Actor network theory. *A Supplementary Dictionary of Transport Studies,* A Supplementary Dictionary of Transport Studies.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What Everyone Needs to Know*. New York, NY: Oxford University Press.

Soghoian, C. (2010). Caught in the cloud: Privacy, encryption, and government back doors in the web 2.0 era. *J. on Telecomm. & High Tech. L.*, *8*, 359.

Soo Hoo, K. J. (2000). *How much is enough? A risk management approach to computer security*. Stanford, Calif: Stanford University.

Steur, G. A., Kamp, H. G. J. (2016). *Cabinet's view on encryption*. Retrieved on 15 January 2018 from: https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/nl-cabinet-position-on-encryption

Sullivan, J. E., & Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the US power grid. *The Electricity Journal*, *30*(3), 30-35.

Thielman, S. (2015). *US and European officials reignite 'back door' encryption debate after Paris.* Retrieved on 14 January 2018 from: https://www.theguardian.com/technology/2015/nov/18/us-europe-reignite-debate-back-door-encryption-paris-attacks

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & security*, *38*, 97-102.

Vultee, F. (2010). Securitization: A new approach to the framing of the "war on terror". *Journalism Practice*, *4*(1), 33-47.

Vuori, J. A. (2017). Constructivism and securitization studies. In M.D. Cavelty & T. Balzacq (Eds.). *Routledge handbook of security studies*. New York, NY: Routledge.

Stallings, W. (1982). Network security essentials: Applications and standards (For VTU). *Pearson Education India*.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.

Williams, C. A. (1966). Attitudes toward speculative risks as an indicator of attitudes toward pure risks. *The Journal of Risk and Insurance*, *33*(4), 577-586.

Wood, C. C. (2004). Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. *Computer Fraud & Security*, *2004*(1), 16-17.

Wynne, B. (2002). Risk and environment as legitimatory discourses of technology: reflexivity inside out? *Current sociology*, *50*(3), 459-477.

Zinn, J. O. (Ed.). (2009). *Social theories of risk and uncertainty: An introduction*. Oxford, OX: Blackwell Publishing Ltd.