“Help?! My Personal Data Has Been Breached… Again”:

News Media Framing of Data Breaches; a Securitised Problem or the New Normal?

Hannah Bakx

S1214144

Supervisor: Ms. L. Adamson

First Reader: Prof. dr. B. van den Berg

Second Reader: Dr. D.J.W. Broeders

Words: 18.974

Master Thesis

Master of Science Crisis and Security Management

Faculty of Governance and Global Affairs

Leiden University

Acknowledgements

I would like to express my sincere appreciation to my supervisor Ms. Liisi Adamson for her patience, assistance, and guidance throughout the whole process. Furthermore, special gratitude to Prof. dr. Bibi van den Berg and Dr. Dennis Broeders for their insightful feedback. Lastly, a thank you to the Cyber Risk Services of Deloitte Netherlands for supporting me throughout the whole thesis writing process.

Abstract

In a world where data is collected unquenchably, cybercrime looms. Data breaches have become part of the news cycle, yet the way these criminal offences are portrayed can differ. This thesis examines whether data breaches, affecting personal data and privacy due to malicious intent, are portrayed by using securitising frames or desecuritising frames. By conducting a discourse and frame analysis on 86 newspaper articles from three different Dutch newspapers, this thesis researches how data breaches are framed and what the possible implications of such frames are. The results show that the majority of the articles use a securitising frame, yet it is argued that this does not necessarily lead to the securitisation of the perception on data breaches, as desecuritising frames and failed securitisation were identified as well. The increase in data breaches and simultaneously an increase in security practices can lead to bug/security fatigue which does not improve data protection. Therefore, for a more cyber secure and privacy aware society it is advised to focus on personal data protection awareness.

Table of Figures

Table of Contents

1. Introduction

“Facebook found a breach in their social network enabling hackers access to accounts and personal information of 50 million users. Passwords of the users did not fall into the hands of the hackers” writes De Telegraaf on September 28, 2018, informing their audience that a large number of Facebook accounts have been hacked, but the passwords are safe. “Is your account a victim of the Facebook-breach?” reads the headline of NRC.nl on September 30, 2018. “Tens of millions of Facebook accounts were accessible for hackers for over a year” (NRC, 2018). The core of these headlines is the same, 50 million Facebook accounts have been breached. The portrayal of the message is however different, possibly affecting the attitude of the public towards the issue.

1.1. Topic

The use of Information and Communication Technologies and networks (ICT) such as the internet, have become increasingly important to our society (Kortjan & Von Solms, 2014, p. 29; Kritzinger, 2017, p. 22). These developments offer many benefits to industries, governments and organisations in general. Moreover, such ICTs play a prominent role in the lives of ordinary people, for the purpose of education, socialising and many forms of entertainment (Kritzinger, 2017, p. 22). On the other hand, the digitalisation of our society also has downsides, involving a risk of violations of security and privacy for many of its users (Van Schaik et al. 2017, p. 547).

Many cyber security related incidents, such as data breaches, happen every day. In 2018, there have been over 20.000 reported data leaks in the Netherlands (Autoriteit Persoonsgegevens, 2019). Simultaneously, in the last decades, and especially in the last few years, regulations have been created, nationally and internationally, in an attempt to protect individuals’ personal data and privacy. For example, since 2016 it is mandatory in the Netherlands to report a data breach and since the General Data Protection Regulation (GDPR) came into effect in May 2018, regulation regarding personal data protection became more rigorous (Autoriteit persoonsgegevens, 2018). A data breach occurs when there is “unauthorised access to, destruction, modification or the release of personal data from an organisation” (Autoriteit Persoonsgegevens, 2018).

Besides the increase in data breaches and an increase in regulation, receive multiple data breaches a large amount of media attention, such as the Facebook data breach in September

2018 (NRC Handelsblad, 2018; De Telegraaf, 2018). A few months before this incident Facebook made the news for a breach of at least 87 million users by a third party (NRC Handelsblad, 2018; De Telegraaf, 2018). Some personal data related incidents enjoy more attention than others. Especially breaches of well-known organisations affecting a large number of people, such as the Facebook hacks, make the news. However, in 2018 there have been notable data breaches in the Netherlands as well, such as the abstraction of personal data of clients from insurance company Achmea (De Volkskrant, 2018).

Moreover, whole industries exist that specialise in cyber security, data protection and privacy. Cyber security is increasingly being researched from various angles and recent data breaches highlight the increasing social and economic impact of such cyber incidents (Liu et al., 2015, p. 1009). Nonetheless, there is a lack of academic research on this topic, especially how data breaches are portrayed by news media. News media is an important source of information that can possibly contribute to the perception that people have on certain issues (Iyengar, 1990, p. 36). However, it is important to keep in mind that the direct effect of the portrayal of data breaches on public perception is not tested in this thesis. Instead, the possible implications of framing on public perception are considered.

The portrayal of data breaches is an interesting theme as it is of interest to many, since personal data of the majority of people is being stored and used by various organisations. There is an increase in size and occurrence of (reported) data breaches and major data breaches have become a "routine in the news cycle" (PRnewswire, 2019). Data breaches appear to become the new normal as, for example, financial losses resulting from data breaches are calculated into business models (Das, 2018). Are data breaches portrayed as a threat or are we getting used to our data being breached? With the help of the theoretical paradigm of securitisation theory (Weaver, 1995; Buzan et al., 1998; Deibert, 2002) including desecuritisation (Weaver, 1995; Hansen, 2012) and Dunn Cavelty's (2008; 2015) research regarding normalisation of cyber incidents, this thesis attempts to identify how data breaches are framed by Dutch newspapers and what the possible implications of such frames are.

1.2. Relevance

The way societal and political issues are framed through news media can influence the perceptions of the public regarding such issues (Berbers et al., 2016; Entman, 1993; Iyengar, 1990; Van Gorp, 2007). Researching how cyber incidents, such as data breaches, are portrayed can help understand how such incidents are perceived (Dunn Cavelty, 2015). Many people thus

far do not feel as if they 'lost' something throughout the breaches. Despite the risk of a data breach, the public is often not worried about their personal data, as they have often not experienced any impact and are therefore not interested (De Bruijn & Janssen, 2017, p. 4). But is this changing? This research hopes to contribute to academic literature and to society by studying media frames on data breaches to obtain a better understanding on the portrayal of data breaches and the possible implications.

1.2.1. Academic Relevance

This research aims to contribute to the multidisciplinary field of crisis and security management as it attempts to study the portrayal of a security issue. By applying framing theory (Iyengar, 1990; Entman, 1993; Van Gorp, 2007; Berbers et al., 2016) combined with securitisation theory (Weaver, 1995; Buzan et al., 1998; Deibert, 2002), including desecuritisation and normalisation (Hansen, 2012; Dunn Cavelty, 2008; 2015), this thesis aspires to provide an analysis of media frames and explore the discourse of data breaches.

Most of the literature on cybersecurity discourse examines high-level securitisation of cyberspace, emphasising 'cyber warfare' and 'cyber terrorism', also known as the militarisation of cyber security (Barnard-Wills & Ashenden, 2012, p. 120). The focal point is on threats arising from the use of cyberspace to (inter)national security and the discourse used by government, however there is a lack of research on desecuritisation and normalisation of cyber incidents. Security discourse regarding cyberspace is "forged, argued and accepted", but it is not the 'truth' (Dunn Cavelty, 2013, p. 106). Scholars tend to focus on the construction and the effects of cyber threat representation with the result that they often point their attention towards the most extreme cases (Dunn Cavelty, 2013, p. 119; Cruz Lobato & Kenkel, 2015, p. 24). Scholars such as Schmidt (2014) argue against these types of cyber threat language and call for a broader perspective in the cybersecurity research agenda.

The aim of this research is to add to the academic field by shining a broader light on cyber incident representation, by studying media and not focusing solely on security language, but also on the normalisation of cyber incidents. Ultimately, an abundance of security language can result in an abundance of security measures. On the other hand, a lack of security language can result in a lack of security measures (Dunn Cavelty, 2008, p. 31). Therefore, this thesis contributes to the academic field by researching whether the frames used to describe data breaches in news media are predominantly using securitising language or desecuritising language.

1.2.2. Societal Relevance

There is an increasing number of reported data breaches (Autoriteit Persoonsgegevens, 2018), and cyberspace is increasingly important to almost anyone (Kritzinger, 2017, p. 22). It is fundamental for people to understand the risks that they take by being online or sharing personal information in general. News media can have a large influence on people's perceptions of societal and political issues because they often do not have knowledge on the underlying details (Iyengar, 1990; Entman, 1993). It is therefore societally relevant to study media frames on cyber incidents as it can give an indication on how data breaches are perceived by the public. Dunn Cavelty (2008, p. 31) claims that the normalisation of cyber incidents can lead to a lack of security measures. The outcomes of this thesis may help address this issue by raising awareness of cyber incidents and support crisis and cyber security professionals in their approach to cyber incidents.

1.3. Research Objective

The intention of this research is to contribute to the constructivist paradigm regarding cyberspace by applying framing theory and securitisation theory, including desecuritisation. By applying these theories, this thesis hopes to provide a better understanding on the portrayal of data breaches and the possible implications of the use of such frames. It is explorative research as there has not yet been much research on media framing of data breaches, although the theories that are being used are well established in the academic field.

1.4. Research Question

In order contribute to the apparent research gap the following research question is proposed:

RQ: How are data breaches framed between 2012 and 2018 by Dutch news media (De Telegraaf, NRC Handelsblad and De Volkskrant) and what are the possible implications of such frames?

1.4.1. Sub-questions

The following sub-questions are created in the attempt to give answer to this partly exploratory and partly explanatory research question:

SQ1: What frames are used to give meaning to data breaches in Dutch media?

SQ2: To what extent can a securitising discourse be identified?

SQ3: To what extent can a desecuritising/normalising discourse be identified?

SQ4: How has the discourse on data breaches changed over time?

SQ5: What are the differences in frames between the three newspapers?

SQ6: What are the possible implications of data breach framing on public perception and cyber security?

The ambition of this thesis is to get a better understanding of the Dutch media portrayal on data breaches and explain whether or not data breaches are portrayed as a 'threat' or as 'normal'.

1.5. Methodological Approach

The method used to answer the research question is an analysis of language. According to Foucault (1972) discourse, is the practice that systematically forms the objects of which it speaks. By analysing discourse one analyses the processes of meaning making and social construction (Wittendorp, 2018). Discourse can be analysed by researching perceptions, that is to say: labels, values and qualities, metaphors, concepts, classifications and hierarchies. The method is inductive in nature and studies the data through the lens of securitisation theory, including desecuritisation and normalisation. By analysing media frames on data breaches, of three newspapers, a popular newspaper and two quality newspapers (Boukes & Vliegenthart, 2017) over the course of seven years, this thesis aims to provide an answer to the research question.

1.6. Reading Guide

The next two chapters of this thesis elaborate on the theoretical and methodological framework. The theoretical framework contains a body of knowledge, the conceptualisation of terms and explains the securitisation theory, desecuritisation, normalisation and the framing theory. The methodological framework explains the research design and the methodological approach of this thesis. Chapter four provides the results of the analysis, chapter 5 contains the discussion and chapter 6 is the concluding chapter.

2. Theoretical Framework

This chapter starts with the body of knowledge portraying previous research on the discourse of cyber incidents. The theoretical framework consists of the conceptualisation of terms, securitisation theory, desecuritisation, normalisation and framing theory.

2.1. Body of Knowledge

In the last few decades literature on cybersecurity has expanded. The next section provides an overview of research on the portrayal of cybersecurity and cyber incidents.

Securing cyberspace has become "one of the major global policy areas of the 21st century" (Deibert & Rohozinski, 2010, p. 29). Matters of cybersecurity have been an issue in security politics for three decades and are associated with (inter)national security (Dunn Cavelty, 2013, p. 105). Regulating cyberspace is rather difficult as it suggests a paradox (Deibert & Rohozinski, 2010, p. 29; De Bruijn & Janssen, 2017, p. 2). Regulating cyberspace in an attempt to secure it with policies can result in surveillance and data mining. While a lack of security can lead to cybercrime and malicious data breaches. As with many security problems, more security can lead to more intrusion to people's freedom and rights (Hansen & Nissenbaum, 2009, p. 1157; Barnard-Wills & Ashenden, 2012, p. 116). This paradox results in dilemmas regarding the security of cyber space, making it a difficult task. Besides the difficulties that come with securing cyberspace, there is also a lack of academic research.

Schmidt (2014) argues that there is an abundance of over-securitised academic literature and their critics. There is a lack of constructivist critical analysis and an overflow of literature on conservative military perspectives. Securitising frames and applying threatening historical events to cyberspace do not solve the problem. The power of discourse has an important role in cyberspace, "much more important here than in other military domains" (Schmidt, 2014, p. 38), because cyberspace as a military domain is a domain created by people and therefore constantly changing and in need of proper conceptualisation (Schmidt, 2014).

Dunn Cavelty (2013) shares this opinion and claims that "most of the political science literature on cybersecurity remains policy-oriented and lacks general international relations theory" (Dunn Cavelty, 2013, p. 105). The exception is a limited number of scholars whom have combined cybersecurity with securitisation theory (Weaver, 1995; Buzan et al., 1998). For example, Dunn Cavelty, 2008; Hansen and Nissenbaum, 2009; Deibert, 2002, 2010; Cruz

Lobato & Kenkel, 2015 focus on politically salient speech acts by visible political figures. However, research using elite speech acts as focal point neglect the influence of other actors in the securitisation process (Dunn Cavelty, 2013, p. 108).

The discourse on cybersecurity policy often portrays cyberspace as "ungovernable, unknowable, making us vulnerable, inevitably threatening and inhabited by threatening actors" (Barnard-Wills & Ashenden, 2012, p. 110). This discourse pays particular attention to threat, risk and, vulnerability from technological sources which gives actors new opportunities. The discourse supports the militarisation of cyberspace, risking a decrease in openness and an increase of surveillance. Cybersecurity discourse has so far been studied largely through formal declarations and policy documents, while actors that also form and shape cybersecurity representations are often non-governmental (Zajko, 2015, p. 147). For example, specialised consultants and ICT experts have the capacity to establish frames about certain issues (Dunn Cavelty, 2013, p. 108). Not just prominent governmental figures shape the frames regarding cyber incidents, such as data breaches, there are many actors involved.

One of the ways to distinguish cyber threat representation is in three clusters: 1) Technical cyber threats, such as malware, 2) socio-political threats, such as hackers, 3) and threats coming from the interaction between people and technology (Dunn Cavelty, 2013, p. 109). The way cyber threats are framed can influence the way policies regarding cybersecurity are constructed (Dunn Cavelty, 2013, p. 106). The more extreme threats are portrayed, the more exceptional the counter measures can be. This can contribute to the securitisation and militarisation of cyberspace (Barnard-Wills & Ashenden, 2012, p. 120; Dunn Cavelty, 2013, p. 106). In short, the way an issue is framed can influence the measures that are taken to counter the issue.

Not only policy is influenced by speech-acts, the public is also receptive to frames (Iyengar, 1990, p. 21; Entman, 1993, p. 55). Cybersecurity presents a complex socio-technical challenge for governments, but requires the involvement of individuals as well. Nonetheless, public awareness remains limited (De Bruijn & Janssen, 2017, p. 1). People know about cybersecurity as a term, yet their behaviour does not reflect a high level of awareness. Most people consider cyberspace as safe environment for daily use, while at the same time a data breach is no exception (De Bruijn & Janssen, 2017, p. 1).

Accordingly, whilst cybersecurity discourse is coloured by terms such as: cyber-crime, cyber-war and cyber-terrorism (Dunn Cavelty, 2008, 2013), the public does not appear to be overly receptive of these threatening terms. The exaggeration of cyber threats and the focus on global

disaster does not contribute to the awareness of how secure the public is dealing with their own personal data. People often feel like a cyber-attack will not happen to them. (De Bruijn & Janssen, 2017, p. 1). De Bruijn and Janssen (2017, p. 1) claim that certain frames can contribute to the awareness of the public. They advise to " not exacerbate cybersecurity, make clear who the villains are, put the heroes in the spotlight, show the importance of cybersecurity for society, personalise it, and connect cybersecurity to other issues". Unfortunately, how this message should be brought to the public is not mentioned. However, a body of research on framing claim that the public is especially receptive of frames that are communicated through news media (Nelson et al., 1997; Chong & Druckman, 2007; Matthes, 2007; Van Gorp, 2007; Slothuus, 2008; Lecheler & De Vreese, 2012).

The construction of cyber incidents as a security threat within the global news media has been researched (Jarvis, MacDonald & Whiting, 2016). Discourses on cybersecurity threats are productive rather than representational, meaning that the representation of threats serve a securitising purpose rather than the representation of the 'truth'. The existing academic literature on cybersecurity tends to neglect this insight on the discourse around cyberspace. Jarvis, MacDonald and Whiting (2016) argue the importance of news media in the framing of cyberspace as a threat and the securitisation of cyberspace. Furthermore, they suggest further research on non-English media framing of cyber incidents (Jarvis, MacDonald & Whiting, 2016, p. 622).

Furthermore, much literature has been written on the agenda-setting function of media (Brosius & Kepplinger, 1990; Soroka, 2002) and the influence of media messages (Berkowitz 1987; Bryant & Zillman, 1994). Yet, the role of media is often overlooked in security studies while 'reality' is a social construct for which media can be a key input (Tuchman, 1978, pp. 109-111). Security theories focus on levels of analysis, causes of war, nature of threat, types of interaction in international systems, types of referent object, and sectors of analysis (Buzan et al., 1998). Furthermore, security is traditionally viewed as the domain of elite players (Buzan, 1991; Waever, 1995) side-lining the role of media. Media should have a notable place in security studies as media frames shape knowledge and practices that relate to security. Individuals perceive their world around them and respond to changes through media (Davis & Gandy Jr., 1999, p. 367).

Therefore, this research hopes to contribute to the apparent research gap by researching the news media frames of particular cyber incidents, namely data breaches. The next part of this

chapter contains the theoretical framework, which is the foundation of this research. The theoretical framework connects securitisation theory, with desecuritisation and with framing theory, but first the next section explains the necessary theoretical concepts that apply to this research.

2.2. Conceptualisation of Terms

In order to get a better understanding of this research it is important to be familiar with the following terms.

2.2.1. Cyberspace

Cybersecurity is security that unfolds in and through cyberspace. Cyberspace is the combination between cybernetics and space and suggests "an unexplored land, free from legal and social constraints" (Dunn Cavelty, 2013, p. 107). Cyberspace can be seen as an ecosystem, a space of network technologies and network technology users (Dunn Cavelty, 2013). Also, Deibert and Rohozinski (2010 p. 16) define cyberspace as "comprising a material and a virtual realm, it is a space of things, ideas, structure and content". The way cyberspace is defined has consequences for the way cybersecurity and cybersecurity threats are perceived and represented (Dunn Cavelty, 2013, p. 108).

2.2.2. Cybersecurity

To understand cybersecurity, it is important to recognise the difference between cybersecurity and technical computer security. The latter concerns the individual-focused conceptions of computer security, originating from computer science (Nissenbaum, 2005, p. 61). Furthermore, it is important not to confuse cybersecurity with information security, although both concepts are often used interchangeably (Von Solms & Van Niekerk, 2013, p. 97). Information security can be defined as "the preservation of the confidentiality, integrity, and availability of information" (Von Solms & Van Niekerk, 2013, p. 98). While, cybersecurity can be defined as "harmonisation of capabilities in people, processes, and technologies; to secure and control both authorised and/or unlawful access, disruption, or destruction of electronic computing systems (hardware, software, and networks), the data and information they hold" (Ani, He, & Tiwari, 2016, p. 170). Cybersecurity involves considerations towards human victims and attackers as well, or the protection of assets besides that of information (Von Solms & Van Niekerk, 2013, p. 101). The definition of the concept of cybersecurity is influenced by the developments within the Copenhagen School regarding the securitisation theory (Nissenbaum,

2005). Cybersecurity is understood as a "combination of linguistic and non-linguistic discursive practices from many different communities of actors" (Dunn Cavelty, 2013, p. 108).

2.2.3. Cyber Incident

The National Coordinator for Security and Counterterrorism (NCTV) together with National Cyber Security Centrum (NCSC) define a cyber incident as "an event whereby information, information systems or information services are disrupted, fail or are misused (NCTV, 2018, p. 52) The NCTV and NCSC are part of the Ministry of Justice and Security and together they work on a more cybersecure society. Cyber incidents can range for example from Distributed Denial of Services (DDoS) and control over systems to stealing and manipulating personal data, also known as a data breach (De Bruijn & Janssen, 2017, p. 2).

2.2.4. Personal Data

Personal data is defined by the GDPR as "any information relating to an identified or identifiable natural person, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (GDPR, art. 4).

2.2.5. Data Breaches

A data breach occurs when there is involuntary access to, destruction, modification or the loss of personal data from an organisation (Autoriteit Persoonsgegevens, 2018). Methods and means that can result in data breaches are for example "user surveillance, identity theft, phishing, viruses, use of spyware, trojans, and keyloggers" (Van Schaik et al., 2017, p. 547). This thesis focal point is on data breaches of personal data in particular due to malicious intent, as almost everyone can be a victim of hackers or malware. This will be further explained in the methodological section.

Since data is being collected continuously and a breach can apply to almost anyone, it is a topic that enjoys much attention. Regulations such as the GDPR are set in place aiming to protect people's personal data, companies are spending on cybersecurity as a breach is bad for their reputation (De Bruijn & Janssen, 2017, p. 2) and large breaches make the news regularly. The aim of this research is to analyse the language that is used in news media regarding data breaches of personal data. Framing theory is used to interpret news media articles in combination with securitisation theory, as explained in the next section.

2.3. Securitisation Theory

"Discourses describing cyberspace as a potentially threatening arena for (inter)national security indicate a broadening of the securitisation process" (Cruz Lobato & Kenkel, 2015, p. 23).

Copenhagen School's securitisation theory was first introduced by Ole Waever (1995) and expanded on by Buzan, Weaver and De Wilde (1998) who define securitisation as "the process by which an issue is presented and accepted as a security issue that poses an existential threat to a given referent object and requires exceptional emergency protection measures" (Buzan et al., 1998, p. 23-24).

Copenhagen School's securitisation theory contains three types of issues: non-political issues, politicised issues, and securitised issues. Non-political issues are not viewed as requiring governmental intervention and are often not included in public debate. Political issues are resolved through normal governmental mechanisms, and securitised issues require urgent action and exceptional measures (Buzan et al., 1998). "Security is the move that takes politics beyond the established rules and frames an issue as being above politics" (Buzan et al., 1998 p. 23). An issue is defined as existential, urgent and to be prioritised over other issues, whether the threat is 'real' is irrelevant, as long as the threat is framed and accepted to be an existential and urgent threat (Buzan et al., 1998, p. 24).

Traditionally, securitising actors are elites such as governmental or public officials, politicians or others with significant political leverage (Huysman, 2002). The issue becomes a matter of security as a result of social processes of who securitises, on what issues or threats, for whom or what (the referent objects), why, with what results and under what conditions, that make the securitisation successful (Buzan et al., 1998, p. 32).

Securitisation occurs when three key elements are present: a securitising actor, a referent object, and functional actors (influencing the process). Furthermore, securitisation requires an audience that accepts the securitising act and determines whether or not the securitisation was successful (Buzan et al., 1998, p. 36).

Traditionally, the theory has been applied within five domains: military (such as war and conflict), political, economic (such as financial crisis), society (such as migration and refugees) and environment (such as climate change) (Buzan et al., 1998). Nonetheless, over the past twenty years securitisation theory has developed and it can be argued that cyberspace is a securitised domain as well. Especially the field of privacy and data protection enjoys and increase in attention, resulting in more and more regulation, especially in Europe. Nevertheless,

the securitisation of data breaches, having an effect on privacy and personal data, has not enjoyed much academic attention, especially from a viewpoint other than that of governmental officials. The next subsection elaborates on other securitising players.

2.3.1. Securitisation and Media

Security has traditionally been treated as the domain of elite players, such as governmental officials (Huysmans, 2002). The theoretical focus on elite actors has side-lined the roles of various other actors, for example media. There are serious consequences involved when any actor uses security language, as security is a concept that is used to "justify suspending civil liberties, war, and the reallocation of resources in the name of national security" (Baldwin, 1997, p. 5). Most research is on securitised issues that are a threat to national security, yet threats to society, the environment, or the economy can also be treated as security issues (Buzan et al., 1998). A data breach for example can be a threat to the economy and to society. The media's security interpretations and representations influence the public, but also elites (Carruthers, 2000, p. 207). Although media does not have official political power or the ability to enforce security policies, media is influential in written security speech acts and in deciding whether an issue should receive a special status. This thesis aims to research whether or not security language is used in the media regarding data breaches. There has been minimal research on security language in news media regarding data breaches, however cyberspace has been associated with securitisation theory before (Deibert, 2002; Hansen & Nissenbaum, 2009).

2.3.2. Securitisation and Cyberspace

During the 1990s, securitisation theorists did not include cyber incidents as an existential threat to security, as cyberspace was not yet as prominent as it is today (Buzan et al., 1998). Yet, as a consequence of the growing dependence upon ICTs and networks, it can be argued that cyberspace has been securitised, since cybersecurity is highlighted by "policy, institutional and strategic responses" (Hansen & Nissenbaum, 2009, p. 1157).

Deibert (2002) was one of the first to connect securitisation theory with cyberspace. He theorised cyberspace securitisation by separating four discourses: 1) national security, cyberspace as a threat to national collective identities; 2) state security, cyber as a military threat; 3) private security, cyber as a threat to privacy and personal data of individuals; 4) network security, cyber as a technological threat. His work has been important for the development of cyberspace securitisation literature.

There is a relatively consistent discourse of cyberspace security that involves uncertainty, risk perception, securitisation and militarisation coming from the military, technological and policy discourses (Barnard-Wills & Ashenden, 2012, p. 120). The incorporation of ICT networks in contemporary warfare, hacker operations, and threats to personal data and privacy, resulted in cyberspace and cybersecurity becoming part of the field of (inter)national security (Cruz Lobato & Kenkel, 2015, p. 24).

The securitisation of cyberspace can be divided in three categories: 1) hyper securitisation, an exaggeration of cyber threats and with a claim for exceptional measures, 2) everyday security practices, connecting cybersecurity issues to daily life and as a threat to citizens, and 3) technification, moving the cybersecurity discourse out of the political realm towards experts, constructing cyberthreats as complex issues requiring expert knowledge (Hansen & Nissembaum, 2009 p. 1163). This model provides a framework of how cyberthreats, including data breaches, can be securitised using different discourses.

The current discourse, heavy policing, and allocation of resources can be interpreted as the militarisation and securitisation of cyberspace (Hansen & Nissenbaum, 2009, p. 1157; Guitton, 2013, p. 21). However, cybersecurity at the level of so called 'cyber war' and 'cyber terrorism' do not personally affect most individuals, meaning that they are often not personally affected or do not have the means or knowledge to offer security measures for these types of threats. There is a contrast between cyber security portrayed by more traditional discourses of (inter)national security and the fields of personal information security, data protection and privacy (Barnard-Wills & Ashenden, 2012, p. 120). Not everyone is concerned with the most extreme cases of cyber incidents as the probability is those incidents are low (Dunn Cavelty, 2015).

Multiple academics claim that the securitisation of cyberspace has failed (Dunn Cavelty, 2008; Guitton, 2013). An issue becomes securitised when that issue is taken out of the 'normal' bounds of political procedure and securitising moves are only successful if an audience accepts the security argument (Buzan et al., 1998). Multiple studies on the representation of cyber threats (Dunn Cavelty, 2008; Guitton, 2013) show a forceful link to national security, but the prognostic language is on solutions and not on consequences, which can be associated with desecuritising language, resulting in the desecuritisation of cyberspace (Dunn Cavelty, 2008, p. 31). The aim of this research is not solely to analyse whether or not data breaches are portrayed as a security issue in need of exceptional measures, but also whether or not data

breaches are being desecuritised in Dutch news media. The way an issue is framed has an effect on how an issue is perceived, which has an effect on how one behaves towards a particular issue (Dunn Cavelty, 2008, p. 31). Securitisation implies a lot of attention and exceptional measures, while desecuritisation implies less attention and a decrease in measures.

2.4. Desecuritisation

As the previous section and the body of knowledge showed, the securitisation of cyberspace has been researched extensively. Yet, the alternative to securitisation is desecuritisation (Weaver, 1995).

2.4.1. Desecuritisation

Essential for understanding securitisation theory is its less notable and less researched counterpart: desecuritisation. Desecuritisation refers to the process by which a previously securitised issue is stripped of its urgency and brought back to the ordinary political or public sphere (Weaver, 1995). After the Cold War, Weaver (1995) was the first to describe desecuritisation as an aspect of securitisation theory. Desecuritisation represents the binary alternative to securitisation and indicates the process that removes a securitised issue from being treated as exceptional and outside 'normal' political bounds back to the political discourse or even away from political discourse at all (Weaver, 1995).

While the securitisation process is a result of a security speech act, desecuritisation not necessarily have a similar rhetorical tool; one cannot 'speak' desecurity. Nonetheless, there are ways in which desecuritisation can take place.

Almost twenty years after Weaver (1995) first wrote about securitisation and desecuritisation, Hansen (2012) restructured the field of desecuritisation and provides an up to date analysis on the subject. She criticises the lack of initial theorisation leaving the field open for interpretation. Desecuritisation is reliant on the fluctuation of identities, meaning that desecuritisation is socially constructed and the change in identity, from enemy to friend, can result in desecuritisation (Hansen, 2012, p. 527). Four categories of desecuritisation can be identified in her analysis. First, change through stabilisation, associated with the post-Cold War era. Second, change through replacement is the combination of one issue moving away from security discourse, while another is being securitised. Third, change through rearticulation, a securitised issue is actively offered a political solution to the threats in question, bringing it back to the political discourse with a positive undertone. Fourth, change through silencing, which happens when an issue disappears from the security discourse (Hansen, 2012, p. 533).

Desecuritisation can also be recognised as a non-securitising process (Biba, 2013, p. 33). For example, some governments are regularising restricted instruments to 'normal' ways of conducting regulation (Giacomello, 2014). This move can be interpreted as a desecuritising move. Desecuritisation is a technique for defining down threats or the normalisation of threats that were once considered extraordinary (Dunn Cavelty, 2008). This normalisation can be viewed as a fifth subcategory of desecuritisation.

There is a lack of research on desecuritisation in general, especially on desecuritisation and normalisation of cyberspace security. Yet, Dunn Cavelty (2008; 2015) provides new insights on how cyberspace security is perceived. She explores the normalisation of cyber incidents.

2.4.2. Normalisation

"We have arrived in an age of mega-hacks, in which high-impact and high-attention cyber incidents are becoming the new normal" (Dunn Cavelty, 2015). Normalisation refers to the process of which ideas or actions come to be perceived as 'normal' in everyday life. This normalisation is a process by which security issues lose their security aspect and become open to new interpretations (Dunn Cavelty, 2008, p. 31).

For years, cyber incidents have made the news, insecurity in and through cyberspace has come to dominate political discussion. Cyber incidents have become a trend, although they do not appear to excite the public. 'Cyber war' attracts attention, as it has a high impact on society, yet experts assure that the probability of this happening is low (Dunn Cavelty, 2015). On the other hand, low-level cyber incidents have a medium to high probability, but a low to medium impact (Dunn Cavelty, 2015), meaning that it is not as interesting for the public. Small incidents have become routine in the daily lives of many people and have become the new normal (Dunn Cavelty, 2015). In short, it could be argued that cyber incidents have been normalised instead of securitised by news media, since the threats are toned down and the prognostic language focuses on solutions and not on consequences (Dunn Cavelty, 2008, p. 31).

The aim of this research is to use the lenses provided by the securitisation theory, including desecuritisation and normalisation to analyse in what way data breaches are framed. Whether data breaches are portrayed and perceived as normal or as a threat to (international) security can be researched by analysing news media. Framing theory is used to understand media interpretation, representation and public perception. The next section elaborates on framing theory and the agenda setting function of frames in news media.

2.5. Framing Theory

Framing is a constructivist theory, as will be explained in the next section, and a research method as will be elaborated on in the methods section.

2.5.1. Constructivism

Framing theory is part of the constructivist theoretical paradigm. According to constructivism the world is socially constructed through interactions (Van Gorp, 2007, p. 61; Bryman, 2012, p. 33). Reality is constructed through personal experiences, interactions, and language, with numerous sources of information (Papert & Harel, 1991). The result is that different individuals have various perceptions of the same 'reality' (Bryman, 2012, p. 33). The constructivist approach explains why perceptions on the same 'reality' do not necessarily align.

An issue, such as a data breach, can be portrayed from a specific angle through media. The angle is chosen consciously or unconsciously. Either way it provides a lens for their audience through which to perceive reality. This thesis argues that reality is constructed through inter alia media (Tuchman, 1978, pp. 109-111). Media and individuals interact, which results in certain perceptions on an issue.

2.5.2. Media Frames

News reports are a source of information that can contribute to the construction of a reality through interaction. Societal and political issues, such as a data breach, are defined predominantly through news media and are therefore the main source for the public (Iyengar, 1990, p. 21). Individuals often do not have the knowledge or expertise to shape their own opinions on security issues and can therefore be heavily influenced by news media with the use of certain frames (Iyengar, 1990, p. 21; Van Gorp, 2007, p. 65).

The frames used by media can influence the way its audience perceives an issue (Berber et al., 2016). News media can offer new perspectives or confirm perceptions that already exist (Entman, 1993, p. 56). The public is specifically susceptible for framing strategies when it concerns a political, societal or security issue, such as data breaches, as most people do not fully understand the complexities involved with these particular issues (Iyengar, 1990, p. 21). The media can have the power to influence public perception on certain issues by using certain frames (Pan & Kosicki, 1993, p. 59; Van Gorp, 2007, p. 66). Therefore, news media could play a role whether individuals perceive data breaches as a security problem or as part of daily life.

2.5.3. Framing

Frames can provide meaning to certain issues (Gamson & Modigliani, 1987, p. 34) and confirm specific understandings of those issues (Shah et al., 2002, p. 368). Entman (1993, p. 52) provides the most widely accepted and detailed definition of framing: "To frame is to select some aspects of a perceived reality and make them more salient in a communicating text, in such a way as to promote a particular problem definition, casual interpretation, moral evaluation and/or treatment recommendation for the item described".

Framing is used as a strategy to construct news discourses (Pan & Kosicki, 1993, p. 57). The effect of framing has been tested by Kahneman and Tverskey in 1984 by formulating or framing solutions in two ways, in terms of likely deaths and in terms of likely lives saved. The result was that people changed their answers even though the solutions were the same, only presented in different ways. The framing effect is not often as visible, media can emphasise an already existing frame, however it is difficult for the audience to interpret and remember an idea that disagrees with the familiar frame (Entman, 1993, p. 57). What is more, supporting an existing perception is less noticeable compared to a change in perception (Entman, 1993, p. 57).

Of course, people can research facts and form an opinion on an issue. People are not mindless beings that will accept any frame that they receive through news media. However, multiple researchers argue that in general people are not acquainted with and/or active on many social and political issues. Therefore, framing can have a large influence on the audience's perceptions on these issues (Kahneman & Tverskey, 1984; Iyengar, 1990, p. 21; Entman, 1993, p. 57).

Frames can possibly influence people's perceptions towards certain issues and perceptions can influence people's attitudes towards these issues. The result is that policies and regulations related to these issues can be shaped by how an issue is framed, especially when such issues concern a security issue (Iyengar, 1990, p. 21; Entman, 1993, p. 57), such as a data breach. This framing effect has been researched thoroughly in multiple disciplines such as sociology, communication science, psychology and political science by multiple scholars such as Nelson et al. (1997); Chong & Druckman, (2007); Matthes (2007); Van Gorp (2007); Slothuus (2008) and, Lecheler & De Vreese (2012).

2.5.4. Agenda Setting

This thesis argues that media plays a significant role in the construction of public perception towards data breaches. Framing theory is also referred to as second-level agenda setting theory, suggesting that there exist various viewpoints on an issue and "the process by which the public develops a particular conceptualisation of a particular issue" (Chong & Druckman, 2007, p. 104). Certain frames can therefore set the agendas of the public.

The weight that is attributed to an issue through media can have an effect on the perceptions of the audience (McCombs & Shaw, 1972, p. 185). By highlighting one issue over others, public agenda can be directed through media by assigning more importance to one issue compared to other issues. Agenda setting theory emphasis the influence of media on public perception. The volume and length of articles or news items on an issue can have an impact on public agenda and public perception (McCombs & Shaw, 1972, p. 185).

Therefore, this thesis can give relevant insights on the possible implications of media frames of data breaches. The aim of this research is to use the theoretical framework on the securitisation and desecuritisation of data breaches to provide as lenses for particular media frames and apply framing theory to Dutch news media to retrieve knowledge on how data breaches are portrayed and what the possible implications of such framing can be. The next chapter explains how news media is analysed in this particular thesis by studying language.

3. Methodological Framework

As the previous chapter shows, there is a lack of research on whether or not data breaches are perceived as a security threat or that the public is used to data breaches in their daily lives. This chapter explains the methodological framework of this thesis, elaborating on the research design and methods to analyse media frames.

3.1. Research Question

To contribute to the appearing research gap the following research question is proposed.

RQ: How are data breaches framed between 2012 and 2018 by Dutch news media (De Telegraaf, NRC Handelsblad and De Volkskrant) and what are the possible implications of such frames?

3.1.1. Sub-questions

The following sub-questions are created in the attempt to give answer to this partly exploratory and partly explanatory research question.

SQ1: What frames are used to give meaning to data breaches in Dutch media?

SQ2: To what extent can a securitising discourse be identified?

SQ3: To what extent can a desecuritising/normalising discourse be identified?

SQ4: How has the discourse on data breaches changed over time?

SQ5: What are the differences in frames between the three newspapers?

SQ6: What are the possible implications of data breach framing on public perception and cyber security?

3.2. Research Design

The research design of this master thesis is qualitative. In order to answer the partly exploratory and partly explanatory research question, an inductive analysis is executed, as this thesis aims to explore and apply theory. The units of analysis are newspaper articles and the units of observation are the particular articles on data breaches. The newspaper articles are selected from three newspapers; De Telegraaf, De Volkskrant and NRC Handelsblad. The aim is to analyse around one hundred articles to ensure generalisability and external validity. The following part of this chapter elaborates further on the research design and the methodology.

3.3. Methodology

The objective of this research is to obtain a better understanding on how data breaches are framed in Dutch news media. To do this, the language used in newspaper articles has to be thoroughly studied, analysing the dominating discourse and frames on data breaches of particular Dutch media. The following paragraphs elaborate on the methods: discourse analysis and frame analysis.

3.3.1. Discourse Analysis

Media can be studied qualitatively and quantitatively. Discourse analysis is a qualitative research method and most fitting for the objective of this thesis. Content analysis is a quantitative research method to study language, however content analysis treats all negative or positive terms as equally salient and influential in a text. When conducting a content analysis the researcher takes the risk of misrepresentation of parts of the message that the audience would pick up and memorise (Entman, 1993, p. 57). Due to the specific focus on language and perception in the Dutch media on data breaches, for this thesis a qualitative analysis of language in news media is appropriate. This thesis will focus on the most salient frames in texts, relating those parts to particular media frames and therefore, discourse or frame analysis is more appropriate than content analysis.

The discourse analysis research method contains the premise that language is constructed; language gives meaning and provides a frame in order to understand issues and phenomena in daily life (Bryman, 2012). A discourse analysis studies how meaning is created and what ‘realities’ or ‘truths’ are accepted by the public. The study of language presents how and why things become possible (Dunn & Neumann, 2016, p. 2).

Meaning is created through language. Society creates and gives meaning to experiences and phenomena through discourse. These discourses occur in communications and texts, they can for example be found in official speeches, public communications and in this case newspaper articles. Discourses are not set in stone, they are always changing as there is competition of other discourses (Dunn & Neumann, 2016, p. 2). This competition is visible throughout this thesis as well, for articles of three newspapers are studied using multiple frames.

When performing discourse analysis one has to look for: labels, values and qualities, metaphors, concepts, classifications and hierarchies in order to understand how a certain issue is perceived and what the implications of those perceptions are. This thesis will use an inductive research method, meaning that the nature of the frames is defined before the research with the

help of the theoretical framework as lenses and the frames are further defined during the course of the research (Wittendorp, 2018).

The analysis is performed with the help of the theoretical lenses: securitisation and desecuritisation. Therefore, a frame matrix is developed beforehand in order to analyse the discourse or frames used in the texts (see figure 1). The next section explains what a frame analysis contains.

3.3.2. Frame Analysis

Frame analysis in this thesis is considered as an approach of discourse analysis. Framing demonstrates how meaning is constructed through texts, such as newspaper articles (Pan & Kosichi, 1993, p. 55). By accentuating certain features of a perceived reality, a particular interpretation of an issue can be promoted (Entman, 1993, p. 53). The public makes sense of particular issues primarily through the discourses and frames used in media (Van Gorp, 2007, p. 63). Therefore, a frame analysis is a suitable method for this particular research.

Additionally, frame analysis helps to explain how communications influence the understanding of the audience by a particular portrayal of information (Gamson & Modigliani, 1984; Entman, 1993; De Vreese, 2012). The process of framing makes certain aspects of information on an issue more salient, this piece of information then becomes more significant to the audience. As certain aspects of information are more significant, the audience is inclined to use it when forming perspective on that particular issue (Entman, 1993; Van Gorp, 2007; De Vreese, 2012).

Frames are difficult to get a grip on, nonetheless one can reconstruct them. Frames are embedded in media content, news messages are constructed in such a way that they refer to a certain frame. Those applied frames are represented as a frame package (Van Gorp, 2007 p. 64). In this particular research, where framing is combined with securitisation theory and desecuritisation the frame packages include these theoretical lenses.

The literature does not provide a frame matrix fitting for this thesis, therefore one is constructed (see figure 1). As the theoretical framework in the previous chapter highlighted, it is important to recognise the threat and referent object in order to recognise a securitising frame (Buzan et al., 1998). The threat representation is inspired by Dunn Cavelty's (2013) matrix that maps cyber security threat representation. Furthermore, there are indicators that can help recognise a securitising frame, such as metaphors, examples or statistics that strengthen the threat representation or the vulnerability of the referent object. Lastly, the matrix provides the different types of securitising frames: hyper securitisation (identifying large-scale disaster

scenarios), every day security practices (connecting cyber threats to daily life and individuals) and technification (moving the cybersecurity discourse out of the political realm towards experts) (Hansen & Nissenbaum, 2009).

The same works for a desecuritising frame, there is a referent object, but the threat is downplayed or not mentioned. Instead solutions are offered or the problem is silenced. Indicators such as metaphors, examples or statistics can also help identify desecuritising frames to, for example, downplay the threat. Moreover, the matrix also indicates the different types of desecuritisation: stabilisation (the threat is no longer apparent), replacement (another threat took its place), rearticulation (a political solution is offered), silencing (the issue disappears from the security discourse) (Hansen, 2012), normalisation (the threat becomes part of 'normal' daily life) (Dunn Cavelty, 2008; 2015). Inspired by these researchers this thesis aims to provide a matrix that can help identify securitising and desecuritising frames regarding data breaches.

Securitising frame	Indicators	Referent object	Threat representation	Type
	Metaphors	Personal data	Exceptional measures	Hyper securitisation
	Catchphrases	Privacy	War/terror language, exaggeration of threat	Every day security practices
	Examples		Metaphors (biological)	Technification
	Visual images		Othering	
	Statistics		Consequences	

Desecuritising frame	Indicators	Referent object	Representation	Type
	Metaphors	Personal data	Solutions	Stabilisation
	Catchphrases	Privacy	Degrading measures	Rearticulation
	Examples		Part of daily life	Replacement
	Visual images		Silencing	Silencing
	Statistics			Normalisation

Figure 1: Frame Matrix

3.3.3. Limitations

A Potential limitation of doing discourse analysis and frame analysis is the risk of research bias and the difficulties that are paired with interpretation. To elaborate, when studying language the researcher is dependent on the perception and insistence of oneself (Bryman, 2012). Discourse and frame analysis depend on the interpretations of the researcher and therefore this method affects the generalisability, replicability and internal validity of this thesis. The frame matrix attempts to overcome these limitations as it provides for a structured research that can be reused. Critique and challenges associated with discourse analysis can be reduced by

introducing more researchers to analyse the specific discourses. However, the resources and timeframe of this particular thesis are limited and do not suffice to such division of labour. The researcher therefore has to be attentive to an objective view and acknowledge potential limitations.

3.4. Data Collection

The selection of texts is chosen according to the criteria set out by Hansen (2005). Hansen has extensively researched language in order to study security as a practice and the criteria she sets out for selecting texts help to make the research manageable. Hansen (2005) outlines four dimensions for structuring research: first, 'intertextual models' define the object of analysis where the texts that are used are from. Examples of intertextual models are: official, such as heads of states, one analyses, amongst others, speeches or interviews. For wider political debate, such as media, one analyses reports. Analysing culture, the focus is on cultural representation, analysing films or photography. Lastly, marginal, emphasis is on social movements, analysing for example websites and blogs. The second dimension is, 'selves'. One can study 'one selve', analysing one position, 'multiple selves', taking various actors in account or 'discursive encounter', one position versus another. The third dimension is 'time', the temporal perspective can be one moment in time, comparative moments in time, or a longer historical timeframe with particular events and periods. The fourth dimension is 'events', one can study one event at a particular time, but other options are different times that are connected by an issue or one moment with multiple issues.

First, the intertextual model of this thesis is the wider political debate, as the focus is be on media, which is part of the political debate. The wider political debate is well represented through media since journalists get their information from political debates and reports on, in this case, data breaches. Second, the research is conducted on multiple selves as there is a distinction of three newspapers. Third, the temporal perspective of this study is a 'longer' historical timeframe, meaning that the analysis is not conducted on one event, but on multiple events during a certain amount of time. The timeframe gives insights in the formation and evolution of the discourse on data breaches. Fourth, this thesis focuses on multiple events that are connected by one issue during the particular time period between 2012 and 2018. By studying one issue over time, this thesis aims to give insights into changes and/or repetition of frames used in newspaper articles. The decision to focus on various breaches over the course of seven years is because it gives insights in the development of the frames that would have been less visible when the focus would be on a few breaches.

Moreover, the aim is to analyse data breaches that have occurred due to malicious intent and have affected the personal data and privacy of individuals. This scope is chosen because it can give insights in similar data breaches. Data breaches with malicious intent refer to the intent to "commit a wrongful act without just cause or reason, with the result to harm another, and with the intent to either copy, modify or destroy data" (Directive 2013/40/EU). This scope was chosen as it leaves out data breaches by accident which occur often as well but are not necessarily a security problem. Furthermore, data breaches related to for example national security are also left out as the aim of this research is to look into the newspaper articles regarding breaches that affect personal data of individuals as these incidents have a direct effect on the public and these 'smaller' incidents are not as vastly researched compared to larger cyber incidents regarding for example state secrets. However, it is important to be aware that there are still differences in severity and impact even though the breaches are similar.

The object of analysis or units of analysis are newspaper articles from *NRC Handelsblad*, *De Volkskrant* and *De Telegraaf*. News media analysis has the advantage that it reflects the social mainstream (Wodak & Kryzanowski, 2008), in order to present the mainstream, data is collected from three different newspapers with different audiences, as will be explained below. Furthermore, newspapers are accessible because they are open sources.

The aim of this thesis is to analyse the Dutch media on data breaches. For this research to be generalisable, not only one newspaper can be studied, therefore three Dutch newspapers were chosen for this thesis to conduct a valid and manageable research. Analysing popular and quality newspapers can help identify a possible variation on how popular and quality newspapers formulate data breaches (Boukes & Vliegenthart, 2017). Popular newspapers aim to reach the 'everyday' person, which is related to working class and people that enjoy news that is clear and easy to read while quality newspapers are more 'elitist' and address higher educated individuals (Boukes & Vliegenthart, 2017).

De Telegraaf is the largest Dutch newspaper and can be categorised as a 'popular' newspaper, also known as a tabloid. The paper can be perceived as a family paper or a paper for 'ordinary' people. De Telegraaf is known to report more on gossip, sensation and sex (Boukes & Vliegenthart, 2017) and does not have many columns (Verschillen tussen, 2017). De Telegraaf is politically coloured as right winged, the majority of its audience votes PVV (Party of Freedom) and VVD (Party of Freedom and Democracy or Liberal Party) (AD, 2015), both

parties are right winged, VVD is perceived as liberal as well. De Telegraaf reached up to 34,3 percent of the Dutch population in 2018 (Vlucht, 2018).

NRC Handelsblad and *De Volkskrant* can be categorised as 'quality' newspapers or broadsheets. Both are often perceived as 'elite' media (Boukes & Vliegenthart, 2017). NRC Handelsblad reports mainly on foreign affairs, politics, economy, opinions, art and literature (Infonu, 2019). The paper is sometimes perceived as centre-right winged, but sometimes as centre-left winged, the editorial office claims to be neither and states to publish from a liberal perspective (Infonu, 2019). The paper's audience votes mainly D66 (Democrats), depending on the topic a centre-right or centre-left winged party and VVD as well (AD, 2015). NRC Handelsblad reached up to 15,7 percent of the Dutch population in 2018 (Vlucht, 2018).

De Volkskrant is known to publish columns, on politics, policies, facts and research (Verschillen tussen, 2017; Boukes & Vliegenthart, 2017). The paper is politically left-winged and progressive (Verschillen tussen, 2017; Infonu, 2019). The audience that reads De Volkskrant mainly vote PvdA (Labour Party) and other left-winged oriented political parties (AD, 2015). De Volkskrant is the largest 'quality' newspaper and reached up to 16.1 percent of the Dutch population in 2018 (Vlucht, 2018).

For this thesis one 'popular' newspaper was chosen and two 'quality' newspapers as NRC Handelsblad and De Volkskrant together have a similar size in audience as De Telegraaf. Furthermore, all three newspapers have different audiences with different political and educational backgrounds (AD, 2015; Infonu, 2019), the three newspapers together reach a large part of the Dutch population. Analysing both popular and quality newspaper articles gives more insights on how data breaches are reported by different media reaching demographically different people.

Newspaper articles from 2012 until 2018 are collected to give insights in the formation and evolution of the discourse on data breaches. This timeframe was chosen because talks about the reform of the data protection directive from 1995 (95/46/EC) started at the beginning of 2012 (EDPS, 2019). Eventually, in March 2014 the first version of the GDPR was approved by the Parliament and the GDPR entered into force on 24 May 2016 and came into effect on 25 May 2018 (GDPR, art. 99). Due to the GDPR, the importance of data protection has increased, as the thresholds set by the regulations are higher and thus set higher standards and obligations on people and actors who process personal data. The GDPR is there for the

“protection of natural persons in relation to the processing of personal data as a fundamental right” (GDPR, General Provisions, paragraph 1).

This thesis does not look into the articles before 2012, as data breaches were not as common and not a widely discussed news items, this becomes visible in figure 2. From 2012 onwards there is a steady increase in news articles on data breaches. Figure 2 displays the news articles provided with the keyword search in ‘Nexis Uni’ used for this thesis between 2009 and 2018. As the figure shows, there is a large increase of news articles from 2012 onwards. This could be a result of the DigiNotar hack at the end of 2011 as well, as it represented a new type of incident, a ‘digital disaster’ (Van Der Meulen, 2013, p. 46). This was not a breach of personal data, but it was the largest digital breach the Netherlands had experienced so far. It showed how vulnerable data can be in the digital realm and it put cyber security in general on the map in the Netherlands (Security.nl, 2011). The decision not the include the first months of 2019 is to give better insights in how the frames have developed over the years and to be able to say something about seven full years as it is impossible to say something about 2019 for this year is not over yet.

Figure 2: Newspaper Articles on Data Breaches Between 2009 and 2018 based on key word search (Nexis Uni)

Analysing texts from the start of 2012 until 2018 provides an analysis of full seven years and gives insights in the framing of data breaches before the GDPR entered into force, after the GDPR entered into force, before it came into effect and after it came into effect (this is a short period of time, however more time has not past yet). Data protection has changed because of legislation: the GDPR forces organisations to be more aware of the data that they are working with. It is interesting to research how the portrayal and perception of data breaches has possibly developed and/or changed in this particular timeframe.

The GDPR is legislation created by the EU to protect EU-citizens with regard to the processing and protection of personal data. However, notifying authorities about data breaches is also required from non-European organisations that process personal data of EU residents, because such data breaches can affect EU citizens as well. These regulations have led to a better

understanding of the number of data breaches (Autoriteit Persoonsgegevens, 2019). For example, there is an increase in reported data breaches, 20.000 in the Netherlands in 2018 (Autoriteit Persoonsgegevens, 2019), compared to 10.000 reported data breaches in 2017 (Autoriteit Persoonsgegevens, 2018). Furthermore, there are many reported international breaches that are presented to the public through news media.

In line with various research on frame analysis, the aim of this thesis is to study approximately one hundred articles (Brown, 2011; Dirikx & Gelder, 2010: Nacos, 2005). The selection of the articles is based on a keyword search in the 'Nexis Uni' database: (databreuk or datalek or lek) and (privacy or persoonsgegevens or "gevoelige informatie" or "persoonlijke informatie" or gegevens) and (malafide or crimineel or cybercrime or identiteitsfraude or hack or hacker or gehackt or darkweb or gestolen or stelen or inbraak or ransom or ransomware or geizelen or gegeizeld or incident or phishing or privacy or persoonsgegevens or AVG or cyberincident, or cybersecurity). This selection of keywords provides newspaper articles about data breaches due to malicious intentions affecting personal information and the privacy of individuals. The focus is on breaches of personal data of people, as these types of incidents can affect everyone who has data stored somewhere on the internet and not just large companies or governments. The aim of this research is to understand how data breaches are framed when it affects the public. The keyword search also provided non relevant articles, therefore further selection of the articles is a result of precise reading in order to select the relevant articles, this resulted in 86 articles in total to be analysed.

4. Results

This chapter contains the results of the frame analysis of the three newspapers. First, this chapter starts with a short recap on the specific data collection and how the analysis is conducted. Then, the results from the analysis are presented. Additionally, the results are interpreted and further discussed.

4.1. Data Collection

Newspaper articles were collected between 2012 and 2018 from three national Dutch newspapers: De Telegraaf, De Volkskrant and NRC Handelsblad.

4.1.1. Relevant Articles

The number of relevant articles collected for this research differs per year. Some years contain more relevant articles than others, as data breaches are in some years a more common news topic than in other years. The reason that the topic is more heavily published in some years than in others can depend on multiple factors, which for example can be technological development, economic loss or cultural of nature (Zeng & Li, 2013, p. 143), the occurrence of a data breach and its implications, the size and location of breaches, how sensitive the stolen data is or the amount of economic loss. Furthermore, certain topics can be of more interest during certain times because of other events, such as new legislation. For example in 2012 reforms in the legislation for the protection of personal data (Wet Bescherming Persoonsgegevens) was proposed making it obligatory to report a data breaches in the Netherlands (De Volkskrant, 2012). Or, new types of breaches, such as the ransomware attack Wannacry in 2017 caused also an upsurge in reporting (De Volkskrant, 2017).

The article selection is based on a keyword search. The keyword search in the period between 2012 and 2018 resulted in 323 articles for the three newspapers combined. However, ultimately only 86 articles were relevant for the analysis, as the focus is on data breaches with malicious intent, affecting the public and not on data leaks by accident. From the 86 articles, 24 were from De Volkskrant, 25 from De Telegraaf and 37 from NRC Handelsblad.

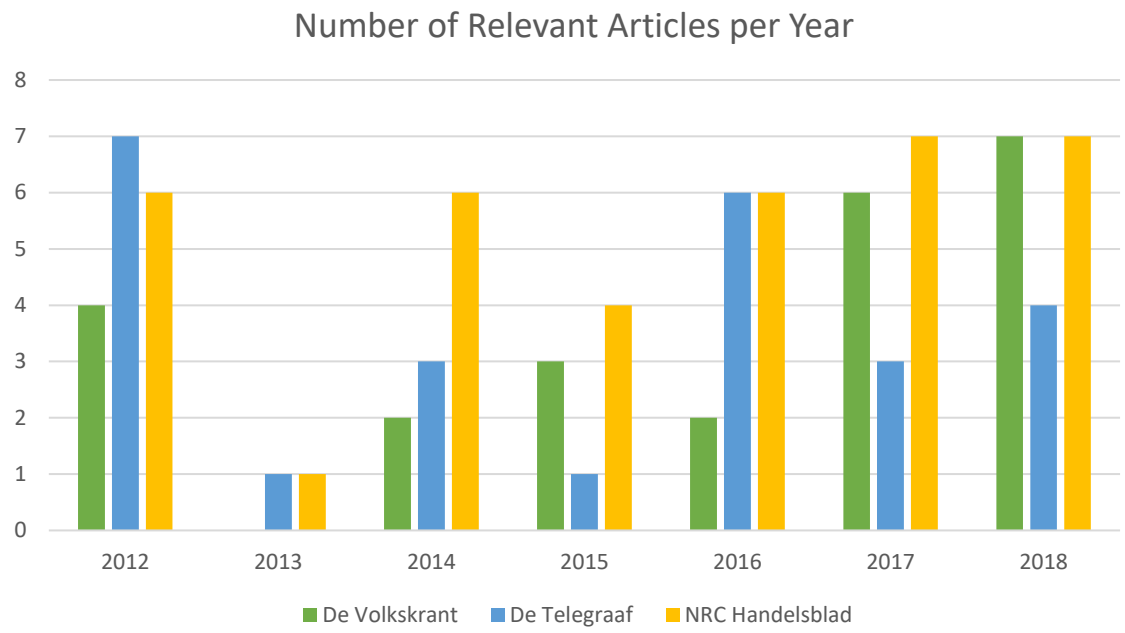

Figure 3: Number of Relevant Articles per Year

4.1.2. Content of the Articles

Figure 3 shows the number of relevant articles per year and per newspaper. As the figure displays, in 2012 there were relatively a large number of relevant articles published on data breaches compared to the years after. In this year legislation for the obligation to report data breaches was proposed with the goal to be able to fine organisations and maintain protection and privacy of individuals (De Volkskrant, 2012; De Telegraaf, 2012).

One of the other reasons for this increased attention is the KPN hack that made a lot of tumult and earned two articles per newspaper in this year (NRC Handelsblad 2012; De Telegraaf, 2012; De Volkskrant, 2012). KPN is a telecom company and possesses personal data of many individuals and provides the networks for the Dutch government as well. Eventually, the data was not copied from the KPN databases, but stolen in a previous hack from an online store that included email addresses from KPN users (NRC Handelsblad, 2012; De Volkskrant 2012). Even though the personal data was not copied from KPN, hackers were able to break into the systems and the newspapers wrote about the lack of security (NRC Handelsblad, 2012) and possible measures such as fines (De Telegraaf, 2012). This hack was mentioned in other articles in the following years as well and NRC Handelsblad wrote another article on this incident again in 2015.

In the same year a hospital in Gouda was hacked because the hacker guessed the password. NRC Handelsblad wrote an article on this breach and De Telegraaf dedicated three articles on

this hack in 2012 including one more in 2013. Furthermore, this data breach was mentioned in other articles as well. Both breaches highlighted that cyber security was not sufficient especially for such important organisations.

These breaches were on Dutch ground, affecting Dutch people, therefore it was interesting news, since the newspapers published more articles on these breaches compared to other breaches that happened in the same year. LinkedIn was hacked as well in 2012 when passwords were stolen and leaked, affecting 6.5 million users (NRC Handelsblad, 2012). Furthermore, iPhone was also breached, personal data of about a million people was leaked (NRC Handelsblad, 2012). These two breaches affected many more individuals worldwide than the KPN hack, nonetheless only little attention was given to these breaches and the attention that was given pertains to the Dutch victims of these breaches (NRC Handelsblad, 2012). The newspapers always highlight whether or not and how many Dutch people are or could have been affected by a data breach. For example, in 2013 Vodaphone was hacked, however NRC Handelsblad only dedicated a short article on this breach as it only affected German people (NRC Handelsblad, 2013). Nonetheless, this was one of the few relevant articles that were published in 2013.

2013 resulted in little relevant articles, while the keyword search resulted in a large number of articles. For example, the Telegraaf published seven relevant articles in 2012 and only one in 2013. Most articles that were found with the keyword search were about the revelations from Edward Snowden, these articles are not included in the analysis as these revelations have a different nature than the articles that write about data breaches due to malicious intent affecting the personal data and privacy of individuals. The Snowden revelations affected the US government by revealing how the NSA is interfering the privacy of individuals. Analysing the framing of the Snowden revelations would be an entirely different research because the offence in this scenario comes from the US government who not necessarily aimed to commit a wrongful act. This also explains why figure 3 differs from figure 2 in the previous chapter. Figure 2 shows a gradual increase in newspaper articles from 2012 onwards, but figure 3 shows a dip because not all articles were relevant for this research that were found with the key word search.

2014 has an increase again in relevant articles, partly due to the ‘Heartbleed’ security failure which resulted in a spill-over effect, as a result of the vulnerability many websites were hacked such as Yahoo, Wetransfer, Flickr, Netflix, Pinterest, Instagram and Tumblr (NRC

Handelsblad, 2014; NRC Handelsblad 2014; De Telegraaf, 2014; De Volkskrant, 2015). Due to this worldwide security vulnerability, 'Heartbleed' or 'Heartbleed bug', it became publicly known that many websites were not properly protected, including governmental websites. The most popular websites appeared to close the gap quickly, but smaller organisations were predicted to have more difficulty with this vulnerability (De Telegraaf, 2014). NRC Handelsblad dedicated two articles on this topic and the Telegraaf one, a year later the Volkskrant wrote an article on 'Heartbleed' as well. De Volkskrant confirms the prediction in De Telegraaf because a year after the vulnerability became public, many websites were still not secured properly, websites did not take the necessary measures to combat the dangers of the vulnerability (De Volkskrant, 2015).

Besides the vulnerability, the European Central Bank, Sony, iCloud and American based bank JP Morgan were hacked and made the news (NRC Handelsblad, 2014; De Volkskrant, 2014; De Telegraaf, 2014). De Telegraaf also warned against "an unprecedented increase" in phishing mails (De Telegraaf, 2014).

In 2015, there was a slight decrease again in the publishing of relevant articles compared to the year before, only eight compared to eleven in 2014. The most notable hack in 2015 was the Ashley Madison hack resulting in millions of personal data used to blackmail people as Ashley Madison is a website for adultery. Many people were affected, also in the Netherlands, as well as famous people and public officials. Eventually, this hack resulted in suicides, which made it a shocking but also sensationalist event (NRC Handelsblad, 2015; De Volkskrant, 2015). NRC Handelsblad wrote two articles, De Volkskrant one and a year later De Telegraaf highlighted the event again.

Furthermore, there was attention for legislation, enforcement of legislation, lack of security and increase of cybercrime. For example, NRC Handelsblad wrote "the privacy and data protection legislation will be renewed" (NRC Handelsblad, 2015). Also, KPN received a fine as a result of the breach in 2012 (NRC Handelsblad, 2015) and many companies appeared still to be vulnerable due to the Heartbleed-bug, organisations failed to protect their data (De Volkskrant, 2015), while there was an increase in cybercrime (De Telegraaf, 2015). The increase in cybercrime and lack of data protection was also recognised by the government. Not only the EU was improving their legislation towards data protection and privacy, but also within the Netherlands new regulations came into effect (Wet Bescherming Persoonsgegevens)

making it obligatory to report a data breach and gives authority to fine organisations (De Volkskrant, 2015).

From 2016 onwards, there is a gradual increase in relevant articles. Due to stricter regulation regarding data protection, this topic receives more attention. Now that it is obligatory to report a breach it became visible how often this happens, also on a smaller scale. For example leaks happen in de medical sector (NRC Handelsblad, 2016) namely, personal data of patients were stolen from Antoni van Leeuwenhoek hospital (NRC Handelsblad, 2016). Additionally, besides the medical sector, increasingly more sectors become victims of cyberattacks. An energy company was hacked (De Telegraaf, 2016), and personal data was stolen from members of the broadcast MAX (NRC Handelsblad, 2016). Furthermore, all three newspapers wrote about the Yahoo hack, as it was one of the largest breaches in history. This breach happened already in 2014 and affected more than 500 million users, their data was copied and sold on the dark web (De Volkskrant, 2016; NRC Handelsblad, 2016; De Telegraaf, 2016).

Due to the increase of data breaches, legislation becomes more intrusive as well. This also receives attention in the news media. New legislation allows the police to hack hackers (NRC Handelsblad, 2016; De Telegraaf, 2016). Officially, this regulation is called Wet Computercriminaliteit III (law against computer criminality), but the more popular name is 'Hackwet' (hack law) because many people oppose to the legislation out of fear for privacy and internet freedom (De Telegraaf, 2016). New legislation and measures are interesting news items as it indicates change, which is news. This in combination with an increase of reported data leaks and breaches raises the topic of data protection and breaches in general.

In 2017, the Yahoo hack became news again, as the hack appears to have affected 3 billion users (NRC Handelsblad, 2017; De Telegraaf, 2017). Other large companies are victims of cybercrime as well, for example, Uber is hacked and pays a sum of money to silence the hackers (NRC Handelsblad, 2017; De Volkskrant, 2017). The breach already happened in 2016 and included data from Dutch clients and drivers as well (NRC Handelsblad, 2017). Because Uber concealed the breach they had to pay a fine to the Dutch Data Protection Authority (De Volkskrant, 2018; De Telegraaf, 2018). Furthermore, Equifax was hacked resulting in the largest cybercrime thus far (De Volkskrant, 2017), yet Dutch clients are reported to be probably safe (NRC Handelsblad, 2017). Lastly, HBO was hacked, the hackers demanded payment otherwise they would release the next Game of Thrones episodes. Besides imagery and scripts also personal data of employees was stolen (De Volkskrant, 2017).

Another notorious incident was the WannaCry ransomware attack. This “wave of attacks exposed vulnerabilities” worldwide in computer systems (De Volkskrant, 2017). This attack portrays how vulnerable society is regarding cyber incidents, as more than 150 countries were infected by the ransomware (De Volkskrant, 2017) This incident also displayed the dark side of Bitcoin, which enabled anonymous payment for the ransomed data (De Volkskrant, 2017).

In 2018, most articles were written on one of the Facebook breaches. This year, Facebook was involved with two scandals as a result of two different data breaches (NRC Handelsblad, 2018; De Telegraaf, 2018; De Volkskrant, 2018). In total the three newspapers wrote eight relevant articles used for this analysis. Facebook did not have their security on point as Cambridge Analytica wrongfully obtained personal data from the platform to use for the US presidency elections. This breach especially questioned the role of Facebook on personal data and privacy. The second breach involved a hack resulting in a leak of 50 million profiles. The second breach was particularly interesting as it affected many people worldwide, including the Netherlands, everyone’s profile could have been hacked and people lose trust in the social media platform (NRC Handelsblad, 2018). In the same year Marriott was hacked, resulting in “one of the largest breaches in history” (De Volkskrant, 2018). This breach affected many more people and even included sensitive financial data (De Volkskrant, 2018; NRC Handelsblad, 2018). This breach received some attention from NRC Handelsblad and De Volkskrant, but the Facebook hacks received outstandingly more media attention even though the amount of data stolen was less significant. This shows that the size of the breach, or the sensitivity of the data does not determine media attention, the more relatable the hack, the more interesting the news is.

Some articles are dedicated to one breach, for example personal data stolen from Erasmus University in the Netherlands (De Telegraaf, 2016), others highlight multiple breaches (Volkskrant, 2014). 68 of the 86 analysed articles were on a particular breach, other articles either highlighted multiple breaches or discussed data breaches in general as a security problem or focused on legislation on data protection. The way these breaches are portrayed by the newspapers depends on the frames that are used. The following section explains how the frame analysis is conducted.

4.2. Frame Analysis

From the collected articles a frame analysis was conducted in order to identify whether or not securitising and desecuritising frames can be identified. The frame matrix is provided in the previous chapter (see figure 1).

A frame matrix is used as a guide for the frame analysis of the newspaper articles. In order to identify a securitising or desecuritising frame there are a few things to look for. First of all, how the threat is represented and what language is used to portray the threat. “Code red” (NRC Handelsblad, 2012; De Volkskrant, 2012) indicates that there is a severe threat, a threat that calls for action. Moreover, terms such as “largest hack in history” (NRC Handelsblad, 2018) or “unknown hacker” (Telegraaf, 2017) also indicate a threat. Certain language can also down play threats. For example, “it is pressured that no sensitive data was stolen” (NRC Handelsblad, 2016) the threat appears not severe and as a result the issue could be desecuritised.

It is also important to indicate to what or to who there is a threat. This is the referent object. In this thesis that is often personal data or privacy, but can also be combined with the economy, finance or society. For example when WannaCry hit, not only was personal data at stake, but also money and even lives (De Volkskrant, 2017). Besides the threat representation and the referent object there are other indicators that can help identify the frame, such as metaphors. For example, “zo lek als een mandje” (leak as a bucket) is a metaphor that is used by the three newspapers many times. Also the use of numbers can be a strong indicator, victims there are, especially when they are Dutch, the more severe the threat appears. For example, “personal data stolen from 57 million Uber users” (NRC Handelsblad, 2017), this was the total amount of data stolen, but the title reads; “personal data stolen from 174.000 Dutch people”, this number is more important because it shows the threat to the Dutch population. Metaphors and numbers can also be used together; such as, “personal data of 8000 children on the streets” (De Telegraaf, 2017). 8000 children is not an incredible number compared to 50 million after the Facebook hack (De Volkskrant, 2018; De Telegraaf, 2018; NRC Handelsblad, 2018). Nonetheless, this made the news probably because its relation with children and the metaphor helps to portray the incident, data was not just stolen, it is ‘on the streets’ available for anyone who is looking for it.

The aim of this research besides identifying securitising and desecuritising frames is also to identify the type of securitisation or desecuritisation. The referent object, the threat representation and the indicators help determine the type of securitisation. Hyper securitising

frames have “a tendency both to exaggerate threats and to resort to excessive countermeasures” (Buzan et al., 1998, p. 27). Hansen and Nissenbaum (2009) restructured the definition towards the cyber sector and define hyper securitisation as discourse hinging on “multi-dimensional cyber disaster scenarios that pack a long list of severe threats” (Hansen & Nissenbaum, 2009, p. 1164). A hyper securitising frame can be; “ransomware is a large threat to everyone and can disrupt society” (De Volkskrant, 2017). This indicates a disaster scenario as the next sentences explain how hospitals were ransomed which could lead to loss of life (De Volkskrant, 2017). Hyper securitising frames can be distinguished from ‘normal’ securitising frames because of the focus on instantaneity and inter-locking effects as the threats can be to society, financial sector or the military and thereby a threat to “all other referent objects and sectors” (Hansen & Nissenbaum, 2009, p. 1164).

Everyday security practice frames link threat scenarios to familiar everyday life experiences, such as “credit card fraud, identity theft and email scamming” (Hansen & Nissenbaum, 2009, p. 1165). This type of securitising frames are most common for data breaches in the Dutch news media as the next sub chapter will elaborate. For example, “phishing, with fake emails from internet criminals with the goal to steal from the consumer, also reached the travel world” (De Telegraaf, 2014). The focus of this threat representation is on small incidents that effect individuals. Even though the financial loss can be large, it is not a disaster scenario.

Lastly, technification of cyber incidents create frames that construct an issue as reliant upon technical, expert knowledge and simultaneously require a politically neutral agenda (Hansen & Nissenbaum, 2009, p. 1167). Technification can be mistaken for desecuritisation but is not, “technifications play a crucial role in legitimating cyber securitisations” (Hansen & Nissenbaum, 2009, p. 1168). Therefore, technification is often not the main frame in the newspaper articles analysed for this thesis. Nevertheless, experts are often mentioned in the articles, such as professors in cyber security (De Volkskrant, 2012).

How an issue or event is portrayed or framed determines the level of securitisation or desecuritisation. A desecuritising frame includes a referent object as well and a ‘desecuritising representation’. ‘Desecuritising representation’ is a vague and broad term, this is because securitising language is easier to recognise than desecuritising language, as this thesis shows in the following section. There are five types of desecuritisation recognised in this thesis: stabilisation, replacement, rearticulation, silencing and normalisation.

Change through stabilisation was not found in this analysis, this will probably only happen when data breaches cease to exist or become very rare, which is an unlikely scenario at the moment. Change through replacement is a frame that was also not identified in this research. Data breach is an umbrella term, as it can include many cyber incidents, therefore this type of threat is not easily replaced, types of breaches could be replaced over the years when some forms of attack go 'out of fashion'. The case is similar for change through silencing, it would rather be the opposite as data breaches are happening every day and newspapers publish more and more about them (see figure 2 and 3). Change through rearticulation frames are recognised in the analysis, such as "not cyber terrorism, but human actions/mistakes" (NRC Handelsblad, 2014). This is a desecuritising frame as the threat is downplayed, not a terrorist is disrupting our systems and networks, but a mistake was made which resulted in a vulnerability. Lastly, change through normalisation is the most common type of desecuritising frame in this analysis. "There is a threat, but it is under control" (De Telegraaf, 2014), or "personal data has been stolen, but it could also have been financial data" (NRC Handelsblad, 2016), the threat is clearly played down in its severity. This type of framing implies that there is no need for action, whereas securitising frames, on the contrary, seek action.

In the frame analysis all newspaper articles are thoroughly studied to find whether or not certain frames can be identified in the paragraphs. In the first round of analysis the articles are read to make sure they are valid for the research. In the second round of analysis the articles are marked and the paragraphs are connected to certain frames when applicable and the dominant or most salient frame in the article is defined. The third round of analysis is the control round to ensure no frames have been left out.

In order to determine which frame is the most salient frame in the article, one analyses the placement and repetition of the frames (Van Gorp, 2007, p. 66). Treating the mentioning of frames as equally salient would give twisted results of what frames would be noticed by the audience and could result in the misinterpretation of the results (Entman, 1993, p. 53). Most articles used for this analysis include more than one frame, some paragraphs even include more than one frame. In order to identify the most salient frame in an article one takes in mind how often a frame is used, where the frames are, for example at the beginning of the article or at the end as a statement, and what the general message is of the article.

4.3. Results and Interpretations

The next section presents the results of the analysis, the frames identified, including the differences between papers and other factors such as length of articles. First the most salient frames are identified. The most salient frame is the most dominant frame in an article. Even though indicating the most salient frame is important, for it portrays the overall message of the article, it is also important to recognise the other frames used in articles. Leaving out the subservient frames in this analysis would give a distorted view of the reality. Newspaper articles often highlight multiple views and therefore also multiple frames.

Besides securitising and desecuritising frame types, a third frame became apparent; the borderline cases. The borderline cases are the failed securitising moves portrayed by the newspapers. This third option does not appear often, but is interesting as it could possibly have a securitising effect. In addition to the frame analysis, this analysis looks at the differences between papers, for the papers have different audiences and different styles and therefore have a difference in what frames they use. The same goes for the length of articles, this differs as well per paper and can influence the number of frames used per article. Lastly, the temporal development is identified to see differences and changes in the seven years of analysis.

4.3.1. Most Salient Frames

The next figure displays the most salient frames found in the newspaper articles of the three newspapers. The frames were identified through precise reading and the most salient frame is the frame that portrays the core of the article.

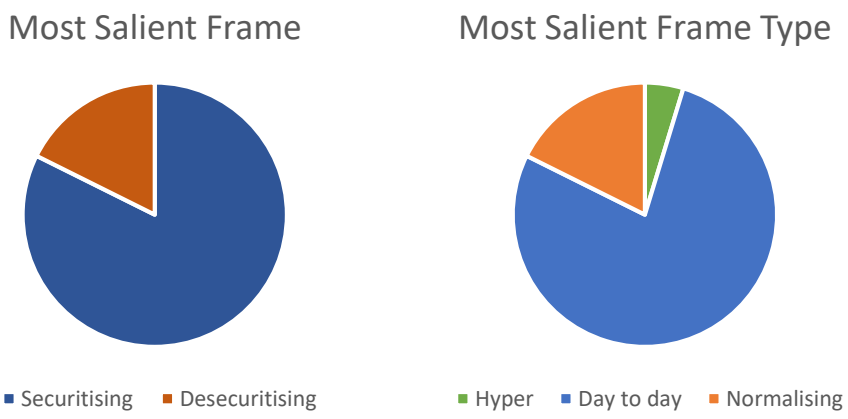

Figure 4: Most Salient Frames and Most Salient Frame Types

The most salient frame in the articles is a securitising frame, indicating that threats are portrayed as a security issue and in need for protection, such as, “society should provide a

larger police force to combat cybercrime" (De Volkskrant, 2017). Nonetheless, almost twenty percent of the articles include desecuritising frames as most salient, indicating that threats are downplayed. For example, "the University of Utrecht sees no need for stricter measurers" (De Telegraaf, 2012), even though an unknown number of usernames and passwords were copied from students and employees of the university.

The most salient frame type is an everyday security practice frame or day to day securitising frame, highlighting the threat to everyday issues, namely individual's personal data and privacy, such as "a hacker copied medical dossiers of almost half a million people" (De Telegraaf, 2012). Reports on sensitive data being stolen from a hospital, affecting a large number of people in that area, portray the threat to everyday life.

Besides everyday security practice frames, hyper securitising frames could be identified as well as most the salient frame type. For example, "when weapons of secret services fall into the hands of criminals, this could be life threatening" (De Volkskrant, 2017). This was one of the frames used during the ransomware attack WannaCry, which provoked disaster scenarios.

The most salient desecuritising frame type is the normalisation of data breaches. For example, in 2016 personal data was stolen from clients from broadcast MAX, but it was pressured that "it was not sensitive data" (NRC Handelsblad, 2016). Here the threat is played down, as it could have been worse.

As the most salient frames are everyday security practices, this is what the audience reads and possibly shapes their perception. Nonetheless, many articles include more than just one frame and this should not be overlooked, because an article can carry more than one message.

4.3.2. Subservient Frames

Most paragraphs include at least one frame and sometimes even more than one frame, for example “on a scale from 1 to 10 this breach is an 11” (NRC Handelsblad, 2014) is securitising language while “we should not all panic en masse” (NRC Handelsblad, 2014) is desecuritising language. Both sentences are in the same paragraph resulting in that this paragraph includes two frames. Simultaneously, not all paragraphs are relevant for this analysis for they do not always include a relevant frame. Therefore, the most salient frame was identified per article, yet articles also include lesser dominant frames, which is here understood as subservient frames. Figure 5 portrays the most salient frame types and the subservient frame types that were found in the articles.

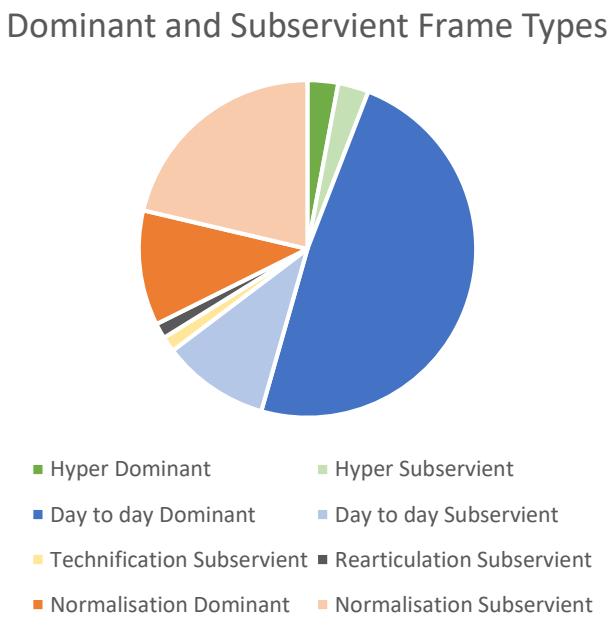

Figure 5: Dominant and Subservient Frame Types

As the figure shows, including less dominant frames shows a larger variety in frames used in newspapers regarding data breaches. As is displayed, some technification (securitising) and rearticulation (desecuritising) frame types, such as use of experts and rearticulating a terror threat to a joke (NRC Handelsblad, 2014), can be identified as well. Furthermore, it shows that even though the securitising frame is often more salient, many articles include desecuritising frames as well. For example, “a data breach was found resulting in theft of personal data” (De Volkskrant, 2018) indicates an everyday security practice frame, however the same article writes, “there are no indicators that Dutch clients are affected” (De Volkskrant, 2018). This has a desecuritising effect because it indicates that Dutch people are safe because “in particular

British people were affected". The threat is portrayed as 'far away'. Besides these frames that were identified beforehand with the help of the literature, a third frame is identified.

4.3.3. Third Option: Borderline Cases

As mentioned in the previous sub section, during the analysis a third frame was identified. Besides securitising frames and desecuritising frames, a third option exists: the portrayal of failed securitisation. These borderline cases indicate that there is or has been a securitising move, but it is or was not accepted by the public.

For example, in 2015, a year after the Heartbleed-bug, De Volkskrant wrote an article arguing that, "a year after the vulnerability was published, hundreds of companies still have not taken measures in order to turn the danger for the better" (De Volkskrant, 2015). This indicates that there has been a securitising move, yet it failed. De Telegraaf (2014) and NRC Handelsblad (2014) advised people to change their passwords as they wrote articles on the topic with securitising language, such as "the largest vulnerability in the history of the internet" (De Telegraaf, 2014) and "Heartbleed causes alarm, hackers have access to passwords" (NRC Handelsblad, 2014). Nonetheless, "86 percent of Americans has never heard of Heartbleed while the bug was in the news for weeks" (De Volkskrant, 2015). Yet the securitising move failed and this failed move is what the newspaper emphasises. De Volkskrant (2015) questions the extent to which people listened to the advice to change their passwords. One reason for this failed move could be 'bug fatigue' (De Volkskrant, 2015), i.e. people are tired of all the cyber incidents - as they have become commonplace - and lose interest. This is similar to 'security fatigue', meaning that people can get tired of security procedures, it can be stressful to remain at a high level of vigilance and security awareness (Bada et al., 2015).

In the same year De Volkskrant publishes another article of a borderline case: "the dangers of data breaches are collectively ignored" (De Volkskrant, 2015). The title already emphasises that there is a recognised danger, however "actions are taken when it is already too late" (De Volkskrant, 2015). People have a "romanticised image of hackers" (De Volkskrant, 2015) and there is a "general lack of attention towards the danger of data breaches" (De Volkskrant, 2015), "when important information such as pin codes or medical data is at stake, people do not seem to worry" (De Volkskrant, 2015). Again, the failed securitising move is recognised by the newspaper. The securitising move and its failure are both acknowledged which can be interpreted as a securitising move or an attempt to securitise.

Lastly, the papers often recognise the failed securitising move by mentioning that people are naïve, use too often the same passwords for various services and inadequately handle their personal data (De Volkskrant, 2014; NRC Handelsblad, 2012). These borderline cases are not very visible and often used in combination with one of the other frames. Nonetheless, it is an interesting way to portray data breaches. Writing about how security is failing could possible improve security practices.

Besides the multiple frame types recognised in the articles of the newspapers, including the borderline cases, this analysis indicates the differences between the newspapers because these newspapers have different audiences and therefore write different about data breaches as the analysis shows in the next section.

4.3.4. Frames per Newspaper

In 2016, Uber became victim of a large data breach and all three newspapers wrote about the Uber hack in 2017 and 2018. Nonetheless, the way this breach was framed is rather different when analysing the different newspapers. De Volkskrant uses mainly securitising frames for this breach, highlighting the threat to the referent objects, "hackers had access to personal data of 57 million Uber-accounts - names, email addresses and phone numbers were stolen, also driver licence numbers of 600 thousand chauffeurs are on the streets" (De Volkskrant, 2017). While NRC Handelsblad and De Telegraaf predominantly use desecuritising frames, "no credit card data, bank account numbers, citizen service numbers, data of birth and location data was stolen" (NRC Handelsblad, 2017). NRC Handelsblad excessively portrays all the personal data that was not stolen, while De Volkskrant only represents all the personal data that was stolen. De Telegraaf accentuates the solutions, "the company assures that the systems are better protected now. Furthermore, Uber appointed board members for privacy, data protection and security. The company declares that they are working hard to keep the promise to win back the trust of the users" (De Telegraaf, 2018). This focus on solutions rather than consequences indicates a desecuritising frame. Overall, it can be argued that De Volkskrant uses more securitising frames compared to the two other newspapers on data breaches (see figure 6).

There are a few prominent differences between the three newspapers, not only differs how data breaches are portrayed, also the style these newspapers use varies. De Telegraaf uses more metaphors such as "zo lek als een mandje" (leak as a bucket) and "gegevens liggen op straat" (data on the streets). Metaphors can help people visualise an incident and can help give strength to a frame. The other newspapers use these metaphors as well, but not as extensively.

Moreover, De Telegraaf uses more strong and direct language such as, “give KPN a fine” (De Telegraaf, 2012), while De Volkskrant and NRC Handelsblad are more reserved. NRC Handelsblad often includes advice in its articles, explaining to its readers how to react to a data breach and how to protect personal data.

Figure 6: Most Salient Frame Types per Newspaper

Figure 6 displays the most salient frame types per newspaper. The everyday security practice frame is often the most salient frame, between 75% and 80% of the time. Notable is that the hyper securitising frame, as the most salient frame, is solely used by De Volkskrant, while the normalising frame type, as the most salient frame type, is more commonly recognised in De Telegraaf and NRC Handelsblad. Hyper securitising frame types occur when something unknown or unprecedented happens such as the WannaCry ransomware attack in 2017. De Volkskrant wrote two articles about this breach and the most salient frame type in these articles were hyper securitising frames, such as, “we cannot match up to the evolution of this type of malware” (De Volkskrant, 2017). De Volkskrant shows a disaster scenario here while NRC Handelsblad and De Telegraaf did not publish relevant articles on WannaCry at all.

NRC Handelsblad includes most normalising frames in this analysis compared to the other newspapers. NRC Handelsblad generally highlights multiple views on an incident, for example, “personal data was stolen from the registered members from the broadcast MAX website” but also “the broadcast pressures that no sensitive data was stolen” (NRC Handelsblad, 2016). Two frames are included in the same paragraph, highlighting two sides of problem. First the threat is explained and afterwards downplayed.

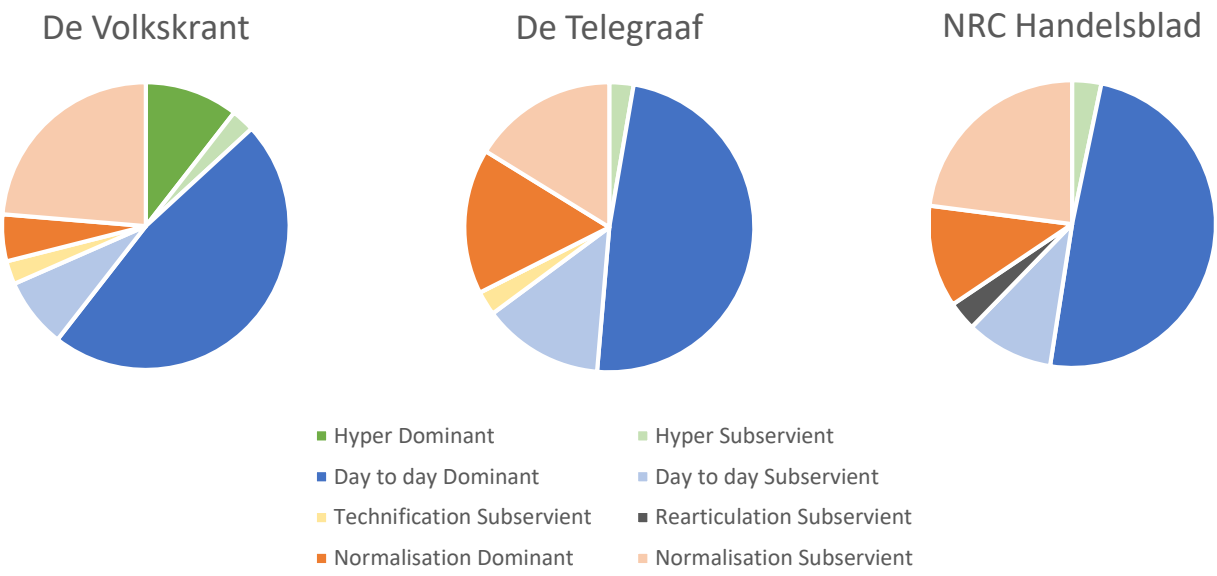

Figure 7: Dominant and Subservient Frame Types per Newspaper

Figure 7 includes the less dominant frames per newspaper. Interesting here is that even though De Volkskrant did not publish frequently using normalisation as the most salient frame, it is often included as a lesser dominant frame in the articles. For example, De Volkskrant uses prognostic language that has a focus on improvements and solutions, such as, "a part of the investments will go to IT-systems" and "they try to understand how hackers breached the systems and how this can be prevented in the future" (De Volkskrant, 2012). The remaining part of the article is however more securitising. Furthermore, NRC Handelsblad uses the most desecuritising frame types compared to the two other newspapers, such as rearticulation, "no cyberterrorism, but the work of people" (NRC Handelsblad, 2014). NRC Handelsblad uses a larger variety of frames as was discussed before, this is also possible because of the size of the articles, as will be discussed in the next section.

4.3.5. Length of Articles

According to agenda setting theory, length and volume of articles and news items can influence the effects that the given topic has on the audience (McCombs & Shaw, 1972, p. 185). News media can set public agenda by assigning various levels of importance to certain topics by reporting on some issues more extensively than on other issues (McCombs & Shaw, 1972). Therefore it is interesting to look into the lengths of the articles to determine how much importance the topic receives from the newspapers as there is a significant relationship between length of the news articles and its perceived importance (Cissel, 2012, p. 71). The magnitude of the articles is often signified by location of the incident and length of the articles (Cissel, 2012, p. 71).

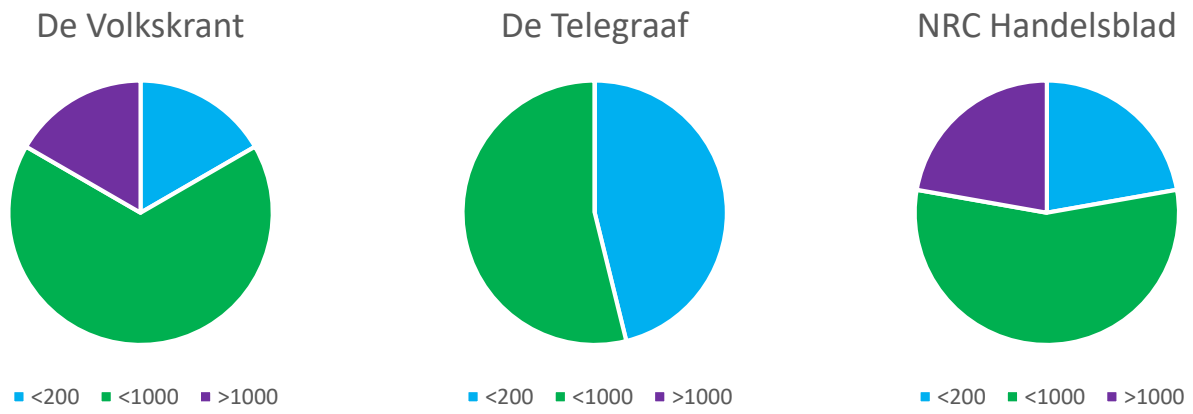

Figure 8: Article Length in Words per Newspaper

Between 2012 and 2017 De Volkskrant published 24 relevant articles, De Telegraaf 25 and NRC Handelsblad 37. NRC Handelsblad dedicates relatively more attention to the topic compared to the two other newspapers. Additionally, when looking at the length of the articles, NRC Handelsblad uses most words per article compared to the other two newspapers.

In general, most newspaper articles are around 800 words (Morrissey, 2015, May 1), however in recent years people increasingly read the news online instead of print (Morrissey, 2015, May 1). Journalists are therefore often pressured to write articles between the 300 and 500 words (Bernstein, 2015, July 15). Hence, articles with a length between 200 and 1000 words are considered 'regular' sized articles for this thesis. Articles with less than 200 words are considered 'short' articles, these articles are often only one paragraph. Articles with more than 1000 words are considered 'long' articles. Distinctive is that De Telegraaf did not publish long articles and a published a significant number of short articles on this topic. However, all three newspapers provided a majority of regular sized articles, as this size is most common.

The longer the article the more frames it can include. Short articles often include one frame type while longer articles highlight different points of view to conform to the balance norm (Berbers et al., 2016) and present various angles from an issue. Nonetheless, an article does not have to be more than 1000 words to include various frames, for example, in 2014 De Volkskrant and NRC Handelsblad both published an article around 600 words that included three frame types (everyday security practice, hyper securitisation, normalisation and rearticulation) (De Volkskrant, 2014; NRC Handelsblad 2014).

It can be argued that the audience from NRC Handelsblad receives most information and the largest variety in frames about data breaches, as this newspaper provides the largest percentage of articles, the largest percentage on long articles about this topic and the largest diversity in frames. Yet, the length of the articles does not necessarily determine the variety of frames per article, also short and comprehensive articles can include various frames.

4.3.6. Temporal Development

The analysis is conducted from newspaper articles over the course of seven years. The aim was to research whether or not a development in the use of frames becomes visible between 2012 and 2018. The timeframe was chosen because of an increase in newspaper articles about data breaches (see figure 2) and because between 2012 and 2018 the legislation around data protection and privacy went through multiple changes on national level and EU level, as explained in the methodology section. The timeframe allows an analysis before the GDPR entered into force, after the GDPR entered into force, before it came into effect and after it came into effect. Nonetheless, there is no significant temporal development in the development in frames, no increase or decrease of particular frames or frame types can be identified over the years of this analysis that can be linked to the adoption of the GDPR.

Despite the fact that this analysis does not identify significant changes in the use of frames over the years there are other temporal developments. There is an increase in newspaper articles as figure 2 visualises, also the number of articles used for this thesis increases in the last few years as becomes visible in figure 3. An increase of news items on this topic could be the result of an increase of data breaches globally (Information is Beautiful, 2019). In the Netherlands there has been an increase in data leaks as well 20.000 reported leaks in 2018 compared to 10.000 reported leaks in 2017 (Autoriteit persoonsgegevens, 2019), with these sources combined it could be argued that there is an increase of data breaches that are relevant for the Dutch news media. In turn data breaches could be a more known topic to the public in general. Moreover,

the increase in regulation regarding data protection nationally and on EU level could also have helped with the increase of news items on this topic, as legislation is regularly mentioned in the newspaper articles.

This sub chapter provided the results and interpretations of the frame analysis. The most salient frames were identified per newspaper including also the subservient frames. Furthermore, a third frame was identified - the borderline cases - and attention was given to the length of the articles and temporal development. The next chapter provides the implications of the results in the discussion.

5. Discussion

This thesis contributed to the knowledge gap by shining a broader light on how data breaches are portrayed by Dutch news media. It did so by not solely analysing securitising language that is frequently associated with cyber incidents, but also by identifying desecuritising language. This thesis hopes to give insights on the possible implications of framing of data breaches. The next section elaborates on the implications of the results of this thesis by synthesising the results with theory. Furthermore, the limitations and further recommendations are discussed as well.

5.1. Discussion

The theoretical framework constructed the fundament of this research. securitisation theory, including desecuritisation, form the lenses through which this research is conducted. Furthermore, framing theory, including agenda setting theory, help understand what the results of the analysis mean.

Overall, the most common frame between 2012 and 2018 regarding data breaches in Dutch media were everyday security practices. Yet, whether these securitising frames resulted in securitisation stays rather unclear as desecuritising frames and failed securitisation were identified as well. As there is still an increase in data breaches globally it would be advisable to keep working on cyber security, especially data protection and awareness. Nonetheless, one has to be aware of security fatigue and bug fatigue in the process.

A securitising discourse can initiate action while a desecuritising discourse can result in a lack of security measures (Dunn Cavelty, 2015). Dunn Cavelty (2015) warns against the latter, she argues that cyber incidents are toned down by the news media. Nonetheless, the results of this thesis imply the opposite, more securitising frames were found in the analysis than desecuritising frames. Although, it is important to keep in mind that the scope of this research was solely on data breaches and not on cyber incidents in general, therefore the results do not necessarily apply to all cyber incidents.

According to agenda setting theory (McCombs & Shaw, 1972; Chong & Druckman, 2007) news media frames can shape public perception and perception can result in action. As securitising frames are the most salient, this could result in more securitising measures and behaviour. The main frame is the everyday security practice frame, securitising daily practices and focus on the threat to everyday life. Many of the researched articles encourage the government, companies and the public to improve their digital security, while highlighting the

threats to their security regarding personal data and privacy. Simultaneously, it is recognised that securitising moves are not always accepted by the public, people appear naïve and do not adequately handle their personal data, this also becomes visible in organisations where cyber security is often not sufficient technology wise, process wise and people wise. Moreover, many articles also include desecuritising frames, one paragraph shows a threat, while the next paragraph downplays the threat again by minimising the consequences and focus on solutions. This normalisation of data breaches does not motivate the public to change their behaviour regarding their personal data and privacy.

Dunn Cavelty (2008) and Guitton (2013) claim that the securitisation of cyberspace has failed and in the some newspaper articles this failed securitisation is recognised as well regarding data breaches. Failed securitisation could be the result of desecuritising language (Dunn Cavelty, 2008) nonetheless, the most salient frame is frequently a securitising frame. Therefore, this failed securitisation could be the result of an abundance of subservient desecuritising frames in the news media or possibly more hidden desecuritising frames were missed in this analysis. Another possibility could be that public agenda is not as easily set as anticipated, possibly as a result of the subservient desecuritising frames. The securitising frames make people aware of a threat to daily life, but the desecuritising frames also make data breaches part of daily life. Lastly, an abundance in securitising frames and security measures can result in security fatigue (Bada et al., 2015). The same is argued in the Volkskrant (2015) about bug fatigue, people are tired of the increase in viruses and bugs that steal or ransom personal data which can result in a lack of security practices.

Overall, the theoretical framework and methodological framework provided well for conducting the analysis and in order to research what frames were used in the newspaper articles regarding data breaches. Nonetheless, it is difficult to make a clear argument for the possible implications of the frames on public perception and cyber security. As mentioned before, De Bruijn and Janssen (2017, p. 1) claim that certain frames can actually contribute to the awareness of the public. They state that one should "1) not exacerbate cybersecurity, 2) make clear who the villains are, 3) put the heroes in the spotlight, 4) show the importance of cybersecurity for society, 5) personalise it, and 6) connect cybersecurity to other issues". Awareness might not be created by using securitising or desecuritising frames, yet the frames mentioned by De Bruijn and Jansen (2017) might be more successful, however these frames were not included in this analysis, it is therefore recommended for further research. Before moving on to the recommendations that resulted from this thesis, the limitations are discussed.

5.2. Limitations

The research design of this thesis implied a number of limitations. First, a discourse analysis and frame analysis include the risk of research bias and the difficulty of interpretation. When studying language, the researcher is dependent on the interpretations of oneself (Bryman, 2012). Therefore, different conclusions could be drawn from the analysis that was conducted for this thesis depending on the researcher. For further research it would be advisable to include multiple researchers for the analysis to overcome this limitation and limit research bias.

Another limitation on bias comes from the newspapers and the journalists. Not only is the researcher biased when doing a frame analysis, also the journalists and the newspapers overall are biased and influenced by each other and other news outlets on how to portray data breaches.

Therefore, the sample of the newspapers and newspaper articles affects the generalisability of this research. The scope of the precise topic of this research was necessary to be able to draw relevant conclusions about similar data breaches and how they are portrayed, as the analysis was limited to articles that concern data breaches affecting personal data and privacy of individuals. Nonetheless, this resulted in a relatively small sample of newspaper articles. For further research it would be recommended to analyse more newspaper articles to increase external validity.

Adding to this, to be able to draw conclusions for a larger audience, it is advisable to analyse news media from various countries as this research is limited to Dutch news media. Subsequently, studying other news outlets could give more insights in the differences between media and how data breaches are portrayed, as this thesis is limited to newspapers and people nowadays receive much of their information from other media.

An additional limitation in this thesis are the theoretical lenses used to recognise the frames. As was indicated before, securitising language is easier to recognise than desecuritising language. The use of a frame matrix helps to identify desecuritising language, but it is still dependent on the researcher whether or not this language is identified. For future research it would help to introduce more researchers and do more research on how to conduct a frame analysis for desecuritising language, this is however limited. Lastly, by focussing on securitising and desecuritising frames, other frames could have been missed, for further research it would be recommended to include the frames De Bruijn and Jansen (2017) propose as indicated in the previous section.

5.3. Recommendations

Besides the recommendations to introduce more researchers to overcome bias, introduce more newspapers from the Netherlands or from abroad, introduce a larger amount of news outlets to increase relevant texts and therefore increase generalisability, additional research directions are proposed. Supplementary research is needed in the desecuritisation of data breaches and especially on how to recognise desecuritising language on this topic. Dunn Cavelty (2008; 2015) made an attempt to research desecuritisation and normalisation of cyber incidents and this thesis attempted to determine whether or not data breaches are being securitised or desecuritised. Further research is recommended on this topic as there still exist questions, such as whether or not desecuritising frames are hidden in the messages that the public receives about data breaches or has the securitisation of data breaches failed possibly as a result of security fatigue.

Therefore, research on public perception is recommended, by testing a research group on the topic of data breaches and what their perceptions are on this topic. This type of research is rather difficult, yet it could give interesting insights to the questions in the previous sections. It could also give more insights in cyber security awareness of the public and how security/bug fatigue works in practice. It would therefore be recommended to keep in mind the frames provided by De Bruijn and Jansen (2017) for this sequential research.

6. Conclusion

This thesis made an attempt to research how data breaches are framed in the Dutch news media. Data breaches are an increasing problem as they happen increasingly and people store large amounts of personal data online. Simultaneously, in the last couple of years regulations have sharpened regarding data protection and privacy, and the topic receives more attention from the media. How data breaches are framed in the news media can help understand how people perceive data breaches which can help combat this security issue.

As a result of doing this research the following conclusions can be drawn. Based on securitisation theory, including desecuritisation, and framing theory, using discourse and frame analysis, this thesis tried to give an answer to the research question which was:

How are data breaches framed between 2012 and 2018 by Dutch news media (De Telegraaf, NRC Handelsblad and De Volkskrant) and what are the possible implications of such frames?

In order to give answer to this research question a theoretical framework was constructed, consisting of securitisation theory, desecuritisation and framing theory. Securitisation and desecuritisation were used as theoretical lenses to establish a frame analysis. The frame analysis itself is based on framing theory, including agenda setting theory. Agenda setting theory claims that public agenda can be set by frames used in news media. Therefore, a securitising frame would possibly result in the public perceiving data breaches as a security problem and desecuritising frames would possibly result in the public perceiving data breaches as part of everyday life and not necessarily a security problem.

The frame analysis of 86 newspaper articles from three Dutch newspapers between 2012 and 2018 resulted in a majority of securitising frames. One would therefore expect that the public perceives data breaches as a threat to their security and initiate action. Nonetheless, almost twenty percent of the most salient frames were desecuritising and many of the articles with mainly securitising frames frequently included subservient desecuritising frames. Furthermore, it was identified that the newspapers recognised failed securitisation; people do not handle their data adequately, they are often naïve when it comes to safe passwords even though they have been advised or warned. It is recognised that people are tired of the increase of data breaches and the increase in security measures. This fatigue is identified as bug fatigue in De Volkskrant (2015) and is similar to security fatigue as identified by Bada et al. (2015).

It is therefore concluded that even though securitising frames were identified as most frequently the most salient frame, that this does not necessarily result in the public perceiving data breaches as a security threat, or at least not enough to actually change behaviour regarding cybersecurity. The implications of the frames are more varied due to the subservient desecuritising frames, possible hidden desecuritising frames and the recognised failed securitisation, including bug/security fatigue. Therefore it is argued that the securitising frames do not have the effect that was expected, namely to securitise the perception that people have on data breaches. Nonetheless, the main goal of this thesis was to analyse the frames used in Dutch newspaper articles regarding data breaches, making proper conclusions about the possible implications of the identified frames is rather challenging. Consequently, it would be advisable to concern further research on data protection awareness within organisations and the public in general in order to create a more cyber secure and privacy/personal data aware society.

References

Altheide, D.L. (1987). Format and symbols in tv coverage of terrorism in the United States and Great Britain. *International studies quarterly, 30*(2), 161-176.

Ani, U.P.D., He, H.M., Tiware, A. (2016). Human capability evaluation approach for cyber security in critical industrial infrastructure. *Advances in human factors in cybersecurity.* Springer: 169-182

Autoriteit persoonsgegevens (2018, April 24). Retrieved from: <https://autoriteitpersoonsgegevens.nl>

Bada, M., Sasse, A., Nurse, J.R.C. (2015). Cyber security awareness campaigns: why do they fail to change behaviour?. *International Conference on Cyber Security for Sustainable Society.* 118-131.

Baldwin, D.A. (1997). The concept of security. *Review of International Studies, 23*, 5-26.

Barnard-Wills, D. & Ashenden, D. (2012). Securing virtual space: cyber war, cyber terror, and risk. *Space and Culture, 15*(2), 110-123.

Berbers, A., Joris, W., Boesman, J. d'Haenens, L. Koeman, J. & Van Gorp, B. (2016). The news framing of the 'Syria fighters' in Flanders and the Netherlands: Victims or terrorists? *Ethnicities, 16*(6), 798-818.

Berkowitz, D.A. (1997). *Social meanings of news: a text-reader.* Thousand Oaks: Sage Publications.

Bernstein, J. (2015, July 15). TLDR: So just how short should your online article be? Retrieved from: < https://www.theguardian.com/media-network/2015/jul/15/tldr-quartz-associated-press-article-length>

Biba, S. (2013). Desecuritization in China's behaviour towards its transboundary rivers: the Mekong river, the Bramaputra river, and the Irtysh and Ili Rivers. *Journal of Contemporary China, 23*(85), 21-43.

Bits of Freedom (2018). Hackwet voor de politie. Retrieved from: <https://www.bitsoffreedom.nl/dossiers/hackvoorstel/>

Boukes, M. & Vliegenthart, R. (2017). Hoe populaire en kwaliteitskranten van elkaar verschillen in verslaggeving. De Nieuwe Reporter, 19 September 2017. Retrieved from: <http://www.denieuwereporter.nl/2017/09/hoe-populaire-en-kwaliteitskranten-van-elkaar-verschillen-in-verslaggeving/>

Brosius, H. & Kepplinger, M. (1990). The agenda-setting function of television news: static and dynamic views. *Communication research, 17*, 183-211.

Brown, K. E. (2011). Muriel's wedding: News media representations of Europe's first female suicide terrorist. *European Journal of Cultural Studies, 14*(6), 705-726.

Bryant, J. & Zillman, D. (1997). *Media effects: advances in theory and research.* Hillsdale: Lawrence Erlbaum Associates.

Bryman, A. (2012). *Social Research Methods.* 4th edition. New York: Oxford University Press.

Buzan, B. (1991). *States, and fear: an agenda for international security studies in the Post-Cold War*. London: Harvester Wheatsheaf.

Buzan, B. Waever, O. de Wilde, J. (1998). *Security a new framework for analysis.* London: Lynne Rienner.

Carruthers, S.L. (2000). *Media at war: Communication and conflict in the twentieth century*. London: Macmillan.

Chong, D. & Druckman, J.N. (2007). Framing theory. *Annual Review of Political Science, 10*, 103-126.

Cissel, M. (2012). Media framing: a comparative content analysis on mainstream and alternative news coverage of Occupy Wall Street. *Strategic Communications Elon University*. 67-77.

Cruz Lobato, L. & Kenkel, K.M. (2015). Discourses of cyberspace securitization in Brazil and the United States.

Das, S. (2018, August 08). Are data breaches becoming the new normal? Retrieved from: < https://www.cioandleader.com/article/2018/08/08/are-data-breaches-becoming-new-normal>

Davis, J.L. & Gandy Jr., O.H. (1999). Racial identity and media orientation: exploring the nature of constraint. *Journal of Black Studies 29*(3), 367.

De Bruijn, H. & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly 34*, 1-7.

Deibert, R.J. (2002). Dark guests and great firewalls: the internet and Chinese security policy. *Journal of Social Issues, 58*(1), 143-159.

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

De Vreese, C.H. (2012). new avenues for framing research. *American Behavioral Scientist, 56*(3), 365-375.

Directive 95/46/EC (1995). On the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Directive 2013/40/EU (2013). On attacks against information systems and replacing Council framework decision 2005/222/JHA.

Dirikx, A. & Gelder, D. (2010). To frame is to explain: A deductive frame analysis of Dutch and French climate change coverage during the annual UN Conferences of the Parties. *Public understanding of science, 19*(6), 732-742.

Dunn, K.C. & Neumann, I.B. (2016). *Undertaking discourse analysis for social research.* Ann Arbor, MI: University of Michigan Press.

Dunn Cavelty, M. (2008). Looming threat or phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology & amp; Politics 4*(1), 19-36.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: threat representations with an impact in cyber-security discourse. *Center for Security Stdues, ETH Zurich, 15*, 105-122.

Dunn Cavelty, M. (2015). The normalization of cyber-international relations. *For Center for security studies (CSS).*

Entman, R. (1993). Framing: Towards a clarification of a fractured paradigm. *Journal of Communication, 43*(4), 51-58.

European Data Protection Supervisor (2019). The History of the general data protection regulation. Retrieved from: < https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en>

Gamson, W.A. & Modigliani, A. (1989). Media discourse and public opinion on nuclear power: A constructivist approach. *American Journal of Sociology, 95*(1), 1-37.

General Data Protection Regulation (2018). Article 4: Definitions.

General Data Protection Regulation (2018). Article 99: Entry into force and application.

Giacomello, G. (2014). *Security in cyberspace: Targeting nations, infrastructures, individuals.* London: Bloomsbury.

Guitton, C. (2013). Cyber insecurity as a national threat: overreaction from Germany, France and the UK? *European Security, 22*(1), 21-35.

Hansen, L. (2005). *Security as practice: discourse analysis and the Bosnian war.* Routledge.

Hansen, L. (2012). Reconstructing desecuritisation: the normative-political in the Copenhagen School and directions for how to apply it. *Review of International Studies, 38*(3), 525-546.

Huysmans, J. (2002). Defining social constructivism in security studies: the normative dilemma of writing security. *Alternatives, 27,* 41-62.

Information is Beautiful (2019, April 24). Retrieved from: <https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

Iyengar, S. (1990). Framing responsibility for political issues: The case of poverty. *Political Behavior, 12*(1), 19-40.

Jarvis, L., Macdonald, S. & Whiting, A. (2016). Analogy and authority in cyberterrorism discourse: an analysis of global news media coverage. *Global Society 30*(4), 605-623.

Kahneman, D. & Tverskey, A. (1984). Choice, values, and frames. *American Psychologist, 39*(4), 341-350.

Kortjan, N. & von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal 52,* 29-41.

Kritzinger, E. (2017). Cultivating a cyber-safety culture among school learners in South Africa. *Africa Education Review, 14*(1), 22-41.

Lexis Uni (2019). Retrieved from < https://advance-lexis-com.ezproxy.leidenuniv.nl:2443/search/?pdmfid=1516831&crid=e58404d0-e143-

4364-99cd-8ef3d207236b&pdsearchterms=(databreuk+or+datalek+or+lek)+and+(privacy+or+persoonsgegevens+or+%22gevoelige+informatie%22+or+%22persoonlijke+informatie%22+or+gegevens)+and+(malefide+or+crimineel+or+cybercrime+or+identiteitsfraude+or+hack+or+hacker+or+gehackt+or+darkweb+or+gestolen+or+stelen+or+inbraak+or+ransom+or+ransomware+or+geizelen+or+gegeizeld+or+incident+or+phishing+or+privacy+or+persoonsgegevens+or+AVG+or+cyberincident%2C+or+cybersecurity)&pdstartin=hlct%3A1%3A1&pdtypeofsearch=searchboxclick&pdsearchtype=SearchBox&pdqttype=and&pdquerytemplateid=&ecomp=7sd5k&prid=1bb4b5bc-e2eb-425d-91d3-ccb164daa0c1&cbc=0>

Lecheler, S. & De Vreese, C.H. (2012). News framing and public opinion: A mediation analysis of framing effects on political attitudes. *Journalism & Mass Communication Quarterly, 89*(2), 185-204.

Li, X. (2013). *Internet newspapers: The making of a mainstream medium.* Lawrence Erlbaum Associats, Inc., Publishers: Mahwah.

Liu, Y., Sarabi, A., Zhang, J., Naghizadeh, P., Karir, M., Bailey, M., & Liu, M. (2015). Cloudy with a chance of breach: forecasting cyber security incidents. In *USENIX Security Symposium*: 1009-1024.

Matthes, J. (2007). Beyond accessibility? Toward an online and memory-based model of framing effects. *Communications, 32*, 51-78.

McCombs, M.E., & Shaw, D.L. (1972). The agenda-setting function of mass media. *Public opinion quarterly, 36*(2), 176-187.

Morrissey, B. (2015, May 1). Quartz's Kevin Delaney: Time to kill the 800-word article. Retrvied from: < https://digiday.com/podcast/wait-this-is-800-words/>

Nacos, B.L. (2005). The portrayal of female terrorists in de media: similar framing patterns in the news coverage of women in politics and in terrorism. *Studies in Conflict & Terrorism, 28*(5), 435-451.

National Coordinator for Security and Counterterrorism (2018). Cyber security assessment Netherlands.

Nelson, T.E., Oxley, Z.M. & Clawson, R.A. (1997). Toward a psychology of framing effects. *Political Behaviour, 19*(3), 221-246.

Nissenbaum, H. (2005). *Building an information technology security awareness and training program.* Washington: The NIST Handbook: Special Publication, 800-50.

Pan, Z. & Kosicki, G.M. (1993). Framing analysis: An approach to news discourse. *Political Communication, 10*(1), 55-75.

Papert, S., & Harel, I. (1991). Situating constructionism. *Constructionism, 36*(2), 1-11.

Politieke kleur herkenbaar in krant (2006, November 21). Retrieved from: <https://www.adformatie.nl/merkstrategie/politieke-kleur-herkenbaar-krant>

Security.nl (2011, September 5). "Diginotar-hack belangrijker dan Stuxnetworm". Retrieved from: <https://www.security.nl/posting/33418/%22Diginotar-hack+belangrijker+dan+Stuxnetworm%22>

Schmidt, N. (2014). Critical comments on current research agenda in cyber security. *Obrana a Strategie, 14*(1): 29-38.

Shah, D.V., Watts, M.D. & Fan, D.P. (2002). News framing and cueing of issue regimes: explaining Clinton's public approval in spite of scandal. *Public Opinion Quarterly, 66*(3), 339-

Slothuus, R. (2008). More than weighting cognitive importance: A dual process model of issue framing effects. *Political Psychology, 29*, 1-28.

Soroka, S.N. (2002). *Agenda-setting dynamics in Canada.* Vancouver: UBC Press.

Three ways to build digital trust in the age of normalized data breaches (2019, January 9). Retrieved from: <https://www.prnewswire.com/in/news-releases/3-ways-to-build-digital-trust-in-the-age-of-normalized-data-breaches-853812933.html>

Tuchman, G. (1978). Professionalism as an agent of legitimation. *Journal of Communication, 28*(2), 106-113.

Van Der Meulen, N. (2013). DigiNotar: Dissecting the first Dutch digital disaster. *Journal of Strategic Security, 6*(2), 46-58.

Van Gorp, B. (2007). The constructionist approach to framing: Bringing culture back. *Journal of Communication, 57*(1), 60-78.

Van Schaik, P. Jeske, D. Onibokun, J. Coventry, L. Jansen, J. Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behavior. *Computers in Human Behavior, 75*, 547-559.

Verschil tussen kranten (2017, December 10). Retrieved from: < http://verschillen-tussen.nl/verschil-tussen-kranten/>

Vlucht, B. (2018, November 13). Bereiksonderzoek mediamerken NU.nl en De Telegraaf versterken posities in online bereik. Retrieved from: https://nederlandsmedianieuws.nl/media-nieuws/Bereiksonderzoek-mediamerken-NU-nl-versterkt-koppositie-online-bereik/

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

Wat stemmen krantenlezers? (2016, March 4). Retrieved from: <https://www.ad.nl/binnenland/wat-stemmen-krantenlezers~a655e176/>

Weaver, O. (1995). *Securitization/desecuritization.* New York: Columbia University Press.

Welke krant past bij mij: Nederlandse dagbladen (viewed on: 2019, March 25). Retrieved from: <https://educatie-en-school.infonu.nl/diversen/28618-welke-krant-past-bij-mij-nederlandse-dagbladen.html>

Wittendorp, S. (October, 2018). Method lab discourse analysis Leiden University.

Wodak, R. & Krzyzanowski, M. (2008). *Qualitative discourse analysis in the social sciences.* Palgrave Macmillan.

Zajko, M. (2015). Canada's cyber security and the changing threat landscape. *Critical Studies on Security, 3*(2), 147-161.

Newspaper Articles Used in the Analysis

De Volkskrant (chronological order)

Keunig, W. (2012). *"KPN: hack gevolg van achterstallig onderhoud"*. De Volkskrant, 14 February 2012.

Keunig, W. (2012). *"De wereldwijde jacht op de KPN-hacker"*. De Volkskrant, 7 April 2012.

De Volkskrant (2012). *"SNMP-lek mogelijk vele malen groter dan affaire-DigiNotar"*. De Volkskrant, 1 November 2012.

Persson, M. (2014). *"Cybercrime kost Nederland 8 mld"*. De Volkskrant, 10 June 2014.

Persson, M. (2014). *"Hackers stelen kiekjes uit iCloud van Hollywoodsterren"*. De Volkskrant, 2 September 2014.

Van Ammelrooy, P. (2015). *"Bedrijven doen te weinig tegen gevaar van Heartbleed-bug"*. De Volkskrant, 7 April 2015.

De Mooij, G. (2015). *"Gevaar van datalek collectief genegeerd"*. De Volkskrant, 12 August 2015.

De Volkskrant (2015). *"Canadese politie: zelfmoord om lek"*. De Volkskrant, 25 August 2015.

De Volkskrant (2016). *"Data half miljard Yahoo-gebruikers gepikt"*. De Volkskrant, 23 September 2016.

Van Kokswijk, J. (2016). *"Het touwtje uit de digitale achterdeur"*. De Volkskrant, 22 December 2016.

Kreling, T. (2017). *"WannaCry bewijst: digitale aanval is echte bedreiging"*. De Volkskrant, 16 May 2017.

Rooduijn, J. (2017). *"Hoog tijd voor een kritische blik op de bitcoin"*. De Volkskrant, 16 May 2017.

Scheurs, B. (2017). *"Afleveringen en scripts gestolen bij cyberaanval HBO"*. De Volkskrant, 2 August 2017.

Kraak, H. (2017). *"HBO-hackers eisen miljoenen dollars aan losgeld in dreigvideo. Ook telefoonnummers Game of Thrones-acteurs gelekt"*. De Volkskrant, 9 August 2017.

De Volkskrant (2017). *"Equifax: aandelenschandaal na inbraak?"*. De Volkskrant, 9 September 2017.

Verhagen, L. (2017). "*Uber verzwijgt datalek"*. De Volkskrant, 23 November 2017.

Persson, M. (2018). *"Wat het Congres wil weten van Facebook"*. De Volkskrant, 10 April 2018.

Morskate, M. (2018). *"Klanten van Ticketmaster mogelijk dupe datalek. Hack treft vooral Britten"*. De Volkskrant, 29 June 2018.

Feenstra, W. (2018). *"Hackers stelen klantgegevens bij de Persgroep"*. De Volkskrant, 5 July 2018.

De Volkskrant (2018). *"50 miljoen Facebookaccounts gehackt"*. De Volkskrant, 29 September 2018.

De Volkskrant (2018). *"Gegevens klanten na hack op straat"*. De Volkskrant, 13 October 2018.

De Volkskrant (2018). *"Uber krijgt geldboete voor verzwijgen datalek"*. De Volkskrant, 28 November 2018.

Andersen, R. (2018). *"Hacker steelt gegevens van half miljard hotelgasten"*. De Volkskrant, 1 December 2018.

De Telegraaf (chronological order)

De Telegraaf (2012). *"Telecombedrijf KPN gehackt"*. De Telegraaf, 9 February 2012.

De Telegraaf (2012). *"Geef KPN megaboete"*. De Telegraaf, 14 February 2012.

De Telegraaf (2012). *"CBP: Meer richten op handhaven"*. De Telegraaf, 14 February 2012.

Van Deinse, I. (2012). *"Universiteitscomputer zo lek als een mandje; Gegevens studenten op straat na aanval hackers"*. De Telegraaf, 3 October 2012.
De Telegraaf (2012). *"Onthutsend"*. De Telegraaf, 8 October 2012.

Graveland, G. (2012). *"Gegevens patiënten op straat; Hacker kraakt ziekenhuis in Gouda"*. De Telegraaf, 8 October 2012.

De Telegraaf (2012). *"Gouds ziekenhuis straffen; Eerdere waarschuwingen hielpen niet. Dus: Einde oefening bestuur"*. De Telegraaf, 9 October 2012.

De Telegraaf (2013). *"Onthutsend"*. De Telegraaf, 20 February 2013.

De Telegraaf (2014). *"Beschermd tegen lek?; Alfred antwoordt"*. De Telegraaf, 19 April 2014.

Basekin, E. (2014). *"Onderzoek naar JPMorgan"*. De Telegraaf, 5 October 2014.

Eldering, P. (2014). *"Toename phishing duizelingwekkend; Internetfraudeurs openen aanval op reizigers"*. De Telegraaf, 23 October 2014.

Monterie, A.(2015). *"Schrik om cybercrime; Marc Goodman schudt Nederlands bedrijfsleven wakker"*. De Telegraaf, 3 June 2015.

De Telegraaf (2016). *"Online vreemdgaan"*. De Telegraaf, 1 February 2016.

Van Bergen, W. (2016). *"Energiedata op straat"*. De Telegraaf, 15 September 2016.

De Telegraaf (2016). *"Yahoo kampte met data-lek"*. De Telegraaf, 23 September 2016.

Goossens, R. (2016). *"Opwinding om datalek"*. De Telegraaf, 15 november 2016.

De Telegraaf (2016). *"Meer gegevens gelekt na hack"*. De Telegraaf, 22 November 2016.

Jonker, J. (2016). *"Omstreden 'hackwet' komt er"*. De Telegraaf, 13 December 2016.

De Telegraaf (2017). "*Datalek drukt waarde Yahoo"*. De Telegraaf, 22 February 2017.

De Telegraaf (2017). *"Gegevens 8000 kinderen op straat"*. De Telegraaf, 24 February 2017.

De Telegraaf (2018). *"Gezichtsverlies"*. De Telegraaf, 21 March 2018.

De Telegraaf (2018). *"Facebook-lek bij miljoenen"*. De Telegraaf, 29 September 2018.

De Telegraaf (2018). *"Lek Facebook minder groot"*. De Telegraaf, 13 October 2018.

De Telegraaf (2018). *"Taxidienst Uber beboet voor datalek"*. De Telegraaf, 28 November 2018.

NRC Handelsblad (chronical order)

Hijink, M. (2012). *"Hacker kraakt KPN-computers"*. NRC Handelsblad, 9 February 2012.

Hijink, M. (2012). *"De dure inschattingsfouten van KPN"*. NRC Handelsblad, 13 February 2012.

Hijink, M. (2012). *"Eerste hulp bij het LinkedIn-lek; Zes vragen over de hack bij LinkedIn"*. NRC Handelsblad, 7 June 2012.

NRC Handelsblad (2012). *"No Headline in Original"*. NRC Handelsblad, 5 September 2012.

Hijink, M. (2012). *"Bedonderd door de browser"*. NRC Handelsblad, 29 September 2012.

NRC Handelsblad (2012). *"No Headline in Original"*. NRC Handelsblad, 8 October 2012.

NRC Handelsblad (2013). *"No Headline in Original"*. NRC Handelsblad, 13 September 2013.

NRC Handelsblad (2014). *"Beveiliginssleutel internet toch niet zo veilig als gedacht"*. NRC Handelsblad, 9 April 2014.

Eigenraam, A. (2014). *"Advies na beveiligingslek: wijzig je wachtwoord maar"*. NRC Handelsblad, 11 April 2014.

Hijink,, M. (2014). *"Vergeet je wachtwoord – het is niet veilig"*. NRC Handelsblad, 7 May 2014.

NRC Handelsblad (2014). *"Hackers stelen gegevens bij Europese Centrale Bank"*. NRC Handelsblad, 24 July 2014.

Hijink, M. (2014). *"Baas in eigen cloud? Vergeet het maar"*. NRC Handelsblad, 3 September 2014.

Van Zwol, C. (2014). *"Filmschurk neemt wraak in echte wereld"*. NRC Handelsblad, 18 December 2014.

NRC Handelsblad (2015). *"Toezichthouder ACM Boete voor KPN na lek in beveiliging klantgegevens"*. NRC Handelsblad, 3 June 2015.

NRC Handelsblad (2015). "*Lek Ook Nederlandse gebruikers vreemdgangerssite Ashley Madison"*. 21 August 2015.

Hijink, M. (2015). *"Losgeld voor je data; De digitale schandpaal"*. NRC Handelsblad, 29 August 2015.

Heck, W. (2015). *"Hoe gaat de EU je privacy beschermen?"*. NRC Handelsblad, 15 September 2015.

Van Steenbergen, E. (2016). *"Gegevens kankerpatiënten gestolen"*. NRC Handelsblad, 4 March 2016.

NRC Handelsblad (2016). *"Critici van Erdogan. Data van 50 miljoen Turken gehackt"*. NRC Handelsblad, 5 April 2016.

NRC Handelsblad (2016). *"Privacy. 'Gegevens MAX-leden gestolen'"*. NRC Handelsblad, 3 May 2016.

Van Lonkhuyzen, L. (2016). *"Justitie wil nu terughacken"*. NRC Handelsblad, 13 December 2016.

Hijink, M. (2016). *"Een hackrecord voor Yahoo"*. NRC Handelsblad, 15 December 2016.

Van Lonkhuyzen, L. (2016). "*Meeste melding van datalekken uit zorgsector"*. NRC Handelsblad, 28 December 2016.

Lonkhuyzen, L. (2017). *"Merry bloody Christmas, zegt schattige Cayla plots"*. NRC Handelsblad, 3 January 2017.

Lonkhuyzen, L. (2017). *"Datalekken bij gemeenten: het is een beetje een zooitje"*. NRC Handelsblad, 28 January 2017.

NRC Handelsblad (2017). *"Nederlandse server bron van malware"*. NRC Handelsblad, 31 August 2017.

NRC Handelsblad (2017). *"Datadiefstal. Hackers stelen gegevens van miljoenen Amerikaanse creditcardhouders"*. NRC Handelsblad, 8 September 2017.

NRC Handelsblad (2017). *"Hack Yahoo nog groter dan gedacht: alle 3 miljard accounts getroffen"*. NRC handelsblad, 4 October 2017.

NRC Handelsblad (2017). *"Digitale chantage Uber betaalde zwijggeld na groot datalek van gebruikersgegevens"*. NRC Handelsblad, 22 November 2017.

NRC Handelsblad (2017). *"Uber: gegevens van 174.000 Nederlanders gestolen"*. NRC Handelsblad, 13 December 2017.

NRC Handelsblad (2018). *"Datalek Facebook heeft wel heel veel vertrouwen verspeeld"*. NRC Handelsblad, 24 March 2018.

Tamminga, M. (2018). *"De bankencrisis op herhaling: Facebook"*. NRC Handelsblad, 27 March 2018.

NRC Handelsblad (2018). *"DELTA 54,21 dollar / +0,65% Hackers treffen vliegmaatschappij"*. NRC Handelsblad, 6 April 2018.

NRC Handelsblad (2018). *"IAG 6,67 pond / -2,0% Datalek bij Britisch Airways"*. NRC Handelsblad, 7 September 2018.

Hijink, M. (2018). *"Hoe Facebook miljoenen digitale sleutels kwijtraakte"*. NRC Handelsblad, 1 October 2018.

NRC Handelsblad (2018). *Ap*NRC Handelsblad, 30 November 2018.

Nagtegaal, B. (2018). "*Groot datalek bij hotelketen Marriott"*. NRC Handelsblad, 1 December 2018.

Appendices

Appendix A. Overview Newspaper Articles

Document name: Hannah Bakx Appendix 1 Overview Articles

Appendix B. Frame Analysis Newspaper Articles

De Volkskrant

Document name: Hannah Bakx Appendix 2 De Volkskrant

De Telegraaf

Document name: Hannah Bakx Appendix 3 De Telegraaf

NRC Handelsblad

Document name: Hannah Bakx Appendix 4 NRC Handelsblad