Regulating the cyber-realm: how political language and framing strategies in the policy document "National Cyber Security Agenda" regulate the Dutch cyber-discourse

Evi Gimbrere
Utrecht University
CIW Bachelor thesis
Word count: 7272 with references included

Student number: 5949254
Utrecht, 14/02/20
Mentor: Anne Kustritz
Second supervisor: Niels Kerssens

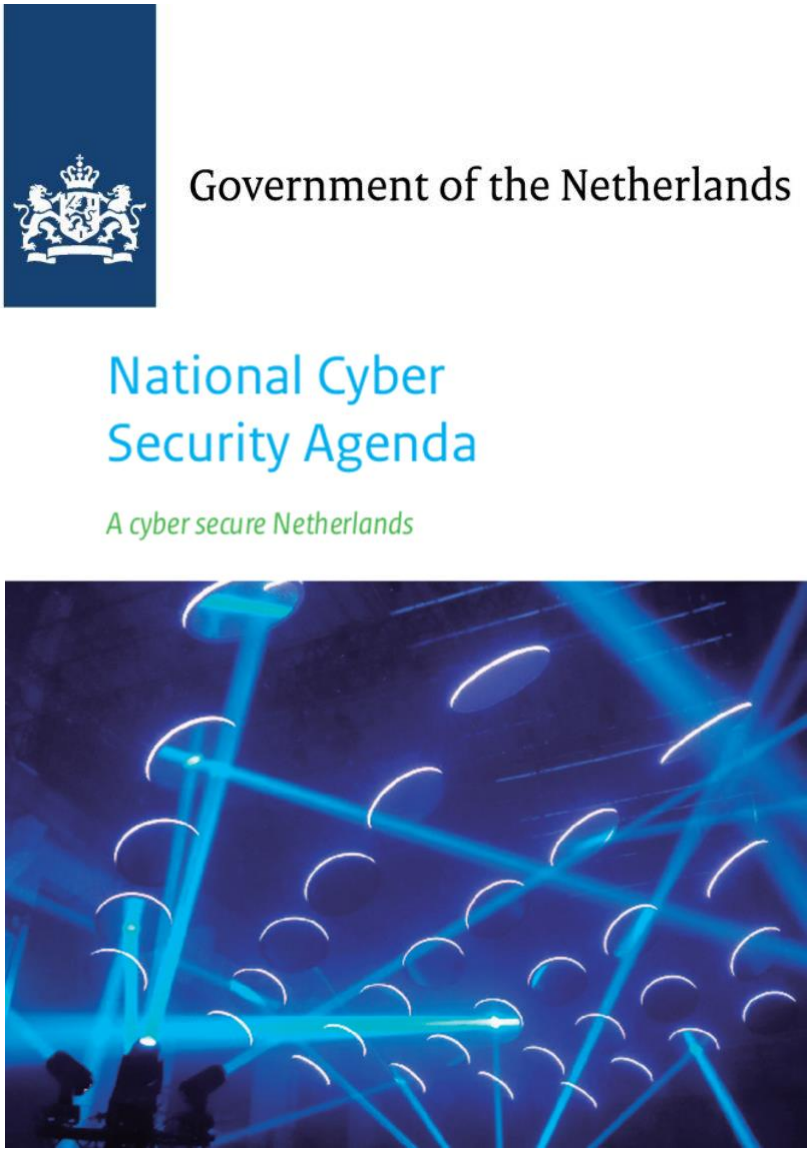

Table of contents

Abstract

This thesis is a case study of a Dutch policy document called the 'National Cyber Security Agenda – a cyber secure Netherlands'. This policy document is established to list seven cybersecurity objectives that are labelled as crucial to respond to cybercrime. A qualitative political discourse approach is chosen to meet its purpose, whereby 'the inclusive technique', 'the fear technique', 'motivational framing', 'prognostic framing', 'conditioning', 'anaphora' and 'referencing' function as categories to display meaning construction in this text and expose what it implies. The analysis of political language and framing strategies fits its purpose to show that by using language as a tool to exert power, the Dutch government, the 'Rijksoverheid' exercises multiple political strategies by exaggerating cyber-threats, aggravating fear, and emphasising the Netherlands as a unity, whereafter the importance of cybersecurity is emphasised and predetermined solutions to achieve this are suggested. The use of "fear-mongering" techniques in combination with offering solutions and unification implies that its function is to gain support from designated parties to fulfil predetermined roles and responsibilities that are in favour of the government.

Keywords: policy, discourse, framing, power, language, politics, strategy, meaning, cybercrime, cybersecurity, regulation, government

Introduction

In the 'National Cyber Security Agenda – a cyber secure Netherlands', cybercrime is depicted as a growing threat that jeopardises society, whereby one in nine people were victims of cybercrime in 2017 (Rijksoverheid, 2018, p.7, 35). 'Cybercrime' is defined by Gordon and Ford as 'any crime that is facilitated or committed using a computer, network, or hardware device' (2006, p.14). Cybersecurity, as its counterpart, is depicted as a crucial foundation for safety in the digital world with a growing need for improvement (Rijksoverheid, 2018). According to the Dutch government, or 'the Rijksoverheid', 'cybersecurity' is defined as 'the entirety of measures to prevent damage caused by disruption, failure or misuse of ICT and to recover should damage occur' (p.9). The Rijksoverheid clarifies the gravity of the cyber-threat by stating that cybersecurity is developing in more and more countries, but that cybercrime is also increasing even more in complexity (p.7). This has consequences, as they state: '[Cybercrime]This forms a direct threat to our economic interests and national security' (p.7, 9, 11). They believe it is of the utmost importance that governments keep the development of cybersecurity in pace with the growth of cybercrime and that it also is important to develop effective law enforcement and related policies continuously. Myriam Dunn Cavelty, a notorious researcher within the field of cybercrime –and security, is Deputy for Research and Teaching at the Center for Security Studies and Senior Lecturer for Security Politics at ETH in Zurich. Cavelty's field of expertise is in (cyber)security politics, specialising in risk and uncertainty within the cyber-domain. Besides that, she advises governments, institutions and companies on cyber issues. Despite of the Rijksoverheid's statement that cybercrime poses a direct threat to national security, Cavelty states that in the last decades, 'the link between national security and cyberspace has become an uncontested, unshakable "truth" with budgetary and political consequences' in politics (2013, p.105). This leaves us with a discussion about how cybercrime as a threat is depicted and immediately centralises the scope of this paper.

Putting aside its degree of truth, according to the Rijksoverheid, improvement of cybersecurity in the Netherlands has become a national concern (Rijksoverheid, 2018, p.5, 7, 8, 9, 11, 13, 17, 19, 35, 43). Cybersecurity policies concern the state as well as the business sector, public-private sector, civil society and relations between these entities. In order to improve cybersecurity, the Rijksoverheid developed the 'National Cyber Security Agenda',

listing several objectives that they assert need to be achieved to manifest a secure, digital Netherlands. With this agenda, the Rijksoverheid endeavours to implement seven contributions. These contributions require close cooperation between public and private organisations, the business sector, and the rest of society (p.5, 8, 17, 43).

Therefore, the question that serves as the very core of this paper is: 'How do the Dutch government's political framing strategies in the "National Cyber Security Agenda" construct regulatory cybersecurity regimes, and therefore regulate how discourse about the cyber-realm in the Netherlands is established in politics?'
The focus is on strategies that shape the depiction of cyberspace. These strategies may function in order to gain public support and 'shirk responsibility', as described by Zheng (2000). This paper therefore attempts to further dig into the depiction of cybercrime and cybersecurity and its meaning formation within the policy document 'National Cyber Security Agenda' (Rijksoverheid, 2018).

First in this thesis, a theoretical framework illuminates discussions between academics and the position this thesis takes among them. This illustrates that there is an infinite discussion about the reality of the cyber-threat and how this threat is depicted in politics. Because statements differ from the idea that cybercrime is increasing and that cybersecurity is 'inextricably linked to national security' (Rijksoverheid, 2018, p.7, 13, 39) to viewpoints that the seriousness of the threat is being exaggerated (Cavelty, 2007, p.4), disagreements about this issue have led to a renewed Dutch interest in research about the depiction of the cyberspace. Additionally, it discusses how language contributes to 'framing', and how that effectuates the depiction of solidarity, the cyber-threat and its seriousness, its responsibilities, the predetermined solutions, and its role determination. It states that there is a need to examine this knowledge-making process in policies and positions this policy within the discussion of government regulation within the cyberspace.

Second, the methodology explains the political discourse analysis as provided by van Dijk, and on a step-by-step basis, the process of conducting this research (1997, 2001). It states that the strategies 'the inclusive technique', 'the fear technique', 'motivational framing', 'prognostic framing', 'conditioning', 'anaphora' and 'referencing' are recognised in this policy and describes their function within the document. Additionally, it shows which words in the policy are marked as important, and why these are connected to these strategies.

The analysis is structured in terms of the aforementioned strategies, whereby language use is explained in terms of these techniques. It implies that the Dutch government's language in the policy document serves to enhance solidarity and unification, to exaggerate threats as a fear-inducing tool, to provide predetermined solutions and to determine roles and responsibilities on how these solutions are meant to be achieved. Furthermore, it states that anaphora and referencing are used to emphasise what is said and that this reinforces other strategies.

This paper will show that by using language as a tool to exert power, the 'Rijksoverheid' exercises multiple political strategies by exaggerating cyber-threats, aggravating fear, and emphasising the Netherlands as a unity, whereafter the importance of cybersecurity is emphasised and predetermined solutions to achieve this are suggested. Their "fear-mongering" techniques in combination with offering solutions and unification imply that its function is to gain support from designated parties to fulfil predetermined roles and responsibilities that are in favour of the government.

Theoretical framework

Policies are used by the government as 'tools of power', according to Braman (1995, p.4). This statement is intertwined with the viewpoint of Teun van Dijk, a professional in the field of (critical) discourse analysis, stating that governmental power is integrated in laws and social practices (2001, p.355). Through them, institutions shape a political power discourse whereby the adoption of discursive power reproductions is accepted because certain groups are dependent on institutional power (2001, p.363). How discourse is signified varies among academics, which is why this paper takes in the definition of how Macdonald defines it: 'a system of communicative practices that are integrally related to wider social and cultural practices and that help construct specific frameworks of thinking' (2003, p.10). Thus, discourse is shaped through language usage in social and cultural practices, and policies are used as a tool to exert this. This is connected to the viewpoint of Howarth, who states that 'the concept of discourse enables us to develop a relational account of social forms, such as the state, economy or governance networks' (2010, p.313). Power is transmitted through language, and therefore examination of the execution of language provides a better understanding of power dynamics (p.340). According to Maginn, one such examination looks at how language contributes to the framing, performing and defining of policy issues and how the transmission of these processes works as a mechanism for support gaining (2007, p.340). Therefore, in analysing the aforementioned policy document, this paper examines, interprets and exposes the discursive reproduction of power through language usage and exposes that it functions as a "support mechanism".

Stating that cybercrime poses a direct threat to national security, the Rijksoverheid uses language to construct meaning about this threat (2018, p.7, 9, 11). Cavelty contradicts the seriousness of this threat to national security and states that it is exaggerated:

> '…all we have seen in the last couple of years suggests that computer network vulnerabilities are an increasingly serious business problem, but that the threat that they represent to national security has been overstated: despite the persuasiveness of the threat scenarios, cyber-threats have clearly not materialised as a "real" national security threat' (2007, p.4).

She explains that many governments happen to regard the degree of the threat to national

security as ‘serious’ in order to implement countermeasures (p.6). Dorothy Elizabeth Denning, a well-known information –and cyber security researcher that won an award in the National Cyber Security Hall of Fame, explains that the threat is being exaggerated due to manipulation, but that it is undoubtedly there and ‘can neither be denied nor can it be ignored’ (Denning 2000, 2001a cited in Cavelty, 2007, p.5). Academics disagree extensively, questioning how serious the threat truly is compared to how it is depicted (p.4). Given these conflicting opinions, investigations into how cybercrime as a threat is positioned, how government policies depict this threat and how to best respond to it are of continuing concern within the field of politics and (cyber)security as well as within communication, information, media and cultural studies (p.6-7). After all, Cavelty states, ‘language is used to talk about cyberspace’ and ‘…it forms the basis for how security and insecurity in this realm are conceptualized’ (2013, p.106). Positioning this paper within this discussion, it acknowledges this gap and contributes to shrinking it by exposing how and why these depictions are made.

The Rijksoverheid constitutes these depictions of the cyber-realm by use of ‘framing’. Framing is closely related to discourse and is considered particularly relevant to political discourse, because it gives structure to how discourse is shaped in political texts, according to Gamson (1992, cited in van Dijk, 2001, p.360). Entman defines framing as: ‘select[ing] some aspects of a perceived reality and mak[ing] them more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation for the item described’ (1993, p.52). This serves as the definition used in this paper, which centralises framing as Cavelty does by upholding the statement that political actors use political language to frame situations or threats (2007, p.8). Since the Rijksoverheid makes use of framing as how Entman defines it, this paper acknowledges word and frame meanings as fluid processes constructed and interchangeable by society (p.7). This is related to how Hall refers to ‘connotations’ as specific meanings that are associated with words (2001, p.168). A particular way of framing that functions as an overarching strategy in this policy is called ‘threat framing’ (Cavelty, 2007, p.1). ‘Threat frames’ are defined by Cavelty as ‘specific interpretive schemata about what counts as threat or risk, how to respond to this threat, and who is responsible for dealing with it’ (2007, p.1). Because cybercrime is a threat and roles and responsibilities that regard cybersecurity are main subjects discussed in this policy, threat frames form the core of this paper. Cavelty explains that cyber threat frames not only expose how the threat itself is given meaning but

also how cybersecurity is validated and practically implemented (2007, p.1). Threat framing is used to evoke fear around the issue to counteract, as various academics state:

> 'Others even consider the debate to be almost entirely dominated by hidden agendas and "fear-mongering" and point to the fact that combating cyber-threats has not only become a highly politicised issue but also a lucrative one: an entire industry has emerged to grapple with the threat' (Smith 1998, 2000; see also Weimann 2004a, 2004b; Bendrath 2001 in Cavelty, 2007, p.5).

According to Voss and Freeman, discourse is crucial in analysing knowledge-making processes as governance (2016, p.7). They explain that meaning construction and 'ordering of knowledge' are forms of governance power (p.7-9). However, academics often seem to neglect this process of knowledge-making within research, which is why Voss and Freeman state there is a need for policies to be examined in this way (p.7-9). Attention should be shifted to how representational models 'of the government, the state, public policy, democracy, and governance more broadly acquire authority' (p.8-9). They address that it is necessary to uncover how knowledge is produced in governance practices, how knowledge production affects policy practices and how it creates a reality of governance (p.8-9). The Dutch government in this policy even emphasises that knowledge development and sharing is crucial (Rijksoverheid, 2018, p.7, 13). Therefore, it is of paramount importance that this gap is acknowledged. In line with that, this thesis contributes to filling the gap and adds to shared knowledge by analysing how the reality of governance is shaped by the Rijksoverheid in their 'National Cyber Security Agenda'. This is done by scrutinising how this process of knowledge-making is effectuated in their policy through meaning production.

Furthermore, policies make it possible to exercise power through regulation. Because the internet, together with its secondary problem of cybercrime, has developed increasingly in recent decades, there has been an emergence of 'cyberanarchy', as Weiser calls it (2001, p.823). According to Baird, because cyberanarchy has led to 'a worldwide crisis of governance', the question of what role the government takes within internet regulation and its security remains an infinite discussion (2002, p.15). Points of view differ, from Baird's declaration that governments would never be able to stay in charge or even informed about technological development (2002, p.15) to Weiser's embrace of the government as being indispensable for the regulation and development of the internet (2001, p.823). However,

Flew, Martin and Suzor state that, even if internet is regulated by the government, a hundred percent effectiveness is unreachable, whereas the idea that the internet is completely ungovernable is an illusion (2019, p.42). This paper positions itself within this discussion by exposing to what degree the Dutch government considers regulation in their policy document. It does so by analysing how the government regulates roles and responsibilities by allocating them to the parties involved.

The policy document 'National Cyber Security Agenda – a cyber secure Netherlands' was published in 2018 and therefore serves as a "new" and relatively uninvestigated document. Its analysis centralises the scope of these academic discussions and connects to strategies that require more examination within discourse analysis of policy documents. Aforementioned framing strategies are discussed in the methodology and show how the Rijksoverheid implements them to regulate how discourse about the Dutch cyber-realm is constructed.

Methodology

This section is dedicated to methodology of this thesis. It will first outline why the 'National Cyber Security Agenda' is chosen as a case, then an explanation why a political discourse analysis suits this case study will be provided, followed by a description about the process of the political discourse approach, its data collection and procedure. This will be explained in terms of aforementioned framing strategies that construct political discourse. When outlining these framing strategies, information will be provided about how language is connected to each strategy, how language is selected and which words are marked in the document. Executing qualitative research, language that appears to contribute to these framing strategies is marked in the document to cluster ideas.

Case

The 'National Cyber Security Agenda' is published by the Dutch government in 2018, establishing seven aims that are considered inevitable in manifesting a cyber-secure Netherlands in the fight against cybercrime. This document is chosen because it concerns developments in cybercrime and cybersecurity that are considered as top priorities by the Dutch government. This immediately highlights the societal relevance of this policy. Additionally, it concerns the state as well as public-private organisations, the business community and society itself, which centralises the subject within all national relations. Furthermore, this document is published in 2018, which makes it not only relatively new, undiscovered and relevant, but because it centralises aims for future development its process becomes even more interesting for future research. However, the focus of this research is not on the contributions that are listed or the legitimacy of these aims, but focuses on the construction of discourse and its manifestation in regulating the cyber-realm.

Method

The 'National Cyber Security Agenda' is scrutinised using a political discourse analysis, as provided by van Dijk (1997, 2001, p.360-361). Political discourse analysis is based on critical discourse analysis (CDA), also provided by van Dijk, that applies to political discourse (2001, p.352-371). This method is used to analyse the construction of discourse in an interpretive way. Since the research question of this paper is 'How do the Dutch government's political framing strategies in the "National Cyber Security Agenda" construct regulatory cybersecurity regimes, and therefore regulate how discourse about the cyber-realm in the

Netherlands is established in politics?' this method was chosen because its focus is on how powerful and dominant parties control discourse within politics (2001, p.355-356). Additionally, it emphasises the importance of context in political text, as van Dijk explains: 'In other words, to assess the political relevance of discourse analysis we need to examine in some more detail the *contextual functions* of various structures and strategies of text and talk' (1997, p.38). Systematically, van Dijk's political discourse centralises the domain of politics (societal domain, political systems, values, ideologies, institutions, organisations, groups, actors, relations, processes, actions, discourse and cognition) and connects it to political action and discourse structures (p.15-37). Therefore, using this method, political domains in this policy are uncovered to shape its context, whereafter their role within discourse construction is explained and a linkage between discourse structures and what political action they imply to accomplish is provided. The focus here is mainly on the discourse structures that are established. These are context-specific, as van Dijk states that 'The specifics of political discourse analysis therefore should be searched for in the relations between discourse structures and political context structures' (p.24). Because discourse analysis is adjusted to the text that's analysed and provides a detailed analysis, it is an in-depth way to interpret a text, but at the same time it is not generalisable to other political texts because of its narrowed context in which it is structured. Thus, its versatility and specificity are both a strength and a limitation. Another limitation is that these structures in political discourse are often 'future-oriented' (p.24). Van Dijk explains that 'Given the role of discourse in the political process, we may typically expect references to or threats about future developments, announcements or promises about future actions and so on' (p.24). In similarity, this policy concerns contributions to future development in cybersecurity and the development of cybercrime as a threat. Therefore, carrying out political discourse analysis provides expectations and implications about what discourse of future developments becomes, but former discourse structures therefore aren't considered relevant to reflect on these expectations. This makes political discourse analysis confined and subjected to insecurity.

Because of its interpretive nature, political discourse recognises framing strategies in discourse, which is why this thesis outlines several framing strategies from different academics that together structure the discourse of this policy. Analysing these structures is a crucial step in discourse analysis, because according to van Dijk, 'discourse structures may also satisfy criteria of effectiveness and persuasion' (p.25). To clarify, van Dijk states, '…they effectively emphasize or de-emphasize political attitudes and opinions, garner support, manipulate public opinion, manufacture political consent, or legitimate political

power' (p.25). Thus, since these purposes described by van Dijk are recognised in this policy and are manufactured by framing strategies, they function as discourse structures and are therefore brought to surface in this research. These discourse structures are recognised as regulated in this policy and regulation in general is expected within discourse analysis, as van Dijk describes that given the powerful nature of political actors, regulation and control are expected actions (p.26-27). Hence, this thesis lays emphasis on the regulative nature of this policy. By examining these discourse structures, van Dijk explains, the aim is to expose that '…these structures as such play a role in the political event and in the political process of which it is part' (p.38).

Data collection and procedure

Bringing this into practice, language use is categorised in a hermeneutic way into seven political framing strategies discussed below. In the 45-paged policy, only textual information is examined and images are excluded from the analysis. This is due to restriction of time and word count of the thesis. Carrying out an inductive approach, the document is first scrutinised in its broad sense by reading through the document to ascertain the domain of politics, as the involved parties, the topics the author(s) refer to, etcetera. These domains are written down to establish the structure of the document. Secondly, by reading through the document in a more detailed way, language that is recognised to be contributing to one or more of these framing strategies (given the meaning, connotation or context of it) is highlighted. In practice, for each framing technique a different colour is used to highlight language, creating coherence and overview in the text using different markers. By doing this, ideas are connected and clustered. The same is done to distinguish positive and negative connotations. Language that occurred frequently was underlined and written down accompanied by page numbers of where it occurs. This was only to recognise the emphasis that was laid on certain language – the count of it wasn't considered as relevant to this study because a qualitative instead of a quantitative approach is used. In other words, its count is not categorised, but its emphasis is. Structuring discourse, framing gives prominence to specific information while excluding other information, according to van Dijk (p.28). Marking language that appears to contribute to these framing strategies, the process of its discourse construction is brought to surface. By spitting through the document, findings with the same colour were linked and put into context, then interpreted based on its corresponding framing strategy. To provide specificity, a selection is made based on the emphasis that was laid on findings. Because 'meanings reflect political contexts', the context in which the words are used are as important as its

meaning (van Dijk, 1997, p.30). Findings that were emphasised the most and were repeated frequently were picked as examples in the analysis, but all other findings substantiate this general discourse structure. Because marking the text already separated the findings, and the framing strategies also directly function as categories to put these into place, coding was not necessary for the analysis.

Framing strategies

One way the Dutch government seems to use framing as a support-evoking tool is through a strategy called 'the inclusive technique', as described by Zheng (2000). Zheng explains that, in this strategy, politicians use inclusion to reach a large group of people (2000). What is characteristic of this group is that the people included are already connected to each other, for instance, by nationality (2000). This technique emphasises that the politicians themselves are part of this group in order to gain support from group members (2000). In this sense, a 'we-perspective' is embraced that harmonises the group and strengthens togetherness. Zheng writes that with this strategy 'politicians attempt to convince their audience that both themselves and their ideas are "of the people"' (2000). In this policy, words that are connected to inclusion such as 'our', 'we', 'Dutch', 'the Netherlands', 'mutual, 'share', 'joint', 'together', 'conjunction', 'partners', 'society as a whole', 'everyone', 'with each other' and 'collectively' were marked as a recognition of this strategy.

Interrelated to threat framing as a fear-evoking strategy is 'the fear technique', as described by Zheng (2000): 'This technique firstly produces some kind of potential threat to the public, and then provides solutions from which the public can then choose from'. Zheng explains that these solutions are established by the politicians themselves and the public is not really in a position of choice (2000). In this way, politicians reinforce control by determining political outcomes and therefore constructing discourse. This strategy is recognised through usage of fear-inducing words that contain negative connotations such as 'victim', 'target', 'attack', 'risk', 'threat' and 'vulnerabilities', but also words that seem to emphasise the degree of the threat or its negativity were marked, like 'direct', 'serious', 'increasing', 'crucial', 'urgent' and 'worrying'.

The fear technique uses 'prognostic framing' as a second step. Prognostic framing is defined by Cavelty as 'offering solutions and proposing specific strategies, tactics, and objectives by which these solutions may be achieved' (2007, p.30). After offering the solutions,

‘motivational framing’, as described by Cavelty, is used to encourage other parties to fulfil predetermined roles (p.30). These strategies are recognised through usage of words such as ‘cooperation’, ‘required’, ‘need’, ‘important’, ‘calling’, ‘effort’, and ‘encourage’, that contain positive connotations or refer to a call for action, and words that emphasise this, as ‘urgent’, ‘extremely’, ‘crucial’ and ‘close’.

‘Conditioning’ is another form of threat framing that may be used in conjunction with motivational framing. When objectives are being discussed, a condition is stated that emphasises the need for others to behave as the politician requires. By stating the condition, a certain situation is framed as a definite causality, which therefore can define meaning’ (Cavelty, 2007, p.30). Conditioning is recognised through usage of words such as ‘if’, ‘then’, ‘must’, ‘only’, ‘responsibility’ and ‘role’.

These techniques can be reinforced by ‘anaphora’, as described by Zheng (2000), and ‘referencing’, as defined by Townson (in Cavelty, 2007, p.27) to enhance the structuring of discourse. Anaphora entails the emphasis of certain words or phrases through frequent repetition (Zheng, 2000). As Zheng explains, through a repetitive act, impact can be enhanced or decreased, both in a positive and negative way (2000). Political discourse analysis focuses on this repetitive act, as van Dijk refers to meaning repetition as ‘semantic repetition’ (1997, p.35). Like anaphora, referencing also contains a positive and a negative way of framing. Cavelty describes positive referencing as constituting connections with words that contain positive connotations without being subjected to chance (p.27). However, negative referencing is pertinent to threat framing: ‘in the instance of threat frames, the connotations are negative, not positive, because the “grammar of security” stresses urgency and evokes an existential threat to security’ (p.27). Thus, referencing and anaphora use both positives and negatives to contribute to the establishment of certain frames that construct discourse. Therefore, the abovementioned words that were repeated frequently and/or contain clear positive or negative connotations were considered as most important. As stated before, a qualitative approach is used, so its emphasis is on the how language use is constructed and deployed, and the frequent repetition of words and phrases only emphasises the importance of its function in the text. Thus, the text is examined by connecting words and sentences that contain a relation, to expose how is talked about a subject and how meaning is constructed. This is manufactured by relationships like causalities, conditions, reasons, or contradictions.

In the analysis, the most important findings were put into context and interpreted in terms of the abovementioned strategies.

Analysis and interpretation

Solidarity and unification as a support mechanism

The inclusive technique

The inclusive technique can be seen in this policy where assimilation is emphasised by equalising state and society. Perspectives are described as 'we', 'the Netherlands', 'Dutch' and 'our', including all parties in the Netherlands. This contributes to the construction of a regulative discourse because, according to Zheng, political discourse is connected to national identity (2000). With the use of nationality in this sense, togetherness is emphasised. It is common in discourse construction that this distinction between 'our' and 'their' is made, whereby the 'in-group' is framed as 'positive' while the 'out-group' is represented as 'negative' (van Dijk, 1997, p.31). Van Dijk confirms this strategy in discourse construction by giving this example:

> 'Thus, the use of the political plural *we* (or possessive *our)* has many implications for the political position, alliances, solidarity, and other socio-political position of the speaker, depending on the relevant ingroup being constructed in the present context: *We* in the West, *we* the people, *we* American citizens, *we* Democrats, *we* in the government, or indeed *we* the President' (p.33-34).

In this policy, this 'in-group' is also emphasised by concretely formulating that fulfilling the predetermined objectives is something to be done together (Rijksoverheid, 2018, p.28, 32, 33, 35). The sense of togetherness is continuously emphasised by terms like 'our society', 'our economy' or 'our economic interests' and 'our national interests' (p.9, 11, 12, 20, 23). This implies that the issues are allocated to everyone in society and therefore are everyone's responsibility. Cybersecurity is also described as a 'shared interest' that requires parties to be 'mutually dependent' and 'share responsibility', when stated:

> 'Cybersecurity is the foundation for all successful entrepreneurship and administration and for confidence in the digital domain: this shared interest means that we are mutually dependent and share responsibility for national security' (p.5).

This not only implies inclusiveness, but also seems to emphasise the roles and responsibilities allocated to the involved parties. This is closely connected to the document's personification of 'the Netherlands'. In general, 'the Netherlands', as used in its finite verb, is not the country in its physical form – which is not capable of human practices – but everyone *in* the Netherlands. As Zheng explains, 'national identity serves as a means by which to target the widest possible section of supporters' (2000). This augments the range of who is responsible because the audience is being addressed as part of 'society as a whole', which implies that the Netherlands is property to every citizen and implies an increase of responsibility of involved parties (Rijksoverheid, 2018, p.27). This is fortified by the focus on building trust (p.19, 23). 'Trust' contains a positive connotation because it implies belief in mutual reliability. This is an example of positive referencing functioning to strengthen the inclusive technique, as Cavelty describes (2007, p.27). Van Dijk confirms that this use of positive as well as negative referencing is recognised in discourse analysis and used to strengthen this in –and exclusivity, as he states that '…politicians will tend to emphasize all meanings that are positive about themselves and their own group (nation, party, ideology, etc.) and negative about the Others…' (1997, p.32). Hence, emphasising inclusion might lead to an increase of patriotism and solidarity, and therefore might function as a support mechanism. This implies that the government regulates the involvement of society by shaping inclusion and the responsibility they carry to fulfil their duty to contribute to this safe cyber-environment.

Threat framing of the cyber-world and the cybersecurity solution

The fear technique

Referencing can also be used to aggravate negative depictions (Cavelty, 2007, p.27). The authors of 'National Cyber Security Agenda – a cyber secure Netherlands' make use of referencing in a negative way when they state:

> 'Criminals pursue their activities on a large scale via the Internet: one in nine people were victim of a cybercrime in 2017' (Rijksoverheid, 2018, p.35).

Because there is spoken of a 'victim', which contains a negative connotation and concerned one in nine people, it immediately emphasises the threat and its danger to (national) security. Using this in combination with the inclusive technique, it emphasises that it concerns everyone in the Netherlands. Terms such as 'target', 'vulnerabilities', 'attack', 'risk' and 'victim' are used frequently in explaining these threats and are examples of negative

referencing fortifying the fear technique (p.11, 12, 13, 14, 19, 20, 23, 27, 28, 29, 31, 32, 35, 36, 39). Furthermore, the threats are stamped as posing a 'direct' and 'serious' problem for (inter)national security, as in this statement:

> 'This forms a direct threat to our economic interests and national security' (p. 7, 9, 11, 23, 43).

Another such statement declares that:

> 'Cybersecurity is inextricably linked to national security: as a result of digitalisation, national security interests are vulnerable to digital attacks' (p.7).

As such words and sentences are shaped in a repetitive act, they become anaphora and form the core of what discourse becomes. In explaining political discourse analysis, van Dijk explains that this is one of the main strategies used in discourse construction, as he states:

> '[repetition]…one of the major strategies to draw attention to preferred meanings and to enhance construction of such meanings in mental models and their memorization in ongoing persuasion attempts or later recall' (Allen 1991; Cacioppo & Petty 1979; Frédéric 1985; Johnstone 1994, cited in van Dijk, 1997, p.35).

In this document, meaning is shaped by this repetitive act by describing dangers in cyberspace repeatedly as 'growing', 'increasing' and having a 'worrying increase' (Rijksoverheid, 2018, p.5, 7, 9, 11, 13, 19, 27, 29, 32, 35). This emphasises the seriousness of the threats and enhances the establishment of such 'mental models', as van Dijk calls them in the abovementioned citation. Statements such as '…vulnerabilities and threats in the digital domain are increasing' (p.7) and '…society has become vulnerable to disruptions from digital attacks' (p.13) therefore are not only shaped in a repetitive act, but are also examples of negative referencing.

In conclusion, this fear-inducement technique uses repetitive negativity to emphasise threats and the need for solutions. After shaping fear, the need to solve this threat then is emphasised by using the inclusive technique, prognostic and motivational framing and conditioning in combination with the fear technique, shaping a problem-solution structure. This implies that the government regulates the discourse of what cybercrime and security is and becomes. Threat framing constructs meaning in a way that's favourable for the government and

therefore the cyber-discourse is regulated by how cyber-threats are framed.

Prognostic and motivational framing

After shaping solidarity with the inclusive technique and emphasising the cyber-threat, the document clarifies that cooperation between all parties is the solution (2013, p.30). This falls into the prognostic framing technique and also adds to the fear technique. As Zheng defines the fear technique, offering politician-created solutions is the second step, after exposing the threat to the audience (2000). Cooperation is emphasised as the solution in this document by not only using the inclusive technique, but also through repetitive mentions (Rijksoverheid, 2018, p.5, 7, 8, 13, 17, 19, 20, 28, 32, 35, 40, 43, 44) and is defined as the foundation for cybersecurity: 'Public-private cooperation therefore forms the basis for the Dutch approach to cybersecurity' (p.5, 7). The policy also discusses how particular measures are only implementable with other market parties and that, in order to establish that, 'close cooperation in the development of the NCSA' is required (Rijksoverheid, 2018, p.7, 13, 17). This is both prognostic framing and a form of motivational framing, as described by Cavelty (2007, p.30), because it serves as a solution as well as a call to action. Additionally, as described in 'conditioning', it is deployed as a condition, as cooperation with and contributions of other parties are referred to as 'the only option'. Futhermore, earnestness with regards to this solution is emphasised, the same as is done in emphasising threats in the fear technique. For instance, the goal that '…the Netherlands [will have] adequate capabilities to detect, mitigate and respond decisively to cyber threats' (Rijksoverheid, 2018, p.5) is described as 'crucial'. Connected to that, the process of establishing these capabilities is described as something for which there is an 'urgent need' (p.19), as is the development of high-quality cybersecurity knowledge (p.39). It is stated that cooperation is a must to establish this 'effective integrated approach to cybersecurity' (p.5) that will lead to the Netherlands having adequate capabilities. Later in the document, this need is also emphasised in the sentence:

> 'Cooperation between public authorities and the business community, citizens and civil society organisations is extremely important in this respect' (p.35).

As the gravity of the situation and its corresponding objectives is emphasised, the urgency of cooperation is increased, as is the social pressure to support the goals of this NCSA.

The Rijksoverheid creates divisions of labour between the included parties to accomplish the proposed solution. These divisions are spoken of as being required (2018, p.13, 43), but here is where contradiction occurs. While pulling other parties closer to them by emphasising cooperation and inclusion, the Rijksoverheid also distances them by giving the parties their own responsibilities which they need to take account for. They shift from a we-perspective that emphasises sharing and conjunction to handing over responsibility to other parties to 'stimulate acceptance of own responsibilities' (p.13):

> 'This is to ensure that the business community and the citizens can shape their own digital security and resilience because, after all, they remain responsible for this themselves' (p.5).

The emphasis on individual responsibility occurs repeatedly in the policy (p.5, 7, 10, 13, 14, 27, 43, 44) and is another example of anaphora enhancing prognostic and motivational framing, but also intertwines the inclusive technique. The inclusive technique emphasises unity, whereby sharing responsibility is emphasised, while at the same time prognostic and motivational framing are shifting this responsibility to other parties. This implies that the government, by bringing these responsibilities to the surface, encourages others to take action. This expectation is foregrounded in the statement:

> 'All parties may and must be expected to accept their responsibilities…' (p.43).

Here an obligation is stated by the use of 'must'. This serves as a call for action and is also another referral to it being 'the only option'. Therefore, this is not only a form of motivational framing but is also a form of 'conditioning', as explained below. Additionally, the social pressure of this responsibility is emphasised by the statement that, due to this collectiveness, 'impact of public and private actions is enhanced' (p.7). This implies that the other groups depend on the actions of each party and therefore stresses urgency.
This implies that by the use of motivational and prognostic framing, the government regulates the roles the involved parties need to take in and requests them to obey to actions connected to these roles. Through determination of roles and responsibilities of all parties involved, the government tries to regulate positions within society in regulating the cyber-realm. Regulating this discourse structure may be used to 'garner support' (van Dijk, 1997, p.25).

Conditioning

In the 'National Cyber Security Agenda – a cyber secure Netherlands', the Rijksoverheid states:

> 'If all parties fulfil their responsibilities and have adequate capabilities and resources, then we can react decisively to digital threats' (Rijksoverheid, 2018, p.5).

This constitutes a condition. Closely related to this, it also states that in order to 'respond effectively to the growing digital threat, public and private parties must cooperate' (p.19). This implies that *only if* all parties cooperate to fulfil their tasks will the Netherlands be capable of reacting to cyber-threats. Anaphora appears in repeated statements saying that the goals are only possible in cooperation with other parties (7, 13, 14, 17), for instance, in the phrase, 'security in the digital domain can only be shaped in cooperation with…' (p.7, 13). Therefore, by the use of 'if', 'then', 'must' and 'only', conditions are stated and function to strengthen other framing strategies. Although this use of conditioning makes the Netherlands' options seem restricted, it is important to acknowledge that the presented option is a preference and not the only option. As Cavelty states: 'Awareness of the power of threat representation and the preferences that come with them can help to understand… that there are always different, and sometimes better options'. Establishing this threat frame through conditioning creates an ultimatum that serves as an 'instrument of social development and change' and exerts power at the same time (Cavelty, 2007, p.30). Thus, conditioning is used to frame proposed solutions as being a 'must' or 'the only option', whereby other framing strategies are reinforced.

Conclusion

In ‘National Cyber Security Agenda – a cyber secure Netherlands’, a ‘we-perspective’ is shaped by language use, which establishes an inclusive group of ‘the Netherlands’. By emphasising inclusiveness, the inclusive technique considers close cooperation and sharing of responsibility among group members as important. The technique includes the government and politicians within this group, to imply that all their statements are “of all group members”. In fact, the roles and responsibilities that are allocated to designated group members are predetermined by the government, which indicates that these are regulated. To increase the chance that group members obey and take up responsibilities and roles, threat framing aggravates the seriousness of cybercrime to emphasise the impact it could have on national security. The fear technique in particular frames the situation by exaggerating vulnerabilities and victimisation, which may induce fear. This is combined with the use of negative connotations, which emphasise the negativity of the threat. Frequently repeating the impact that cybercrime may have to national security, society as a whole and individuals within the Netherlands, it is emphasised that it is of paramount importance that members respond to this threat by answering to the given solutions. Prognostic and motivational framing shape these predetermined solutions as a reaction to the fear technique, whereby conditioning frames them if they are the only options to respond to cybercrime and enhance cybersecurity in the Netherlands. By laying emphasis on cooperation, roles and responsibilities as is done by the inclusive technique, and putting these in context of conditions and causalities, solutions are shaped as a call for action. By regulating roles and responsibilities involved parties need to take in, it gives rise to the implication that this policy document functions to regulate the cyber-realm. What is framed is emphasised by repetition in favour of the government. Therefore, the combination of these political strategies, its connotations and its emphasis construct how cybercrime and cybersecurity are depicted in the Netherlands and thus determines how the cyber-realm discourse is given meaning to in this policy document. As Hacker states, ‘Politics, after all, is largely constituted by language games’ (1996, p.33).

Discussion

This research brings new insight in the recognition of political framing strategies in policies and how these may function to make a depiction of the cyber-realm in this actual time, but

also how it is planning to be constructed in the future. This thesis connects multiple framing strategies to discourse in Dutch policy and shows that policies contain hidden strategies that governments use and combine to regulate meaning, but also to steer positions and roles in society. Furthermore, this thesis adds to debate in this field by showing that threats (to national security) might be exaggerated to shape meaning in favour of the government. This shows that governments do use policies as a 'tool' to regulate and that regulation can be exerted through power over discourse construction. Implementing policies in order to regulate discourse construction might function to gain support from society.

However, due to lack of time, this thesis had to be limited. Therefore, not all words and relations that were found could be analysed and discussed. Additionally, images in the policy weren't discussed. Researching depiction of cybercrime and cybersecurity in politics in future research, it might be valuable to combine qualitative analysis with quantitative analysis, analysing word occurrence to substantiate discourse analysis. Furthermore, an additional value might be added by analysing images in terms of threat framing combined with semiotics as described by Roland Barthes (1972). Barthes established the theory of semiotics as a method to analyse meaning construction and interpretation in images. Thus, this thesis might function as a foundation for a more detailed analysis of the document. It can function as an example to approach this or other policy document(s) through the lens of a political discourse approach, whereby focus may be shifted to other framing strategies or other discourse constructions that are recognised in the document. It also paves the way to research this policy in a more linguistic way, to dig deeper into the field of meaning construction. There are parts of political discourse analysis that focus more specifically on speech acts (van Dijk, p.36-37), which this thesis didn't focus on but might be a valuable contribution to the field of how politics shape meaning and use language in policies. Additionally, future qualitative research might give more insight in how readers experience discourse and meaning construction when reading the text. It might be valuable to research opinion influence or persuasion. This research shows what its premises imply, but other researches might focus on what the actual outcome or result is by researching how readers experience reading the policy. This might be based on questions like; do readers agree? Do they want to take action after reading the policy? What was their opinion towards the problem and solutions before reading it? And how are their opinions after reading the policy? Interacting with readers, interviews will provide more in-depth answers to what discourse construction effectuates.

Bibliography

Baird, Z. (2002). Governing the Internet: Engaging Government, Business, and Nonprofits. *Foreign Affairs, 81*(6), 15-20.

Braman, S. (1995). Horizons of the State: Information Policy and Power. *Journal of Communication*, *45*(4), 4-24.

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

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

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

Flew, T., Martin, F., & Suzor, N. (2019). Internet regulation as media policy: Rethinking the question of digital communication platform governance. *Journal of Digital Media & Policy*, *10*(1), 33-50.

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

Hacker, K. L. (1996). Political Linguistic Discourse Analysis. *The theory and practice of political communication research*, 28-55.

Howarth, D. (2010). Power, discourse, and policy: articulating a hegemony approach to critical policy studies. *Critical policy studies*, *3*(3-4), 309-335.

Macdonald, M. (2003). *Exploring media discourse*. London: Oxford University Press.

Maginn, P. J. (2007). Deliberative democracy or discursively biased? Perth's dialogue with the city initiative. *Space and Polity*, *11*(3), 331-352.

Rijksoverheid. (2018). *National Cyber Security Agenda - a cyber secure Netherlands*. Accessed on https://www.enisa.europa.eu/news/member-states/CSAgenda_EN.pdf

Van Dijk, T. A. (1997). What is political discourse analysis. *Belgian journal of linguistics*, *11*(1), 11-52.

Van Dijk, T. A. (2001). 18 Critical discourse analysis. *The handbook of discourse analysis*, 349-371.

Voss, J. P., & Freeman, R. (2016). Introduction: knowing governance. In *Knowing Governance* (pp. 1-33). London: Palgrave Macmillan.

Weiser, P. J. (2001). Internet Governance, Standard Setting, and Self-Regulation. *N. Ky. L. Rev.*, *28*, 822.

Wilson, J. (2003). 20 Political Discourse. *The handbook of discourse analysis*, *18*, 398.

Zheng, T. (2000). Characteristics of Australian Political Language Rhetoric: Tactics of gaining public support and shirking responsibility. *Journal of Intercultural Communication*, *4*. Accessed on http://mail.immi.se/intercultural/nr4/zheng.htm