Cyber Securitization and Security Policy

The Impact of the Discursive Construction of Computer Security on (National)Security Policymaking in the Netherlands.

By Max Edgar Floris Geelen

Leiden University
Department: Crisis and Security Management
Date: 25-01-2016
Supervisor: dhr. prof. dr. Edwin Bakker
Word Count: 25.618

Acknowledgements

I blame all of you. Writing this thesis has been an exercise in sustained suffering. The casual reader may, perhaps, exempt herself from excessive guilt, but for those of you who have played a larger role in prolonging my agonies with your encouragement and support, well… you know who you are and you owe me. – adapted from Dispensational Modernism by B. M. Pietsch.

Abstract

This thesis is devoted to testing the theoretical robustness of the cyber securitization framework developed by Lene Hansen and Helen Nissenbaum. Derived from Securitization Theory, this framework theorizes cyber security as a distinct sector with a particular constellation of threats and referent objects, which are articulated and linked through three distinct forms of securitizations: hyper-securitizations, everyday security practices, and technifications. As the applicability of this theoretical framework has hitherto only been demonstrated using a single, limited case, this thesis uses a less incident, more longitudinal approach to provide additional empirical data. This thesis uses discourse analysis to uncover the discursive construction of computer security in security policymaking in the Netherlands and compares this to the three grammatical modalities of this framework. This analysis has shown that throughout consecutive decades of Dutch computer security policymaking, a gradual degree of intersection with the cyber securitization framework exists.

Table of Contents

1 Introduction

Over the last few decades, the protection of the state and society against digital threats and risks (*"cybersecurity")* has become a high priority issue on the national security agenda of many nations. From the United States and Europe, to China and Russia, this has spurred a wide range of institutional, cybersecurity related developments such as the creation of highly sophisticated governmental cyber agencies and numerous measures like the drafting of national cybersecurity strategies and intensification of legislative efforts on 'cyber'-related issues. These developments have been largely triggered in recent years by sophisticated cyber-attacks combined with intensifying media attention. They are not only spawned by, but have also led to, an increasing tendency by nations to construct cyber issues as security problems rather than political, economic, criminal or purely technical issues. This has led to the effective *securitization* of the digital domain, as many digital matters are increasingly being brought within the purview of security.[1] This development is particularly evident in the realm of national security, where the linkage of security and cyberspace has almost become an uncontested truth with many budgetary and political consequences.[2]

Policies and the political significance of events depend heavily on the language through which they are politicized. By constructing an issue as being a matter of national security, it is immediately endowed with a status and priority that a non-security problem does not have. Moreover, the framing of issues in security terms also reinforces a particular manner in which these issues are viewed.[3] For example, security discourse that links labor migration to leaking borders and the loss of national identity tends to mobilize certain emergency measures and invests fear and unease in a policy issue.[4]

Although initially limited, the field of Security Studies has since seen much empirical research on cybersecurity. However, this research has often focused on sub-issues closely related to cybersecurity, such as cyber-war, network security, cyber-terrorism and critical

[1] Lene Hansen and Helen Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly* 53 (2009), 1155–1175; Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (London, 2008).
[2] Myriam Dunn Cavelty, 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', *International Studies Review* 15 (2013), 105–122.
[3] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1156.
[4] Jef Huysmans, *The Politics of Insecurity: Fear, Migration, and asylum in the EU* (London, 2006), 7.

infrastructure protection, rather the framing of cybersecurity, i.e. how it is interpreted within the communication of policy-makers, and thus attributed meaning. [5]

In recent years, however, several exceptions have emerged as a number of scholars have made endeavors to research how different actors within the field of politics discursively construct cyber threats, and how this affects not only their perception, but also the responses to them in the form of particular policies. Specifically, such scholars have tried to uncover how cybersecurity has become constituted as an important issue on the national security agenda, arguing a specific link between the cyber-dimension and national security.[6]

Of this research into framing, perhaps one of the most promising explanatory frameworks is the cyber securitization framework developed by Lene Hansen and Helen Nissenbaum. Explained in their seminal article "Digital Disaster, Cybersecurity, and the Copenhagen School", this framework, which is derived from Securitization Theory, represents one of the most articulate attempts to study the manner in which cyber issues are effectively framed as a "security problem" through the use of a specific manner of threat discourse which constitutes them as potentially threatening to the physical or ideational survival of one or more referent objects.[7]

Nevertheless, while this framework presents a notable step forward in the theorizing of cybersecurity, its authors provide very little supporting empirical evidence in support of their theory. Indeed, their cyber securitization framework is applied only to the Estonian "cyber war" incident of 2007 during which distributed denial of service attacks took the websites of the Estonian president, parliament, a series of government agencies, news media, and two of the country's largest banks offline. Consequently, while the cyber securitization framework provides compelling arguments, an obvious empirical limitation presents itself through the use of a single case. As such, more empirical data are required in order to adequately test the robustness of this theoretical framework.

---

[5] James Der Derian, *Antidiplomacy: Spies, Terror, Speed, and War* (Oxford, 1992); John Arquilla and David Ronfeldt, 'Cyberwar is Coming!', *Comparative Strategy* 12 (1993), 141–165; Ralph Bendrath, 'The American Cyber-Angst and the Real World – Any Link?' in Robert Latham (ed.), *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*(New York, 2003); John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, 2001).

[6] Ralf Bendrath, 'The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection', *Information & Security: An International Journal* 7 (2001), 80–103; Sean Lawson, 'Putting the "War" in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States', *First Monday* 17 (2012), [http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3848/3270 accessed December 15, 2015]; Johan Eriksson, 'Cyberplagues, IT, and Security: Threat Politics in the Information Age', *Journal of Contingencies and Crisis Management* 9 (2001), 211–222.

[7] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1156–1175.

This thesis aims to provide such empirical data by applying Hansen and Nissenbaum's cyber securitization framework to the discursive constitution of computer security in security policymaking in the Netherlands. Over the course of several decades, the Netherlands has developed a sophisticated and mature legal and policy framework for cybersecurity, which consists of a comprehensive national cybersecurity strategy, as well as highly specialized "cyber" institutions.[8] Its development is intrinsically connected to the emergence of computer security as a securitizing concept within the Netherlands, which has slowly but surely transformed into cybersecurity and has become an increasingly important issue on the national security agenda of the Netherlands. By charting how this discursive construction of computer security has influenced security policymaking, and by comparing this construction to the cyber securitization framework, this thesis aims to test the robustness of Hansen and Nissenbaum's theory. Moreover, through its longitudinal based approach, this thesis hopes to yield more detailed empirical data than Hansen and Nissenbaum's limited, incident based Estonian case. To this purpose, the following research question has been formulated:

> *How has computer security been discursively constructed within security policymaking in the Netherlands and to what extent does this correspond to the cyber securitization framework as developed Hansen and Nissenbaum?*

Given the cyber securitization framework's ontological underpinnings, which theorize the construction of cybersecurity as occurring through a particular securitizing discourse, a complementary methodological approach has been selected, namely discourse analysis.[9] Essentially a methodology which aims establish the meaning of texts shaped by distinct contexts, discourse analysis is a useful tool to map the emergence and evolution of patterns of threat representations which are constitutive of a threat image.[10]

For purposes of this thesis, this mapping will be conducted through an extensive analysis of the discursive construction of computer security within security policymaking in the Netherlands. The premise behind this approach is that this discursive construction, as presenting itself in a variety sources, including mainly, but not limited to, official statements, official policy documents, and political debates on the subject of computer security, represents the speech-act of state representatives proclaiming it to be an important issue of national security. This speech-act not only constructs the security of computers as a problem,

[8] Ministerie van Veiligheid en Justitie, Nationale Cyber Security Strategie (2014)
[9] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1156–1175.
[10] Thierry Balzacq, *Securitization Ttheory: how security problems emerge and dissolve* (New York, 2011), 39

but also simultaneously articulates particular policies to deal with the issue, effectively advancing cybersecurity as a policy field. Consequently, by analyzing this discourse, and mapping out what meaning computer security has had, and what meaning it has acquired in security policymaking in the Netherlands, an answer to the abovementioned research question can be formulated.

This thesis is divided into five chapters. The first chapter will begin with a detailed engagement with the Copenhagen School's securitization theory addressing its theoretical origins, main assumptions, and some of the criticism which has been leveled against it. This chapter will argue that while Securitization Theory has received notable criticism, its core theoretical premise which regards security as a concept that is essentially *socially* constructed presents a new and invaluable way of gaining insight into the dynamics of security politics. This chapter will also highlight one of the main conceptual pillars of Securitization Theory: sectors. This concept refers to a division within Securitization Theory of five different spheres of security in which distinct sub-forms or grammars of securitization tie referent objects, threats, and securitizing actors together. In addition, this chapter will also discuss some of the criticism which has been levelled against securitization theory.

The second chapter will discuss the main theoretical concepts of Hansen and Nissenbaum's cyber securitization framework. This framework, which defines and theorizes the cyber sector of security working from a discursive, Copenhagen School-inspired perspective, posits that within the cybersecurity sector, the sub-forms or grammars of securitization which tie referent objects, threats, and securitizing actors together, occur through the linkage of the referent object of "the network" and "the individual" to national security in a threefold manner: (1) hyper-securitizations (2) everyday security practices and (3) technifications.

The third chapter will specify the methodology of this thesis with regard to the specific research interest: the discursive construction of computer security within security policymaking in the Netherlands. For this purpose, the chapter conceptualizes the notion of discourse and discourse analysis in relation to Securitization Theory. It will explicate securitizations as a discursive practice, suggest a manner in which to operationalize this notion through a systematic historical description, and provide in-depth analysis of the discourse surrounding the emergence of cybersecurity as a policy field cross-referenced to the main theoretical concepts of the cyber securitization framework by Hansen and Nissenbaum.

The fourth chapter will constitute the main empirical chapter of this thesis. Using historical description and discourse analysis, this chapter will trace the discursive constitution

of computer security in Dutch security policymaking, ranging from the mid 1980s and early 1990s, when it first entered policymaking considerations through rapid technological advancements, to the late 1990s and early 2000s, when, in the advent of Y2K, it became an integral part of a larger policymaking process revolving around the protection of critical infrastructure, to the mid 2000s, when it was effectively transformed into *cyber security* through the adoption of a new *all-hazard approach* to national security policymaking and ending in the early/mid 2010s was it was imbued with a great sense of urgency in the wake of the DigiNotar incident. During each of this stages, this chapter will highlight to how the discursive constitution of computer security in security policymaking unfolded and to what extent did, and did not, correspond to the cybersecurity framework as developed by Lene Hansen and Helen Nissenbaum.

The fifth conclusive chapter provides a comparative perspective between the discursive construction of computer security in security policymaking in the Netherland and the cyber securitization framework as theorized by Hansen and Nissenbaum. It reconsiders the implication for its empirical value and proposes a pathway for further research.

2 Securitization Theory

In order to properly explain the basic tenants of the cyber securitization framework, it is first and foremost important to elucidate the source from which it is derived: Securitization Theory. Conceptualized as an attempt to offer a framework to analyze how certain issues become a security problem, securitization was developed by the Copenhagen School (CS) of Barry Buzan, Ole Wæver, Jaap de Wilde and others. Currently, it is still best developed in *Security: A New Framework for Analysis* (1998) which lays out a detailed and systematic overview of the main tenants of securitization. Defined as a "a successful speech-act 'through which an inter-subjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object, and to enable a call for urgent and exceptional measures to deal with the threat", securitization holds that security isn't an objective (or subjective) condition, but rather that security has particular discursive and political force of doing something: securitizing, or the presentation of an issue in security terms — in other words, as an existential threat.[11]

According to the CS, this framing of an issue in security terms is effected through the so-called "securitizing move", the process through which a valued referent object is moved into the domain of security by discursively constructing its existence as being threatened, thus in need of urgent protection.[12] This securitizing move depends, according to Buzan, Wæver and de Wilde, on a number of facilitating conditions in order to be successful. These facilitating conditions are (1) the demand internal to the speech-act of following the grammar of security (2) the social conditions regarding the position of authority for the securitizing actor — that is, the relationship between speaker and audience and thereby the likelihood of the audience accepting these claims made in a securitizing attempt and (3) features of the alleged threats that either facilitate or impede securitization.[13]

The specifics of a securitizing move differs between sectors of society, each of which is characterized by a specific ways in which distinct sub-forms or grammars of securitization tie referent objects, threats, and securitizing actors together.[14] These five sectors are (1) the political (2) the economic (3) the military (4) the societal and (5) the environmental; they serve as analytical devices to discern the various applications and dynamics of securitization. Each of these different sectors has a specific form of security logic, meaning that the

[11] Buzan, Wæver and de Wilde, *Security: A New Framework for Analysis*, 23.
[12] Buzan, Wæver and de Wilde, *Security: A New Framework for Analysis.* 23.
[13] Buzan, Wæver and de Wilde, *Security: A New Framework for Analysis*, 33.
[14] Buzan, Wæver and de Wilde, *Security: A New Framework for Analysis*, 27

securitizing actor has to apply a securitizing sub-form or grammar which is specific to the intended sector. Failing to do so would mean that the relevant audience will encounter difficulties understanding the attempted securitization correctly, constituting a failure of the speech-act. For example, in the military sector, the security grammar is mainly focused on the protection of the sovereignty and/or territorial integrity of states or would-be states. It is traditionally constructed around military force (the opposing army), geographical (distance and type of terrain), historical (past experiences on present perception) and political factors (contradicting ideologies, recognition and status). In the economic sector however, a different set of grammar or security logic exists, one which focuses on well-being of the sovereign economy. This grammar involves different actors, having a security logic constructed around 1) the individual involving basic human needs such as adequate food, water, education, clothing and shelter, or 2) the firm, involving risks of boycotts and risk of investment.[15]

According to Securitization Theory, what follows from such discursive construction, is that an issue is effectively framed either as a special kind of politics or as transcending politics altogether. This occurs along a spectrum which ranges public issues from the *non-politicized* ("the state does not deal with it and it is not in any other way made an issue of public debate and decision") through *politicized* ("the issue is part of public policy, requiring government decision resource allocations or, more rarely, some other form of communal governance") to *securitization* (in which case an issue is no longer debated as a political question, but dealt with at an accelerated pace and in ways that may violate normal legal and social rules).[16]

2.1 Debate and Criticism

While Securitization Theory has produced many new avenues of inquiry in the field of International Relations, debate has also arisen concerning a wide range of theoretical issues. In particular, such debates have revolved around the question as to the extent to which it adequate reflects real-world practices, resulting out of differences of opinion as to when and how issues become securitized within a specific political community and what specific conditions are required in order for a securitization to be successful.[17] Indeed, these specific conditions, although defined in Securitization Theory as consisting of existential threats,

[15] Buzan, Wæver and de Wilde, *Security: A New Framework for Analysis,* 27
[16] Buzan, Wæver and de Wilde, *Security: A New Framework for Analysis,* 23.
[17] Thierry Balzacq, *Securitization Ttheory: how security problems emerge and dissolve* (New York, 2011).

emergency action, and effects on inter-unit relations by breaking free of rules,[18] have since been questioned by a number of scholars within International Relations. In particular, this questioning has pertained to a number of grounds, ranging from the conceptualization of the audience within securitization, to a lack of a coherent model of failure of securitizations, to lack of conceptual clarity and consistent applications of Securitization Theory in empirical analysis.[19]

While such criticism raises valid points and undoubtedly underscores the need for additional research in order to further insights into the process of securitization, it is worth noting that much of this criticism essentially emanates from different philosophical-ontological commitments. This ontological difference lies at the core of the criticism leveled against the CS since it influences the perspectives on, and subsequently the evaluation of, Securitization Theory. This ontological difference has since been illustrated by Thierry Balzacq as constituting the difference between the so-called "philosophical" and the "sociological" view of securitization, with the latter seeking to move securitization towards a more empirical form of research by isolating and determining exact variables within a large number of cases of "real-world securitizations".[20] This sociological view approaches securitization from a neo-positivist perspective, claiming that securitization insufficiently adheres to what they refer to as real-world securitizations, meaning the measure to which the theory can adequately explain securitizations as they actually occur in political communities.

While such efforts essentially seek to move Securitization Theory towards a more empiricist direction, the "philosophical" approach of the CS adheres to a viewpoint altogether. Indeed, in contrast with the "sociological" view, it adheres more to the viewpoint that the theory is meant to provide new insight into the basic modality of complex security issues through the use of an ideal-typical analytical model. As such, much of the criticism leveled against the Copenhagen School does not speak to its account of a specific logic of security but instead focuses on:

> "(…) other aspects of the theory such as the lack of empirical and methodological detail, or that the Copenhagen School is focused on the 'speech-act'

[18] Buzan, Wæver and de Wilde, *Security: A New Framework for Analysis,* 23 - 33

[19] Holger Stritzel, 'Towards a Theory of Securitization: Copenhagen and Beyond', *European Journal of International Relations* 13 (2007) 357-383; Sarah Léonard and Christian Kaunert, "Reconceptualizing the Audience in Securitization Theory" in Balzacq (ed.), *Securitization Theory: How Security Problems Emerge and Dissolve* edited by Thierry Balzacq (New York, 2011), 57-76; Mark Salter, 'Securitization and Desecuritization: Dramaturgical Analysis and the Canadian Aviation Transport Security Authority', *Journal of International Relations and Development* 11 (2008), 321-349.

[20] Balzacq, *Securitization Ttheory,: how security problems emerge and dissolve.* 1 .

ignoring then the context of such acts, failing to specify how audiences, the specific local audience, sociological conditions and choice of policy tools affect the likely outcome and motivation of securitizing moves."[21]

By treating security not as an objective condition but rather as the outcome of a particular discursive modality through which security can be said to be socially constructed, the theoretical perspective of securitization represents a new approach within Security Studies. It presents a significantly different conception of security than other, more traditional accounts of security. Viewing security in such a manner opens the option to study a wide range of issues as security is not only limited to traditional military dominated subjects, but rather any issue can become securitized through the securitizing speech-act. As such it can be applied to a wide range of subjects from HIV/AIDS and SARS, to migration and societal security in Europe, water politics in the Middle East and, most relevantly, cybersecurity.[22] As such, it constitutes one of the most useful analytical frameworks with which to analyze how security problems emerge and dissolve.

2.2 Securitization Theory and Cyber Security

The abovementioned division into different sectors for analytical purposes has led to much debate within Securitization Theory. In particular, many of these discussions revolve around the question as to whether the list of sectors should be expanded; for example, by either differentiating separate sectors from existing ones or by adding new sectors.[23]

Although not originally theorized as one of the five distinct sectors of securitization, Hansen and Nissenbaum have extensively argued for the inclusion of cybersecurity as a distinct sector within securitization theory. Indeed, according to both authors, computer security has rapidly become associated with the development of an expanding policy field

[21] Olaf Corry, "Securitzation and 'Riskization': Two Grammars of Security", working paper prepared for Standing Group on International Relations, 7th Pan-European International Relations Conference, [http://www.eisa-net.org/be-bruga/eisa/files/events/stockholm/Risk%20society%20and%20securitization%20theory%20SGIR%20paper.pdf, accessed online 28 December 2015].

[22]Colin McInnes and Simon Rushton, HIV/AIDS and Securitization Theory, *European Journal of International Relations* 19 (2013), 115-138; Mely Caballero-Anthony, Combating Infectious Diseases in East Asia: Securitization nad Global Public Goods for Health and Human Security, *Journal of International Affairs* 59 (2006) 107 – 127; Jef Huysmans, T*he politics of insecurity: fear, migration, and asylum in the EU* (London: Routledge, 2006); Mark Zeitoun, *Power and Water in the Middle East: The Hidden Politics of the Palestinian-Israeli Water Conflict* (London: I.B. Tauris, 2008); Lene Hansen and Helen Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly* 53 (2009) 1155 – 1175.

[23] Carsten Bagge Laustsen and Ole Wæver, 'In Defence of Religion: Sacred Referent Objects for Securitization', *Journal of International Studies* 29 (2000), 705-739.

known as cybersecurity.[24] Originating from the field of computer and information sciences as ‘‘technical computer security”, a conception of computer security which referred mostly to the general security of computers, in which the majority of computer scientists adopted a technical discourse which focused on the development of systems and programs designed to reduce the possibility of external attacks, computer security has since developed over the last decades into a different conception which is rapidly entering the public sphere: cybersecurity. This conception, according to Hansen and Nissenbaum, is typically articulated by government authorities, corporate heads, and leaders of other non-governmental sectors and differentiates itself from the previous, more technical conception of computer security in that it links computer security to traditional notions of national security.[25]

By linking the security of computer networks to national security, many states have seen the emergence of a new securitizing discourse in which those concerned with digital security identify a wide variety of intricate cybersecurity issues. These issues range from digital espionage emanating from a foreign state to the use of hacking by terrorists, to cyber criminality and, especially, the protection of vital, digital infrastructure.[26]Throughout various policy documents and other sources, these states have increasingly articulated and developed a notion of computer security as cybersecurity, pointing to a potential magnitude of cyber threats and cyber disasters emanating through the reliance on computers for the functioning of a wide array of important public and private assets.[27] These threats range from the ability to ‘‘control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, and radars’’ to the “compromise systems and networks in ways that could render communications and electric power distribution difficult or impossible, disrupt transportation and shipping, disable financial transactions, and result in the theft of large amounts of money’’.[28] The networked infrastructure of computers is also often referenced in such threats, by stressing the implications of network break-downs for wide range of other referent objects, such as “society” or “the economy”. As a result, numerous referent objects are tied together, expanding the securitization potential of cybersecurity and increasing both political and media

[24] Hansen and Nissenbaum, ‘Digital Disaster, Cybersecurity, and the Copenhagen School’, 1155 – 1175.
[25] Helen Nissenbaum, ‘Where Computer Security Meets National Security’, *Ethics and Information Technology* 7 (2005), 63.
[26] In Hansen and Nissenbaum, Digital Disaster, Cybersecurity, and the Copenhagen School, this is illustrated using the case of the United States.
[27] See for example the numerous national cybersecurity strategies released by such countries as Germany, the Netherlands, Belgium etc.
[28] Computer Science and Telecommunications Board, *Cybersecurity Today and Tomorrow: Pay Now or Pay Later* (Washington, DC, 2002), 6.

attention.[29] As such, this conception, or "cybersecurity" can be interpreted as being "computer security" plus "securitization".[30]

As Hansen and Nissenbaum point out: "(…) securitization works in short by tying referent objects together, particularly by providing a link between those that do not explicitly invoke a bounded human collectively, such as 'network' or 'individual,' with those that do".[31] From this perspective, cybersecurity has indeed been successfully securitized, increasingly becoming a high priority issue on the national security agenda of many nations worldwide. Indeed, currently, a growing number of nations have adopted national cybersecurity policies and other cyber-related security practices, all of which constitute significant institutional developments in the field of cybersecurity.[32] As a result, this has created a dynamic in which digital issues are increasingly moved into the domain of national security.[33]

[29] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1163
[30] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1160.
[31] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1163.
[32] Organization for Economic Co-operation and Development, *Cybersecurity policy making at a turning point* (2012), [http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf accessed online 22 December 2015].
[33] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1155 – 1175; Cavelty, 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', 105–122.

3 The Cyber Security Framework

Derived from securitization theory, the cyber security framework developed by Hansen and Nissenbaum employs securitization, and applies it to this conception of cybersecurity by theorizing it as a distinct sector in securitization theory, with particular constellation of threats and referent objects. As such, it seeks to uncover the manner in which cyber issues are effectively framed as a "security problem" through the use of a specific manner of threat discourse which constitutes them as potentially threatening to the physical or ideational survival of one or more referent objects.[34]

According to Hansen and Nissenbaum, the security logic or grammar which ties referent objects, threats, and securitizing actors together in the cybersecurity sector consist of three elements, or as they refer to them, security modalities: (1) hyper-securitizations (2) everyday security practices and (3) technifications. The premise behind these security modalities is that they contain certain acuteness and, more crucially, a specific interplay which is distinct to the cyber sector. As such, Hansen and Nissenbaum essentially seek to uncover the specific narrative which underlies securitizations in this sector, by creating a theoretical framework that facilitates an understanding of the connections between these discourses as well as of the political and normative implications of constructing cyber issues as security problems rather than as political, economic, criminal, or purely technical ones.[35] The following section will outline each of the three specific security modalities.

3.1 Hyper-securitizations

The first security modality in the sector of cybersecurity identified by Hansen and Nissenbaum is hyper-securitizations. Originally introduced by Barry Buzan, the concept of hyper-securitization was used to indicate an intensification or move of securitization beyond a 'normal' level of threat and danger, or, as Buzan describes it: "a tendency to both to exaggerate threats and to resort to excessive counter-measures".[36] This tendency potentially has quite adverse effects, in that it can lead to the establishment of a systemic securitization environment, akin to what Jef Huysman's refers to as "political communities of insecurity". These political communities are characterized by a peculiar process in which their quest to secure unity and identity are essentially underlined by a continuous institutionalization of

[34] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1156.
[35] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1157.
[36] Barry Buzan. *The United States and the Great Powers: World Politics in the Twenty-First Century* (Cambridge, 2004), 172.

existential insecurity.[37] As such, hyper-securitizations have potentially far-reaching effects as they can produce a recurring cycle of securitization in which a political community continually reconstructs its insecurity and increasingly institutes measures that are perceived to decrease it.

While Buzan's definition of hyper-securitizations has been widely employed within securitization literature, it has also been criticized, most notably by Hansen and Nissenbaum themselves. This criticism is based on two important issues, namely (1) the "objectivist ring" to Buzan's definition, or as Hansen and Nissenbaum put it: "to identify 'exaggerated' threats implies that there are 'real' threats that are not exaggerated" and (2) the fact that the question of whether a securitization is seen as "exaggerating" concerns the degree to which it is successful (as unsuccessful securitizations are seen as "exaggerating") which is not part of the grammatical specificities of sectors. Instead, Hansen and Nissenbaum, for the purposes of their cyber securitization framework, proposed a small change definition to Buzan's definition of hyper-securitization (one in which ''exaggerated'' is not included). This definition was applied to the cyber sector in order to identify "the striking manner in which cybersecurity discourse hinges on multi-dimensional cyber disaster scenarios that pack a long list of severe threats into a monumental cascading sequence and the fact that neither of these scenarios has so far taken place".[38]

According to Hansen and Nissenbaum, hyper-securitizations in cybersecurity discourse are identifiable by the several distinguishing features. In particular, hyper-securitizations distinguish themselves from regular securitizations by their instantaneity and inter-locking effects. These two features endow hyper-securitizations in the cybersecurity sector with a uniquely high degree of power as they contain the ability to tie in referent objects from a wide range of sectors (societal, financial, military etc.) by linking them through an almost domino-like sequence to the consequences of a damaged network.[39] This enables the securitizing agent to link what are essentially abstract referent objects such as "the network", to defined ones, such as "infrastructure" and "society" by stressing their reliance on the network for their proper functioning or security.

Another notable distinguishing feature of Hansen and Nissenbaum hyper-securitization in cybersecurity discourse involves the hypothetical nature of cyber incidents. Indeed, instead of citing actual precedents, securitizing actors emphasize the urgency to take extraordinary

[37] Huysmans, *The Politics of Insecurity*, 47.
[38] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1164.
[39] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1164.

measures in order to protect the referent object by invoking images of historical catastrophes.[40] Notable examples include such statements as those made by U.S. Secretary of Defense Leon Panetta who likened the potential devastation of a serious cyber-attack both to Pearl Harbor and to 9/11, stating that "a cyber-attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11. Such a destructive cyber terrorist attack could paralyze the nation".[41] The invocation of such images of historical disasters effectively establishes the vulnerability of the referent object, making a strong case for extraordinary measures to be urgently taken in order to counter the existential threat. Moreover, as Hansen and Nissenbaum explain: "The extreme reliance on the future and the enormity of the threats claimed at stake makes the discourse susceptible to charges of ''exaggeration,'' yet the scale of the potential catastrophe simultaneously raises the stakes attached to ignoring the warnings".[42]

3.2 Everyday Security Practices

The second grammatical modality of cyber securitization discourse revolves around the manner in which a wide range of securitizing actors are able to mobilize the experiences of normal individuals. This is referred to by Hansen and Nissenbaum as "everyday security practices", and operates in a two-fold manner: firstly, it secures the individual's partnership and compliance in protecting network security; secondly, it makes hyper-securitization scenarios more plausible by linking elements of the disaster scenario to experiences familiar from everyday life.[43] Within Securitization Theory, this grammatical modality can be directly linked to the concept of the audience, defined by Buzan as "those the securitizing act attempts to convince'' as it facilitates the success of the securitization by making the consequences of cybersecurity breaches more relatable.[44] Indeed, as Thierry Balzacq theorized: "the success of securitization is highly contingent upon the securitizing actor's ability to identify with the audience's feelings, needs, and interests". Thus, in order to ensure a greater measure of success, the securitizing actor has to tune their language to the audience's experience.[45] According to Hansen and Nissenbaum, this is precisely what everyday security practices do;

[40] Ralph Bendrath, 'The American Cyber-Angst and the Real World – Any Link?', 50
[41] Leon Panetta, 'Cybersecurity', speech given on 12 October at the Intrepid Sea, Air and Space Museum (New York, 2012).
[42] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1164.
[43] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1165.
[44] Buzan, Wæver and de Wilde, *Security: A New Framework for Analysis*, 41.
[45] Thierry Balzacq, 'The Three Faces of Securitization: Political Agency, Audience and Context', *European Journal of International Relations* 11 (2005), 182.

they facilitate the acceptance of public security discourses by generating a resonance with an audience's lived, concrete experiences'.[46]

According to Hansen and Nissenbaum, while elements of such everyday security practices may be evident in other sectors as well, they particularly excel in the case of cybersecurity. Indeed, as they point out: "(…) there is for example a marked difference between Cold War military securitizations of nuclear Holocaust which implied the obliteration of everyday life, and the securitizations of everyday digital life with its dangers of credit card fraud, identity theft, and email scamming". Key here is the reach of such everyday security practices in cybersecurity, as "those few who do not own or have computers at work are nevertheless subjected to the consequences of digitization". As such, these everyday security practices do not reinstall a de-collectivized concept of "individual security" or "crime", but rather constructs various threats as being threats towards the entire network, thus, to a larger extent, to society.[47]

Another distinguishing feature of everyday security practices in cyber securitization is their simultaneous constitution of the individual not only as a responsible partner in fighting insecurity, but also as a liability or even a threat. This introduces a particular dynamic within the cybersecurity sector, in which both private and public actors mobilize expert positions and rhetoric in order to convince a specific targeted audience that they should be concerned with cybersecurity. The result is often a discourse which is both educational and securitizing, as exemplified by the Stop.Think.Connect Campaign by the U.S. Department of Homeland Security, a national public awareness campaign aimed at increasing the understanding of cyber threats stated: "Cybersecurity is a shared responsibility. We each have to do our part to keep the Internet safe. When we all take simple steps to be safer online, it makes using the Internet a more secure experience for everyone".[48] The Cyberstreetwise awareness campaign launched by the United Kingdom's Home Office, a campaign that employs a positive message method in order to influence the online behavior of users, featured a similar discourse, stressing that: "the weakest links in the cybersecurity chain are you and me''.[49] Such

[46] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1165.
[47] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1165.
[48] Department of Homeland Security, *National Public Awareness Campaign Stop.Think.Connect* (2015), [http://www.dhs.gov/stopthinkconnect accessed 29 December 2015].
[49] Maria Bada and Angela Sasse, 'Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?' *Global Cyber Security Centre* (2014), [https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Awareness%20CampaignsDraftWorkingPaper.pdf accessed 23 December 2015].

discourse, according to Hansen and Nissenbaum, facilitates the move of cybersecurity into the modality of national/societal security.[50]

3.3 Technifications

The third grammatical modality in the cybersecurity sector is technifications and concerns the role of technical, expert discourse within cyber securitization. As Hansen and Nissenbaum point out, due to the required knowledge to master the field of computer science and the fact that this knowledge is often not available to the broader public, the field of cybersecurity leans heavily on the specialized knowledge of cybersecurity experts. Sophisticated computer threats are given significance through a wide range of experts which are consulted whenever issues of cybersecurity are discussed. This grants such experts a unique position in which they are able to speak in an authoritative manner to the public about matters of cybersecurity and to give significance to them.[51] As such, such cybersecurity experts no longer fulfill the invisible role behind scenes traditionally occupied by experts in other sectors. Instead, they become securitizing actors themselves by transcending their specific scientific locations to speak to the broader public in a move that is both facilitated by and works to support cyber securitizations claimed by politicians and the media.[52]

The privileged role that experts play in cyber securitization discourse has important consequences. Indeed, as Hansen and Nissenbaum point out, cybersecurity experts are not only merely experts, but *technical* ones who technify cybersecurity by constituting it as being their domain. This technification fulfills a similar role as the speech act in securitization in that they are not merely descriptive, but that they "do something". They construct an issue as reliant upon certain technical expertise for its resolution and hence as politically neutral or unquestionably normatively desirable.[53] As such, the mobilization of technifications is strongly related to what Huysmans refers to as the concept of 'security experts'; professionals who gain their legitimacy of and power over defining policy problems from trained skills and knowledge and from continuously using these in their work. These security experts play an extremely important role in modulating social and political practice in both the public and private domain.[54]

[50] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1165.
[51] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1165.
[52] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1165.
[53] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1157.
[54] Huysmans, *The Politics of Insecurity: Fear, Migration, and Asylum in the EU*, 9.

The construction of the sector of cybersecurity as a domain requiring an expertise that is not readily possessed by the public and politicians, not only allows cybersecurity experts to become securitizing actors, but also to differentiate themselves from politicians and other political actors. The result is a specific discourse in cybersecurity which is unique to the cybersecurity sector in that it provides less direct points of engagement for those wishing to challenge it, as securitizing actors are able to depoliticize their discourses' enemy and threaten constructions by using their technical expertise to make linkages to politically and normatively neutral agenda. In sum, technifications play a crucial role in legitimating cyber securitizations, not only on their own, but also in supporting hyper-securitizations and in speaking with authority to the public about the significance of its everyday practices. [55]

[55] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1167.

4 Methodology

Securitization Theory typically describes the discursive process of construction of an existential threat as an act of successfully attaching "security" to a particular object, case or development, and focuses on the manner in which different conceptualizations of security mobilized within policy discourse.[56] This construction essentially involves a speech-act positing a security threat as being existential for the survival of a particular referent object which, while traditionally consists of the state, can include a wide range of referent objects, including identity or culture, the environment and even the financial system.[57]

This premise of Securitization Theory means that in order to measure the extent to which the three grammatical modalities of Hansen and Nissenbaum can be said to be present within the constitution of computer security as a security issue in the Netherlands, a technique needs to be adopted which is tailored to the task of uncovering the structures and practices that produced the threat image whose source, mechanisms, and effects need to be explicated. Towards this purpose, this thesis will employ a method which has been widely and successfully applied in Securitization Theory research, namely discourse analysis.

4.1 Discourse and Discourse Analysis

While widely employed by scholars in numerous academic fields, the concept of "discourse" and its subsequent analysis have been subject to much debate. In particular, much discussion has focused on the difficulties surrounding the crafting of a generic definition the concept of "discourse", leading to different opinions as to what it constitutes and how it should be analyzed.[58] As such, it is important to clarify what is understood as "discourse" within this study, and also how it will be subsequently analyzed. While the following section will briefly mention different conceptualizations, its main focus will be on how discourse and discourse analysis is conceptualized within securitization literature. This choice has been made due to the fact that a conceptual and methodological debate on different conceptualizations of discourse and discourse analysis would constitute an endeavor which falls outside the scope of this study, particularly due to the fact that these terms have different meanings to scholars in different fields. Indeed, as Balzacq points out, the term "discourse" is

[56] Buzan, Wæver and de Wilde, *Security: A New Framework for Analysis*, 29; Huysmans, *The Politics of Insecurity*, 124–144.
[57] Buzan, Wæver and de Wilde, *Security: A New Framework for Analysis*, 7; Columba Peoples and Nick Vaughan-Williams, *Critical Security Studies: An Introduction* (London, 2010), 80.
[58] For an example of such numerous ways in which both terms are interpreted, see: Teun van Dijk, *Discourse as Structure and Process* (Thousand Oaks, 1997).

widely contested, meaning different things to different people.[59] Thus, as a matter of practicality, a discussion of such different conceptualizations will not be part of this study, and a choice has been made to limit this study to how discourse and discourse analysis are conceptualized within the relevant field of Securitization Theory.

4.2 Discourse in Securitization Theory

The concept of discourse features prominently within the framework of Securitization Theory. Within the theory, security is conceptualized as being not merely an objective (or subjective) condition, but rather as the outcome of a particular discursive modality with a specific rhetorical structure through which security can be said to be socially constructed. This conceptualization of security, and the corresponding idea of securitization, draws heavily on what is known as the theory of language, in particular the branch known as speech-act theory; a theory which focuses on the manner in which speech acts (or utterances) have performative functions. Within Securitization Theory, the securitizing speech act is conceptualized as having such a perfomative function, meaning that its utterance serves to accomplish a social act.[60] Indeed, as Wæver himself stated "by saying it [security] something is done (as in betting, giving a promise, naming a ship). By uttering 'security', a state-representative moves a particular development into a specific area, and thereby claims a special right to use whatever means necessary to block it".[61]

The concept of language as having performative functions forms the foundation of Securitization Theory's conceptualization of discourse in which language is interpreted as being constitutive for what is being brought into being. This conceptualization of discursive dynamics as a process of creation, contestation, and change of meaning is often referred to as the "politics of meaning". It emphasizes that language is ontologically significant through construction in language "things" such as objects, subjects, and material structures, which are given meaning and/or are endowed with a particular identity.[62] The uttering of "security" can be viewed as such a speech-act by which a wide range of issues (military, political, economic, and environmental) can become staged as a threat. Securitization Theory thus has a very broad conceptualization of discourse as being the use of language, which is used to construct an issue as a matter of security through a specific rhetorical structure namely: (1) the claim

[59] Thierry Balzacq, *Securitization Theory: How Security Problems Emerge and Dissolve* (New York, 2011), 39.
[60] Peoples and Vaughan-Williams, *Critical Security Studies*, 95
[61] Ole Wæver, 'Securitization and Desecuritization', in Ronnie Lipschutz (ed.), *On Security* (New York, 1995), 55.
[62] Lene Hansen, *Security as Practice Discourse Analysis and the Bosnian War* (Oxford, 2006), 17.

that a referent object is existentially threatened (2) demanding the right to take extraordinary countermeasures to deal with that the threat and (3) convincing an audience that rule-breaking behavior to counter the threat is justified.[63]

Nevertheless, while Securitization Theory has traditionally interpreted the process of securitization as being performed through the use of language, several criticisms have been aimed at the narrow manner in which such an understanding of discourse is conceptualized. In recent years, a wide range of authors have argued for the need to take account of the role of other sources of securitization, such as images or forms of bureaucratic practices that are not merely the results of securitizing speech-acts, but part of the process through which meanings of security are communicated and constructed.[64] Consequently, such authors have opted for a broader conceptualization of discourse which takes in account the role of other potential sources of securitization. Indeed, as some have pointed out, while the most conventional manners in which discourse materializes is through text, this does not merely refer to written text, but to a notion of text which refers to a wide variety of signs, including written and spoken utterances, symbols, pictures, and music.[65]

4.3 Discourse Analysis in Securitization Theory

Discourse analysis refers to a range of different approaches in several disciplines and theoretical traditions. Each of these approaches potentially differs, either through the sources on which they rely, or even to the problems and research questions they seek to investigate.[66] However, for the purposes of this thesis, the choice has been made not to extensively delve into the broader discussion on the different approaches to discourse analysis, but rather to focus on how it is employed in Securitization Theory.

Within the literature of securitization, the concept of discourse analysis has been widely and successfully employed by scholars to analyze and map out the emergence and evolution of patterns of representations which are constitutive of a threat image.[67] As explained earlier, Securitization Theory aims to capture a distinct social phenomenon of how some public problems become security issues. This premise means that the technique adopted

[63] Buzan, Wæver and de Wilde, *Security: A New Framework for Analysis*, 36–39.
[64] Michael C. Williams, 'Words, Images, Enemies: Securitization and International Politics', *International Studies Quarterly* 47 (2003), 511- 532; Lene Hansen, 'Theorizing the image for Security Studies: Visual securitization and the Muhammad Cartoon Crisis', *European Journal of International Relations* 17 (2011), 51-74.
[65] Balzacq, *Securitization Theory*, 39.
[66] For extended discussions on discourse analysis, see Phillips and Hardy, *Discourse Analysis* (Thousand Oaks, 2002).
[67] Balzacq, *Securitization Theory*, 39.

to research this social phenomenon needs to be tailored to the task of uncovering the structures and practices that produced the threat image whose source, mechanisms, and effects need to be explicated.[68] Discourse analysis is one of these techniques as, in its most basic form, it is an attempt at answering the question of where meaning comes from, which is conducted by studying discourse and the social reality that it constitutes.[69] In its simple form, this entails a process of analyzing various sources of discourse, such as interviews, archival materials, newspaper coverage, and pictures to uncover social and institutional practices associated with the construction and evolution of various threat images.[70]

Discourse analysis is thus interested in ascertaining the constructive effects of discourse through the structured systematic study of texts—including their production, dissemination, and consumption— in order to explore the relationship between discourse and social reality.[71] These discourses are shared and social, emanating out of interactions between complex societal structures in which the discourse is embedded. For example, policy discourses not only construct problems, objects, and subjects, they also simultaneously articulate policies to address them.[72] Indeed, as Philips and Brown point out:

> "(…) texts are not meaningful individually; it is only through their interconnection with other texts, the different discourses on which they draw, and the nature of their production, dissemination, and consumption that they are made meaningful. Discourse analysis explores how texts are *made* meaningful through these processes and also how they contribute to the constitution of social reality by *making* meaning."[73]

4.4 Operationalization

This thesis aims to test the empirical robustness of the cyber securitization framework by mapping out how computer security has discursively been constituted within security policymaking in the Netherlands. Towards this purpose, the interrelated concepts of discourse

---

[68] Balzacq, *Securitization Theory*, 39.
[69] Royston Greenwood, Christine Oliver, Roy Suddaby, and Kerstin Sahlin-Andersson, *The Sage Handbook of Organizational Institutionalism* (Thousand Oaks, 2008), 712.
[70] Balzacq, *Securitization Theory*, 41.
[71] Nelson Phillips, Thomas Lawrence and Cynthia Hardy, 'Discourse and Institutions', *Academy of Management Review* 29 (2004), 635– 652.
[72] Michael Shapiro, *The Politics of Representation: Writing Practices in Biography, Photography, and Policy* Analysis (Madison,1988); Hansen, *Security as Practice Discourse Analysis and the Bosnian War*, 21.
[73] Nelson Phillips and John L. Brown, 'Analyzing Communication in and around Organizations – A Critical Hermeneutic Approach', *Academy of Management Journal* 36 (1993), 1547-1576 as cited in Phillips & Hardy, *Discourse Analysis*, 4.

and discourse analysis will need to be properly operationalized. Pertaining to discourse, this thesis will employ a conceptualization which corresponds to the poststructuralist understanding of discourse as an interrelated set of texts, whose practices of production, dissemination, and reception, bring an object into being.[74] The reason for this choice is that this particular conceptualization not only adheres to the general conception of discourse within securitization literature, which focuses on how particular issues are effectively securitized through particular discursive practices, but also to the conception of discourse as understood by Hansen and Nissenbaum in their cyber securitization framework in the form of the three grammatical modalities (hyper securitizations, everyday security practices and technifications). Indeed, these grammatical modalities represent a particular discourse which operates according to the poststructuralist logic, in that they effectively construct an issue as being a ‘‘security problem’’ by articulating referent objects as being threatened.[75] Thus, by matching the understanding of discourse within this framework, the chosen conceptualization of discourse is thus best suited towards the abovementioned goal of this thesis.

Having elucidated the conceptualization of discourse which will be employed in this thesis, the method which ascertains its constructive effects will also be highlighted. In order to study how computer security has been discursively constructed within security policymaking in the Netherlands and to what extent this corresponded to the cyber securitization framework, a structured and systematic study of relevant text must be conducted in order to explore the relationship between these two questions. Towards this purpose, this thesis will conduct an extensive analysis of computer security discourse in the Netherlands, which will map out what particular meaning computer security has had in the past, and what meaning it has acquired throughout several decades of Dutch security policymaking. This analysis will start from when computer security first entered policymaking considerations, to when it became an integral part of a larger policymaking process revolving around the protection of critical infrastructure, ending with when it was effectively transformed into *cyber security* and was imbued with a great sense of urgency in the wake of the DigiNotar incident. During each of this stages, the analysis will highlight to how the discursive constitution of computer security in security policymaking unfolded and to what extent did, and did not, correspond to the cybersecurity framework as developed by Lene Hansen and Helen Nissenbaum.

[74] Ian Parker, *Discourse Dynamics: Critical Analysis For Social and Individual Psychology* (London, 1992) as quoted in Nelson Phillips and Cynthia Hardy, *Discourse Analysis: Investigating Processes of Social Construction* (Thousand Oaks, 2002), 3.
[75] Hansen and Nissenbaum, ‘Digital Disaster, Cybersecurity, and the Copenhagen School’, 1163 – 1168..

With discourse analysis, the research question commands the kind of data collected and the hierarchy established among them.[76] Since the research question of this thesis relates to the discourse employed in the establishment of cybersecurity as a policy field, a field in which the Dutch government is the largest actor, the primary source of data will consist of material published by the Dutch government. This data includes policy documents, transcripts of political debates, as well as other parliamentary sources, along with newspaper interviews and other related source materials. These policy documents pertain to the national cybersecurity strategy as well as other political documents related to cybersecurity such as reports of parliamentary debates/inquiries or otherwise related to the Dutch House of Representatives. They represent the speech-act of state representatives proclaiming cybersecurity to be an important issue of national security. This speech-act not only constructs the security of computer networks as a problem, but also simultaneously articulates particular policies to deal with the issue, advancing cybersecurity as a policy field.

Within this approach, the goal is not to render a value based judgment on the views presented within the analyzed discourse, but rather to construct a better view about how the development of the concept under discourse has historically unfolded. Lastly, while it has been noted above that discourse can be interpreted in a variety of manners, ranging from body language, to states undertaking military exercises or even material objects, for practical purposes, the analysis in this thesis will limit itself to the primarily written or spoken language. As Hansen points out political collectives such as states are traditionally very verbal entities which communicate widely both domestically and internationally.[77] Consequently, a focus on written material is deemed adequate to cover the scope of the research question.

[76] Balzacq, *Securitization Theory*, 41.
[77] Hansen, *Security as Practice Discourse Analysis and the Bosnian War*, 23.

5 The Netherlands and Cybersecurity

The Netherlands currently has a sophisticated and mature legal and policy framework for cybersecurity which consists, amongst other things, of a National Cybersecurity Strategy, a National Cybersecurity Assessment and specialized institutions such as the National Cybersecurity Center.[78] This framework, however, did not appear overnight. Its development is intrinsically connected to the emergence of computer security as a securitizing concept and can be traced back several decades, to when computer crime/security as it was initially called, slowly but surely became an increasingly important issue on the security agenda.

The following chapter will provide a historical and chronological account of the discursive constitution of computer security in security policymaking in the Netherlands. By charting this discursive construction, this chapter serves to not only to address the criticism often leveled against Securitization Theory concerning its lack of proper historical context, but also as a background against which the empirical value of the cyber securitization framework can be evaluated.

5.1 The Emergence of Computer Security as a Securitizing Concept in the Netherlands

In the Netherlands, the history of cybersecurity as a securitizing concept can be traced back to the mid-1980s when the security of communication and information technology became a politically salient issue. The expeditious development of computer technology, in particular the personal computer, during the 1980s led to an increasing influence of computers in Dutch society. Increasingly, many private and public organizations relied on computers to perform a wide array of tasks, including administrative processes, process controls, and analyses of complex issues. Such organizations would also facilitate the dispersal of computer amongst private citizens through "PC-private-projects", where a large number of computers would be acquired and subsequently issued to staff. For example, in November 1987, the ABN Bank (later known as ABN AMRO), one of the largest banks in the Netherlands, distributed more than 5,000 computers among its employees. In May 1988, this number was exceeded by the Ministry of Defense with their distribution of over 9,000 computers to its staff. Over a period of three years beginning in 1989, it is estimated that over 250,000 PCs were distributed through such projects.[79]

[78] Ministerie van Veiligheid en Justitie, Nationale Cyber Security Strategie (2014)
[79] Frank Veraart, 'De domesticatie van de computer in Nederland 1975-1990', *Tijdschrift voor Wetenschaps- en Universiteitsgeschiedenis* 1 (2008), 158.

The increasing adoption of computer technology in the Netherlands revolutionized Dutch society and public administration.[80] Initially recognized and framed by the Dutch government as being a favorable development leading to new and innovative opportunities for the national economy, national focus on computer technology started as early as 5 November 1979, with the presentation of the report of the Advisory Commission on Microelectronics. This committee — chaired by G. W. Rathenau, the former director of Philips NATLAB — was established by the Dutch Minister of Science Policy in order to study the social consequences, particularly the impact on the labor market, of the rise of so-called *micro-electronics*.[81] The report issued by this commission placed the advent of a so-called information society on the political and social agenda and laid the basis for a targeted industrial policy.[82] The report also devoted much attention to a broad-based preparation of society for the advent of the new information technology through both information and education. The commission's recommendations were widely supported by the Dutch government and led to numerous experiments with public information services. Most notable of these endeavors were those by the state-owned Dutch Broadcasting Stichting (NOS) and PTT who, utilizing centralized computers, co-developed a so-called View Data System. The NOS developed the Dutch version of Teletext, where information could be accessed through a customized TV remote control. Meanwhile, the PTT developed an interactive system called Viditel, through which databases could be accessed via terminals and personal computers connected to the telephone line.[83]

While mainly framed as a positive development for Dutch society, many politicians and policymakers were slowly expressing their concerns regarding the security of such information technology.[84] Within the international community, high-profile "computer abuse" incidents such as the cases of Robert Schifreen and Stephen Gold, who gained unauthorized access to British Telecom's Prestel interactive view-data service using conventional home computers and modems in late 1984 and early 1985, and the hack of the Los Alamos National

[80] Marc Groenhuijsen, 'Het wetsvoorstel computercriminaliteit bezien vanuit het gezichtspunt van een behoorlijk wetgevingsbeleid op strafrechtelijk gebied' in F. Wiemans (ed.), *Commentaren op het wetsvoorstel computercriminaliteit* (Maastricht, 1991), 9-22.
[81] Handelingen I, 1980/1981, 25 November 1980**.** The Handelingen are the Parliamentary Proceedings of the debates in the Second (II) and First (I) Chambers.
[82] Veraart, 'De domesticatie van de computer in Nederland 1975-1990', 151.
[83] Veraart, 'De domesticatie van de computer in Nederland 1975-1990', 151.
[84] Ministerie van Verkeer en Waterstaat, *Interactieve videotex in Nederland Standpunt van de regering met betrekking tot het 'Eindrapport van de Stuurgroep ter begeleiding van de PTT-praktijkproef met viewdata'* (1984) [http://publicaties.minienm.nl/download-bijlage/9866/interactieve-videotex-in-nederland-standpunt-van-de-regering-met-betrekking-tot-het-eindrapport-van-de-stuurgroep-ter-begeleiding-van-de-ptt-praktijkproef-met-viewdata.pdf accessed online 14 December 2015].

Laboratory, Sloan-Kettering Cancer Center, and Security Pacific Bank by the a group of hackers in the early 1980s, had already raised numerous concerns internationally regarding the possibilities of malignant use of computers.[85] In the Netherlands, the controversial intrusion into the computer system of the National Institute for Environment (RIVM) by a freelance journalist in March 1985 had already introduced these issues into the Dutch national political arena, leading to several parliamentary questions for the Minister of Justice Korthals-Altes regarding the security of computer systems.[86]

The break-in at the computer of the RIVM marked the beginning of political discussions of potential penalization of computer intrusions. In legal terms, such intrusions were not incorporated in to Dutch criminal law and thus not yet punishable. As a result, this raised the question amongst politicians and policymakers as to whether or not existing traditional criminal provisions still provided adequate protection under law. While criminal codes of most of nations, including the Netherlands, traditionally focused on the protection of visible, physical, and tangible objects, the advent of the computer prompted many nations to institute legal reforms aimed to deal with these issues of the so-called "digital domain". In particular, much of this new legislation addressed the new capabilities of criminal acts using a computer to impact traditional objects and to protect incorporeal objects such as computer software.[87] In the Netherlands, this led to the initiation of a legislative process in the mid-1980s, as existing jurisprudence was viewed insufficient to achieve adequate control of different forms of the now emerging phenomenon of what was then referred to as "computer crime".[88]

To investigate legal matters and to prepare potential legislation in the area of computer technology, the Dutch government opted for the formation of a special commission to deal specifically with issues related to new information technology and criminal law: the Commission on Computer Crime (Commissie Computercriminaliteit). This commission was established to provide legislative recommendations on potential revisions of the Dutch Criminal Code and the Code of Criminal Procedure in light of the developments in information and communication technology.[89] Its formation roughly coincided with

[85] 'Timeline: The U.S. Government and Cybersecurity', The Washington Post, 16 May 2003, [http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html accessed online 12 December 2015].
[86] 'Computerinbraak wordt strafbaar', Leidsch Dagblad, 13 March 1985, [http://leiden.courant.nu/issue/LD/1985-03-13/edition/0/page/5?query=Maart%201800&sort=relevance accessed 12 December 2015].
[87] Ulrich Sieber, 'Legal Aspects of Computer-Related Crime in the Information Society', report prepared for the European Commission (1998), 24–26, [http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf accessed online 12 December 2015].
[88] Mischa van Perzie, *ICT en Recht* (Wolters Kluwer, 2008), 106.
[89] Kamerstukken II, 1989/1990, 21 551, nr. 3, 1 - 2.

international developments where the Netherlands was also actively involved in legal matters relating to the misuse of computer technology through organizations such as the Organization for Economic Cooperation and Development (OECD). In 1986, this organization released a report which introduced the concept of computer crime in international law as *"computer - related crime"*, stating that member states had to ensure a basic level of criminal law protection of governmental services which employ computer technology. These findings were also incorporated into a Recommendation of the Committee of Ministers of the Council of Europa.[90]

5.2 A Security Discourse Develops

In 1987, the Commission on Computer Crime released its report entitled "Information Technology and Criminal Law" (Informatietechniek en Strafrecht).[91] The report was intended as a framework for the first major computer-related legislative act by the Dutch government, the Computer Criminality Act, and it contained recommendations for 29 amendments to Dutch criminal law.[92] Its release signified the initiation of a complex policymaking cycle in which recommendations by the Commission for Computer Crime became the topic of detailed discussions. Indeed, shortly after its publication, several seminars were held by the Dutch Ministry of Justice which were instrumental in shaping early legislative discussions on the subject of the security of information and communication technology.[93] These seminars, based on the recommendations made in the report of the Commission on Computer Crime, reflected the manner in which the issue of computer abuse and computer crime were effectively problematized as issues of security by leading policymakers through discussions on the background of the threat, and the way it needed to be confronted.

Initiated by the Commission on Computer Crime's report, many of these discussions defined the threat as primarily a criminal/legal/technical issues, arising out of the potential misuse of newly-developed information and communication systems and its potentially harmful consequences for society. Indeed, as the Judicial Explorations journal by the Ministry of Justice notes: "In addition to positive effects, technological developments often also have negative effects. One noteworthy dark side of the so-called information society is the

[90] Council of Europe, Recommendation, No. R (89) 9.
[91] Commissie Computercriminaliteit, 'Informatietechniek en Strafrecht', *Rapport van de Commissie computercriminaliteit* (Den Haag, 1987).
[92] Commissie Computercriminaliteit, 'Informatietechniek en Strafrecht', *Rapport van de Commissie computercriminaliteit* (Den Haag, 1987).
[93] Ministerie van Justitie, 'Computercriminaliteit', *Justitiële Verkenningen* 13, (1987)

increased vulnerability. Modern information technologies give, in numerous ways, the opportunity for abusive use and new forms of crime".[94]

These opportunities for malicious use and new forms of crime were an occurrence which, according to the journal, "could no longer be spoken of in terms of a marginal phenomenon."[95] Interestingly, while estimates as to the exact frequency of occurrence, as well as the extent of damage of such computer abuse and criminality remained vague, both were framed as being essentially "a growth market", due to "growing dependence and vulnerability of private companies, institutions and even society as a whole on computers and telecommunication".[96]

Another important feature of these early seminars and discussions on Dutch security of information and communication systems is the manner in which discursive links are created between ''network security'' and "individual security'' and human collective referent objects. In a move which simultaneously gives political importance to these referent objects by linking them to the collective referent objects of "the state", "society", and "the economy", computer-related violence was framed as not only leading to the causing of financial harm, it was, according to one of the leading contributors A.C. Berghuis, "also very well conceivable that such violence can endanger the health and even the lives of people".[97] The potential magnitude of such threats to human referent objects is further illustrated in the report by referencing the networked character of computer systems, and its ability to control physical objects. Here, examples are given, ranging from the manipulation of medical data to the interfering with air traffic control systems to potential intrusions in defense systems leading to false assumptions of nuclear attack by an enemy. Thus, "while often technical information resources are the object of computer abuse, such examples demonstrate that such agents can also serve as an instrument of violence".[98]

In addition, expert discourse also played an integral role in shaping much of the early thinking on Dutch information and communication security policy. During the Euroforum seminar held shortly after the publication of the Commission on Computer Crime's report, numerous leading experts highlighted the background of the problem of computer criminality from different societal perspectives.[99] Following largely similar articulations of the issue as mentioned above, one expert, Professor G.P.V. Vandenberghe, the director of the Institute for

[94] Ministerie van Justitie, 'Computercriminaliteit', *Justitiële Verkenningen*, 13 (1987) 5.
[95] Ministerie van Justitie, 'Computercriminaliteit', *Justitiële Verkenningen* 13 (1987) 6.
[96] Ministerie van Justitie, 'Computercriminaliteit', *Justitiële Verkenningen* 13 (1987) 35.
[97] Ministerie van Justitie, 'Computercriminaliteit', *Justitiële Verkenningen*, 13 (1987) 12.
[98] Ministerie van Justitie, 'Computercriminaliteit', *Justitiële Verkenningen*, 13 (1987) 13.
[99] Ministerie van Justitie, 'Computercriminaliteit', *Justitiële Verkenningen*, 13 (1987) 49 – 50.

Computer Science and Law of the VU University Amsterdam, noted "a growing vulnerability of the information society" in which "an infinite number of computers will be accessible from an infinite number of places".[100] This situation was described by Vandenberghe as leading to a "general security problem", one that would entail "physical catastrophes, flaws in hardware, software, human errors and mistakes, but also malicious attacks, theft and fraud".[101]

Similarly, J.B.F. Tasche, Division Director of Rabobank Netherlands NV, an expert who was tasked with highlighting the issue from a business perspective, not only characterized the issue using medical terminology, stating that it was advisable to regard computer criminality as a virus, but also tied it to narratives of organized crime and mafia, introducing the term "InforMafia" into the seminar.[102] Against such discourse, the only noticeable restraint was expressed by the expert responding from the perspective of the citizen, F. Kuitenbrouwer, publicist and commentator for the influential newspaper NRC Handelsblad, who warned of the impact of criminal law and the considerable powers it attributes to the government on the lives and liberties of ordinary citizens.[103]

Following the initial discussions within the Ministry of Justice on the recommendations made by the Commission on Computer Crime, a draft for the Computer Crime Bill was submitted to the Dutch House of Representatives on the 16 May 1990.[104] Having been the subject of intensive debate in legal circles for several years, this submission represented the last stage of the policymaking cycle, with the draft now becoming subject of political debate.[105] This draft was introduced by means of an explanatory memorandum by the Minister of Justice, E. M. H. Hirsch Ballin, in which the legislation of computer crime and computer abuse was essentially framed as a legal matter arising due to the question "as to whether substantive criminal law still provides adequate protection against the possibility of using new techniques to harm legitimate interests". This concern was also extended to the Code of Criminal Procedure which was, in light of technological developments, also questioned as being sufficient, particularly for purposes of truth establishment.[106]

After various amendments and heated debate in the House of Representatives, the definitive version of the Computer Crime Act was enacted and came into effect on 1 March 1993. This act criminalized hacking, referred to then as 'certain breaches of the automated

[100] Ministerie van Justitie, 'Computercriminaliteit', *Justitiële Verkenningen*, 13 (1987) 49 – 50.
[101] Ministerie van Justitie, 'Computercriminaliteit', *Justitiële Verkenningen*, 13 (1987) 51.
[102] Ministerie van Justitie, 'Computercriminaliteit', *Justitiële Verkenningen*, 13 (1987) 52.
[103] Ministerie van Justitie, 'Computercriminaliteit', *Justitiële Verkenningen*, 13 (1987) 53.
[104] Kamerstukken II, 1989/90, 21 551, nr. 2.
[105] For an extensive overview of such legal debates, see: F. Wiemans, *Onderzoek van gegevens in geautomatiseerde werken* (Nijmegen, 2004).
[106] Kamerstukken II, 1989-1990, 21 551, nr. 3.

information systems' for the first time in the Netherlands. However, such hacking was only deemed criminal under the precondition that some form of security had been to be bypassed.[107] The maximum sentence for this crime of hacking into an information system was set at a maximum of up to four years of imprisonment. A notable exception was made for stolen information which served the public interest.[108] For law enforcement purposes, the bill also contained comprehensive regulations regarding computer-related investigative powers. This included the ability to tap into such modern forms of electronic communication such as faxes and computer messages.[109] Nevertheless, while the Computer Crime Act followed many of the legislative recommendations made by the Computer Crime Committee, several exceptions were made. Most notably, the provisions dealing with search and seizure were not implemented.[110]

The enactment of the Computer Crime Act and its antecedent legislative process firmly established computer security as an important security issue on the political agenda of Dutch politicians and policymakers alike. Unlike the conception of *computer security* previously adopted by the majority of computer scientists, revolving around a technical discourse that was focused on developing good programs with a limited number of (serious) bugs and systems that were difficult to penetrate by outside attackers, the events of the mid 1980s to early 1990s marked the advent of the constitution amongst politicians and policymakers of computer security as a viable security issue with the capabilities to pose a potential threat to Dutch society.[111] To mitigate this threat, numerous legislative and regulatory efforts were undertaken by the Dutch government which resulted in an increasing degree of governance in this area. This culminated not only in the Computer Crime Act, but also in various projects aimed at strengthening connections between government and citizens as well as a growing focus on the security of information. As a result, a policy field centered on the effective use of modern information technology slowly emerged, one in which the security of such technology played an integral part as evident from the implementation of complex computer security protocols within the Dutch government, as well as the establishment of multiple government organizations tasked with information security.[112]

---

[107] Erwin Muller, Joanne van der Leun, Martin Moerings, and Patrick van Calster, *Criminaliteit en criminaliteitsbestrijding in Nederland* (Alphen aan de Rijn, 2010), 271.
[108] Kornelis Mollema, *Computercriminaliteit : de wetgeving, de gevolgen voor bedrijven en de accountant* (Deventer, 1993) 52.
[109] Mollema, *Computercriminaliteit : de wetgeving, de gevolgen voor bedrijven en de accountant* 24.
[110] Bert-Jan Koops, 'Cybercrime Legislation in the Netherland', *Electronic Journal of Comparative Law* 14 (2010), 3.
[111] Kamerstukken II, 1989/1990, 21 551, nr. 3.
[112] Kamerstukken II, 1994/1995, 24 175, nr. 2.

In terms of securitization, what is most striking about this development is that at its moment of inception, there appeared to be no substantive basis for regarding computer security as a significant security issue. Indeed, much of the criticism surrounding the legislative process centered on the question on whether developments surrounding computer crime were indeed so worrying that they justified a significant change in Dutch law. During the initial legislative process in 1987, there was little evidence to suggest marked increase in computer criminality in the Netherlands. Further, that which did occur, such as software piracy, was remarkably not covered in the recommendations by the legislative proposals, as it was deemed to already be properly covered under copyright law. Granted, although some disturbing cases of hacking had occurred, little clarity existed as to the extent of the problem, leaving this matter, along with other harmful forms of computer abuse, subject to much speculation.[113] This fact was even acknowledged by the commissioner on Computer Crime itself whom noted in her report that although the proposed legislation was not so much a response to a perceived and urgent need, it was rather "an anticipation of almost certain developments in the near future".[114]

However, arriving several years later during the introduction of the first draft of the Computer Crime Bill, it seemed the situation had not changed, as evidenced from such statements by the then incumbent Minister of Justice in the explanatory memorandum which acknowledged that "at the time of the decision to prepare legislation, there was clearly a gap between the thinkable damage which can be caused by computer crime and the actual damage which was known at that time".[115]Nevertheless, as an apparent means of justification, it was added that "although even today little insight into the actual extent of the problem exists, it is clear that the next few years, serious consideration should be taken with regard to an increase in the number of cases of criminal behavior related to process automation data".[116] To give more credence to this claim, a number of figures were highlighted by the Minister of Justice, including an increase in the number of cases of fraud committed using a computer from 1 case in 1986, to 15 cases in 1989, as reported by the National Criminal Intelligence Service (CRI). In addition, an increase was noted in the involvement of the CRI with cases of computer abuse, rising from 38 cases in 1988 to 72 cases in 1989.[117] Such figures were however not representative of a growing trend, as many of these cases included in the memorandum were

[113] Wiemans, *Onderzoek van gegevens in geautomatiseerde werken*, 88.
[114] Commission on Computer Crime, 'Report Informatietechniek & samenleving', 24-25.
[115] Kamerstukken II 1989/1990, 21 551, nr. 3, 2.
[116] Kamerstukken II 1989/1990, 21 551, nr. 3, 2.
[117] Kamerstukken II 1989/1990, 21 551, nr. 3, 2 - 3.

characterized as instances of computer crime or computer abuse merely due to the fact that automated administration systems (computers) had been encountered during the investigative process. In such cases, the CRI had simply provided technical assistance which primarily consisted of making data visible to investigators, meaning that computer crime or computer abuse was not necessarily involved.[118] The instances of computer hacking and computer viruses were similarly low, with the explanatory memorandum citing only eleven cases of hacking and computer viruses in 1989.[119]

From contrasting such figures against much of the prevalent discourse surrounding computer security at that time, much can be said in terms of proportionality of the enactment of the Computer Crime Act and its accompanying implementation of quite far-reaching investigative instruments. Indeed, it raises the valid question as to whether developments relating to computer crime were indeed so worrying that they justified a profound change in Dutch criminal law. This was, however, cleverly countered by the subsequent employment of a justifying narrative, consisting of repetitive statements to the effect that computer security was essentially an issue of growing magnitude and implications in the future. In terms of securitization, such discourse displays striking similarities to the central if-then character of Securitization Theory: "If we don't deal with this, then…". This type of logic, which appeared to be quite prevalent in the discourse surrounding computer security at that time, appealed in an important sense, to a central tenant of security; to fears of the unknown, the unforeseen and perhaps even the unforeseeable – to dire possibilities that might be realized even if no knowledge exists, or even can exist of what these may entail.[120] Indeed, much of discourse in the explanatory memorandum of the Computer Crime Act appeared to have followed such logic, noting that "despite uncertainties regarding the definition of computer crime or related concepts, and despite the suspicion a high dark number, one cannot escape the impression of an actual threat to society".[121]

5.3 (Cyber) Securitization – Sub-conclusion I

With regard to the cyber securitization framework, the discourse surrounding the legislative process of the Computer Crime Act displayed only minor occurrences of the three grammatical modalities. Computer security, although connected to the larger referent object

[118] Wiemans, Onderzoek van gegevens in geautomatiseerde werken, 89.
[119] Kamerstukken II 1989/1990, 21 551, Nr. 3, 2.
[120] Michael C. Williams, 'The Continuing Evolution of Securitization Theory', in Thierry Balzacq (ed.), *Securitization Theory, How Security Problems Emerge and Dissolve*, (New York, 2011), 215.
[121] Kamerstukken II, 1989/1990, 21 504, Nr. 3, 3.

of society, did not entail a framing akin to the instantaneous cascading disaster scenarios typical of hyper-securitizations. Everyday security practices were similarly lacking as computer technology, although rapidly disseminating throughout society, was still both unavailable to many as well as relatively unknown in terms of its capabilities and thus potential to impact society. Indeed, with regard to the latter, such familiarity with computer technology existed primarily in the growing scene of computer hobbyists.[122] As such, it was prohibited from drawing upon and securitizing the lived experiences of the individual.

It is of the three grammatical modalities, that perhaps only technifications were, to a minor degree, visible. Veritably, computer security, through its emergence out of concerns regarding the relevance of criminal law, involved a wide array of legal and other experts. In particular, their involvement in the policymaking process leading up to the submission of the Computer Crime Act, constituted to a certain extent the establishment of an epistemic authority which, by virtue of its invitation by the Dutch government to play an active role in shaping these policies, was also granted political legitimacy. Nonetheless, while this involvement arguably signified a view of the issue as being reliant upon expert knowledge, it did not entirely presuppose a politically and normatively neutral agenda. Granted, although some experts saw adjustments to the Dutch criminal law as entirely desirable given the growing threat of computer criminality and computer abuse,[123] there was also a considerable counter-narrative. Here, the contributions of Kuitenbrouwer stand out, which openly questioned the desirability of the expansion of governmental criminal measures.[124] In addition, other experts and expert groups, including the Dutch Association for Information Technology and Law (NVIR) also expressed notable legal criticism in relation to the proposed adjustments.[125] Moreover, while arguably defying what Huysmans described as the invisible role of most security experts, the also question remains to what extent such experts spoke to the broader public.[126] Here, perhaps the notable exception again being Kuitenbrouwer who, through his role as a commentator for the influential newspaper NRC Handelsblad, had the potential to reach a larger audience.

Taking the above into account, there is little evidence to suggest cyber securitization having occurred during the early stages of computer security policymaking. The issue was primarily approached from a legal/technical perspective, without a pronounced securitizing

[122] Veraart, 'De domesticatie van de computer in Nederland 1975-1990', 151.
[123] Ministerie van Justitie, 'Computercriminaliteit', *Justitiële Verkenningen*, 13 (1987) 24 – 35.
[124] Ministerie van Justitie, 'Computercriminaliteit', *Justitiële Verkenningen*, 13 (1987) 53.
[125] Wiemans, Onderzoek van gegevens in geautomatiseerde werken, 90 - 122.
[126] Huysmans, *The Politics of Insecurity*, 9.

move from ‘‘computer security’’ to ‘‘cybersecurity” in which technical discourse is linked to the securitizing discourse ‘‘developed in the specialized arena of national security’’.[127] Moreover, even when analyzed in terms of ‘regular’ securitization, notable deficiencies are observable. Indeed, while the emergence of computer security as a securitizing concept in the Netherlands contained, to a minor extent, some characteristics of securitization, little suggests the presence of an actual act of securitization itself. According to Securitization Theory, security ‘‘frames the issue either as a special kind of politics or as above politics’’ and involves the definition of a spectrum which ranges public issues from the non-politicized—(‘‘the state does not deal with it and it is not in any other way made an issue of public debate and decision”) through politicized—(‘‘the issue is part of public policy, requiring government decision and resource allocations or, more rarely, some other form of communal governance’’) to securitization—(in which case an issue is no longer debated as a political question, but dealt with at an accelerated pace and in ways that may violate normal legal and social rules.”)[128] Although lacking substantive basis, the entire legislative process and its resulting enactment of the Computer Crime Act, did not fall within the aforementioned securitization-end of the spectrum. On the spectrum, it fell definitively under the category of being politicized, as the entirety of the legislative process was very much the subject of political debate and bargaining. Primary evidence to this fact are the various proposed amendments by House of Representatives members, as well as the intensive, and long lasting period of debate between its initial submission in 1990 and its final enactment in 1993.[129]As such, the emergence of computer security as a securitizing concept merely politicized the matter, effectively establishing it as an important security issue on the political agenda in the Netherlands. However, while government activity in this field was steadily taking shape, new developments would soon trigger a significant change within the political discourse on computer security. In particular, several important developments in the early 21st century, i.e. the Millennium Bug. This event played an important role in Dutch computer security policy, imbuing it with a new sense of urgency by emphasizing not only a specific societal reliance on the proper functioning of such systems, but also their vulnerability and the potential harmful effects of their failure.[130]

[127] Nissenbaum, ‘Where Computer Security Meets National Security’, 65.
[128] Buzan, Wæver and de Wilde, *Security: A New Framework for Analysis*, 23.
[129] For an extensive overview of such amendments, and indeed the entire process of political deliberation, see: Wiemans, *Onderzoek van gegevens in geautomatiseerde werken* (Nijmegen, 2004), 87 – 88.
[130] Erwin Muller, Uri Rosenthal, Ira Helsloot & Erwin van Dijkman, *Crisis: Studie over crisis en crisisbeheersing* (Deventer, 2009), 725.

5.4 A Competing (In)Security

Cybersecurity is a terrain on which multiple discourses and (in)securities compete.[131] Having effectively emerged as a securitizing concept, and correspondingly as an important security issue on the political agenda, through articulations of threat based on computer criminality and computer abuse, a competing articulation of linked referent objects emerged during the latter part of the 1990s. During this period, the Millennium Bug became an increasingly worrisome issue for both Dutch politicians and policymakers alike. First introduced onto the political agenda by parliamentary member of the General Elderly Alliance (AOV) Willibrord Verkerk, the Millennium Bug essentially entailed that on 1 January 2000, the hardware and software of essential computer systems would behave unreliably and unpredictably, due to problems in computer programs' date systems.[132] Consequently, due to the growing dependence on technology and interconnectedness between organizations and systems, this entailed a major technological challenge for the Dutch government as it feared that without action to ensure the proper functioning of the national infrastructure Dutch society would face potentially massively disruptive consequences. While these consequences were foremost presented as being an economic in nature, many risk scenarios described potential cumulative health and safety consequences. Without proper mitigation, such risk scenarios were expected to have consequences in the financial and business world, military and health care organizations, nuclear power plants, the chemical industry, the energy supply, transport sector, in small and medium sized businesses, and eventually in people's homes".[133]

In order to mitigate the Millennium Bug problem, the Dutch government employed a proactive strategy which included very specific and highly-coordinated risk management and communication. On the national level, this strategy included a comprehensive range of initiatives, including extensive public awareness campaigns for both businesses and the general public; the tasking of all Dutch ministries with making a comprehensive inventory of their vital products, services and processes in order to effectively secure their functioning; and the establishment of a special task force, consisting of a cooperative venture between government and the largest employers' organization in the Netherlands, the Confederation of Netherlands Industry and Employers (VNO-NCW).[134] This task force, called the Millennium Platform, functioned as a central hub for information collection and exchange and as a

[131] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1162.
[132] Handelingen II, 1995/1996, nr. 1647.
[133] Jan Gutteling and Margot Kuttschreuter, 'The role of expertise in risk communication: laypeople's and expert's perception of the Millennium Bug risk in The Netherlands', *Journal of Risk Research* 5 (2002), 35-43.
[134] Kamerstukken II, 1997/1998, 25 674, nr. 15.

coordinating organ for efforts undertaken in the Netherlands aimed at solving the millennium problem. Its tasks included creating an comprehensive risk analysis designed to clarify the extent of the millennium problem for both public and private actors and to indicate where priority action plans should be drawn up or undertaken.[135] This approach was also marked by an extensive international dimension, with a wide range of diplomatic initiatives aimed at increasing both millennium awareness and encouraging subsequent international action.[136]

The potentially devastating effects of the Millennium Bug had a significant impact on discourse on computer security. Following the rapid expansion of computers in the late 1980s to early 1990s, their use had steadily increased to the degree that certain extent of societal reliance existed within the Netherlands. The Millennium Bug thus presented a significant security issue. As a result, the discursive constitution of computers as being essentially vital for the proper function of society, discourse which had only marginally established itself during the initial policymaking stages of computer security, became more dominant in computer security discourse. Encapsulated under the umbrella term ICT, this discourse continuously stressed the implications of network break-downs for other referent objects such as ‘’society’’, “the state” or ‘‘the economy” effectively tying these referent objects together in a particular securitizing pattern described Hansen and Nissenbaum as operating by providing a link between referent objects that do not explicitly invoke a bounded human collectively, such as ‘‘network’’ or ‘’individual’’, with those that do.[137] This pattern became particularly prevalent in the protection of critical infrastructure, where a threat logic emerged akin to what Cavelty referred to as the conceptualization of security threats as problems of (system) vulnerabilities — the singling out of particular systems and framing of their functions as being ‘vital’ or ‘critical’ due to the fact that their unavailability holds the potential for a political and social crisis.[138]

5.5 Critical Infrastructure

Following the rapid expansion of government initiatives in the field of ICT in the wake of the Millennium Bug issue, a memorandum entitled “The Digital Delta” was presented to the House of Representatives in June of 1999. Prompted by concerns regarding potential fragmentation of such government initiatives, this policy document, which was created in a joint effort by the Ministries of Economic Affairs, Interior and Kingdom Relations, Finance,

[135] Kamerstukken II, 1996/1997, 25 000-VII, nr. 41.
[136] Kamerstukken II, 1998/1999, 25 674, nr. 34.
[137] Hansen and Nissenbaum, ‘Digital Disaster, Cybersecurity, and the Copenhagen School’, 1163.
[138] Cavelty, ‘From Cyber-Bombs to Political Fallout’, 114.

Justice, Education, Culture and Science and Transport and Water, laid out detailed plans for the future of government ICT policy. Building on the National Action Plan Electronic Highways of 1994 and the letter sent to the House of Representatives in April 1998 entitled "Re-evaluation of the National Action Program Electronic Highway" this policy document announced a division of the future development of ICT in into five separate policy pillars, which together were seen as determining of the strength of the ICT base of the Netherlands.[139] Technical reliability of (tele)-communication infrastructure was seen as the constitution one of these pillars, with the policy stating that the strong integration of ICT in society makes "the functioning of society increasingly dependent on the technical reliability of the (tele)communications services. Security information systems and communication infrastructures, and management of the increasing complexity of ever advanced applications are thus increasingly important". This statement was further clarified and repeated throughout the document, which continuously established links between various referent objects by noting not only that "many functions, such as financial and logistical functions depend on an adequate operation of infrastructure for their diverse data and voice services" but also that there are "strong chain dependencies, such as those between energy, communication techniques and computers". The vulnerability of the networked nature of telecommunications infrastructure was also emphasized, with networks deemed "in principal, vulnerable, both to technical failure (cable breach, failure of computers) as well as attacks by hackers."[140] Here, the profound impact of the Millennium Bug was acknowledged, with the policy document noting "the millennium issue has made us realize how dependent we have become the reliability of computers, and how the danger can lurk in a small corner".[141]

To deal with the aforementioned structural dependency on ICT, an in-depth exploration into the vulnerabilities and weaknesses of the ICT infrastructure was announced. The memorandum 'Kwetsbaarheid op Internet' (Vulnerability on the Internet) or KWINT was released in 2001 as part of these explorations. Forming a part of a wider policy on vital infrastructures, such as the power grid, water supplies and the transportation infrastructure, this document defined the Internet as "one of the critical infrastructures of a modern society like the Netherlands".[142] As such, it would mark the inception of a linkage of technical discourse to the securitizing discourse developed in the specialized arena of national security by constituting the reliability of the critical infrastructure as a vital security issue with

[139] Kamerstukken II, 1997/1998, 24 565, nr. 7; Kamerstukken II, 1998/1999, 26 643, nr. 1, 5.
[140] Kamerstukken II, 1998/1999, 26 643, nr. 1, 41.
[141] Kamerstukken II, 1998/1999, 26 643, nr. 1, 41.
[142] Kamerstukken II, 2000/2001, 26 643, nr. 30, 9.

potentially far-reaching consequences to a wide range of sectors, including national security, by defining critical infrastructure as "a system either, physical or virtual, so vital for a country that the loss of this has a weakening effect on the social and economic functioning and national security".[143] Towards reducing this vulnerability, the memorandum KWINT offered various plans including the establishment by the Interior Ministry of a CERT (Central Emergency Response Team) for the government.[144]

The release of the KWINT memorandum marked the predominance of a securitizing computer discourse in which critical infrastructure played an integral role. During that same year, as part of a wider framework centered on addressing the vulnerabilities of critical infrastructure, a National Telecommunication Continuity Plan (NACOTEL) was formulated.[145] Aimed at creating a reliable telecommunications infrastructure, this plan traced back to March of 2001, when a political motion issued by House of Representatives member Wijn (CDA) was passed, which "in the light of the growing dependence on ICT" and "growing vulnerability of vital social, ICT-related services", asked for a broad "cross-sector plan on protection of vital infrastructure" to be implemented by the Dutch government.[146] This cross-sector plan would eventually result in the setting up of the large scale project Protection of Vital Infrastructures in 2002, which focused on "vital sectors, services and products that have national impact in the event of disruption".[147] Framing ICT as a critical infrastructure which was an essential component vital to the functioning of many sectors of Dutch society, it listed its goals as the establishment of (1) a coherent package of measures to protect the infrastructure of government and industry, including ICT and (2) the anchoring of this package of measures in the ordinary course of business.[148] In 2004, this framework was further developed through the formulation of the so-called "government-wide ICT-agenda". Part of the wider ongoing discussions on the digitization of Dutch society, this policy document laid out the goals, aspirations and actions of the Dutch government towards the creation of a set of conditions which would allow for a more optimal use of ICT by Dutch society. [149] Here, security was heavily emphasized security as an essential precondition, with

[143] Kamerstukken II, 2000/2001, 26 643, nr. 30.
[144] Kamerstukken II, 2000/2001, 26 643, nr. 30, 6.
[145] Kamerstukken II, 2000/2001, 26 643, nr. 30.
[146] Kamerstukken II, 2000/2001, 26 643, nr. 20.
[147] Kamerstukken II, 2002/2003, 26 643, nr. 39, 2.
[148] Kamerstukken II, 2002/2003, 26 643, nr. 39, 2.
[149] Kamerstukken II, 2003/2004, 26 643, nr. 47.

one of the stated objectives listed as the creation of a 'security culture' in the design and implementation of ICT products.[150]

The establishment of KWINT, NACOTEL and ICT-agenda laid the basis for what was eventually a more coordinated and comprehensive Dutch ICT security policy framework. Prompted by the Millennium Bug issue, computer security, as a securitizing concept, gradually shifted during this period from a focus on computer criminality and computer abuse to a discourse based on the protection of critical infrastructure. Following a Cavelty-esque pattern of discourse, government initiatives in this area widely expanded, leading to the formulation of various policies in which security of "the network" was framed as playing an integral role in the proper functioning of Dutch society.[151] These policies led to the initiation of a multitude of interdepartmental ICT projects, many of which featured significant national security components. Such initiatives included aforementioned launch of CERT-RO, a Computer Emergency Response Team for the Dutch government (which eventually became GOVCERT and, respectively, the National Cybersecurity Center), and even, as a supplementary measure, a "cyber doom" warning system for both citizens and private companies.[152]

5.6 (Cyber) Securitization – Sub-conclusion II

With regard to the cyber securitization framework, a number of interfaces can be observed. Hyper-securitizations, although not adhering to the typical historical reference structure, slowly but surely presented themselves in computer security discourse. The most notable being the Millennium Bug, which exemplified the typical cascading disaster scenario of hyper-securitization. During this period, Y2K's potentially devastating effects were discursively connected to a host of referent objects, including the state, the economy and the society, through an extensive emphasis on the protection of critical infrastructure. This protection was regarded by many as a vital security matter as critical infrastructure was, through its networked nature, connected to a host of societal interests.[153] The severity of such connections in discourse become particularly evident when contrasted to government action, which even included the readying of military personnel in case of major societal problems.[154]

[150] Kamerstukken II, 2003/2004, 26 643, nr. 47, 14.
[151] Cavelty, 'From Cyber-Bombs to Political Fallout', 114.
[152] Kamerstukken II, 2003/2004, 26 643, nr. 47, 14.
[153] Handelingen II, 1997/1998, Nr. 49, 3767-3769.
[154] 'Militairen paraat tijdens eeuwwisseling', NRC Handelsblad, 24 December 1998, [http://retro.nrc.nl/W2/Lab/Millennium/981224.html accessed online 19 December 2015].

The grammatical modality of everyday security practices was also evident in discourse, as the effects of Y2K, without proper mitigation, were expected to have consequences in a wide array of areas which drew upon experiences familiar from everyday life. However, such everyday security practices did not yet seek to secure the individual's partnership and compliance in protecting network security. Indeed, apart from perhaps the mobilization towards business, and to a smaller extent the individual to ensure their computer was Y2K compliant, the Millennium Bug, was largely constituted as a matter of the larger entities of the government and business, as evident from the majority of policies. This focus was also continued in the subsequent period after Y2K, as evident throughout the policies pertaining to critical infrastructure protection. Connected to this modality, there was also a notable absence in discourse regarding the constitution the individual as a liability or indeed a threat. Through its nature as being a technical problem which was already present in computer technology, the Millennium Bug was, to a convincingly large degree, not framed as an issue in which the compliance of the individual was seen as vital. Granted, individuals were urged to make their computers Y2K compliant, but the overall focus in policy towards the business community, as well as critical infrastructure, suggests only a minor importance being placed on the role of the individual.

The last modality of cyber securitization, namely technifications, manifested itself primarily through the government's formation of the Millennium Platform. This panel of experts, including many from outside the government, was actively involved the mitigation process of Y2K. By its formation by the government, this panel was granted political legitimacy and acknowledged as constituting an epistemic authority.[155] Its prominent role in the resolution of Y2K largely solidified proposed policies and measures as politically neutral or unquestionably normatively desirable. Indeed, government policymaking was underlined by a remarkable securitizing discourse from various experts within the Millennium Platform, which advocated such measures which included stockpiling, reduction of business investments, and a moratorium on the installation of new computer software. In addition, the government itself was also warned, especially in relation to the introduction of new legislation.[156] Such warnings however, were not only limited to the experts of the Millennium

[155] Kamerstukken II, 1997/1998, 25 894, nr. 261.
[156] Michiel van Nieuwstadt, 'Vul de schuren: De voorbereiding op het millenniumprobleem', NRC Handelsblad, 31 December 1998 [http://retro.nrc.nl/W2/Lab/Millennium/981231b.html accessed online 13 December 2015].

Platform, as a host of computer experts now appeared in the media, which spoke to the public in an increasingly securitizing discourse.[157]

Relating to securitization, the policies and initiatives formulate during this period contained a remarkable securitizing discourse revolving around the continuing emphasis on how the connectedness of critical infrastructures poses a danger to Dutch society. Increasingly, the dangers of ICT failure were presented as having tremendous impact, as they were linked an enlarging number of referent objects.[158] This linkage ensured the relevance of computer security, now captured under the umbrella term ICT, to a large number of issues, effectively drawing them into a securitizing logic. This discourse was best exemplified in a joint letter from then incumbent Ministers of Economic Affairs and Administrative Innovation and Kingdom Relations, which noted that "ICT is everywhere."[159]

That being said, it should be noted that, despite this securitizing discourse, the issue was still part of public policy, requiring government decision and resource allocations, and arguably not a securitization—in which case an issue is no longer debated as a political question, but dealt with at an accelerated pace and in ways that may violate normal legal and social rules. Granted, although Y2K, through its ominous specter of total societal meltdown, had undoubtedly introduced a sense of urgency which arguably reduced the contestation of ICT policy, its formulation and implementation still adhered to regular political procedures. Moreover, in terms of exceptionality, a certain measure of legislative restraint was also present. For example, although the KWINT memorandum was based primarily on government activities, the role of government it envisioned for the government was modest. The primary responsibility for security was placed with each involved party itself, and the government restricted its regulatory involvement, performing only a facilitating role, as not to "needlessly to disturb the still developing market".[160]

The securitizing discourse resulting from Y2K effectively laid the groundwork for the further development of computer security as a securitizing concept. Encapsulating it within the broader framework of ICT and critical infrastructure protection, it developed new importance and urgency. As such, it continued to gain momentum, drawing ever increasing attention from politicians and policymakers. Nevertheless, despite both the discourse which continually stressed the vulnerability stemming from complexity, interdependency, and

[157] Ine Poppe, 'De oplossing voor het millenniumprobleem: Vlucht!', NRC Handelsblad, 19 December, [http://retro.nrc.nl/W2/Lab/Millennium/981219.html accessed online 3 December 2015].
[158] Kamerstukken II, 2000/2001, 26 643, nr. 30, 9.
[159] Kamerstukken II, 2003/2004, 26643, nr. 47.
[160] Kamerstukken II, 2000/2001, 26643, nr. 30, 4.

dependency, and the myriad of projects and programs initiated the area of ICT security, a coherent Dutch cybersecurity strategy did not yet come into existence. Although policy in the field of computer technology had advanced significantly since the initial policymaking stages in the 1980s and 1990s, many governmental activities dealing with its security were not always carefully coordinated. This resulted in multiple departments often working on the same issue, without any form of consultation amongst each other or even knowledge of each other's activities. In addition, these projects would not always build upon the successes or attained knowledge from previous endeavors. Consequently, despite policies aimed specifically to prevent it, fragmentation still occurred, as each department strictly focused on their own specialization and field of operations.[161]

5.7 Towards a Unified Strategy

With the launch of the project "Reassessment ICT security policy" in 2006, another important step was taken towards the creation of more coordination and coherence of Dutch ICT security policy. Initially starting as a large scale inter-ministerial stocktaking towards the creation of proactive governmental policy towards avoiding social disruption, this project was essentially geared towards creating greater coordination between the relevant ministries themselves and between the various parties (companies, organizations, also local governments and foreign) active in the field of ICT security.[162] Coordinated by the Ministries of Home Affairs, Economic Affairs and Justice, this project's objective was to "recalibrate" the fragmented nature of ICT safety-related activities of the government, which had seen a tremendous proliferation of projects and programs which had "come out of the ground like mushrooms".[163] The main findings of this report underlined the need for a more coordinated and effective ICT security strategy, stressing the need for a common governmental policy and recommending structural improvements in three fields: governance, professionalization, and internationally.[164] This increase in coordination and coherence was to be achieved within the broader context of the programs National Security and Protection of Vital Infrastructure.[165] In the following years, much of this coherent policy was formulated in the form of various programs and projects, of which some gradually evolved into structural policy issues. In

[161] Denktank Nationale Veiligheid, ICT-kwetsbaarheid en Nationale Veiligheid (2010), 41.
[162] Kamerstukken II, 2006–2007, 30 821, nr. 1.
[163] Rijksoverheid, Rapport Herijking ICT Veiligheidsbeleid (2006), 2, [http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2007/07/16/project-herijking-ict-veiligheidsbeleid.html accessed online 19 December 2015].
[164] Rijksoverheid, Rapport Herijking ICT Veiligheidsbeleid (2006), 2.
[165] Kamerstukken II, 2007/2008, 26 643, nr. 103.

addition, new institutions, sometimes at the instigation of government departments and sometimes based on its own initiative of social groups and sectors, were set up in the field of ICT security.[166] Many these programs and projects actively contributed to the framing ICT as security issue, stressing the vulnerability of "systems of societal importance", even making a classification of events which were deemed "societally disruptive" and those which weren't, with the former being framed as events which "at the expense of almost everything" should be prevented".[167]

In late 2006, prompted by "a rapidly changing and more diffuse threat assessment",[168] the Dutch government initiated a development which would significantly change the face of national security policymaking. Introduced in the House of Representatives in letter on the 2 October, the then incumbent Minister of Interior and Kingdom Affairs, J. W. Remkes, announced the Project on National Security, which involved extensive plans for the introduction of a new "*all-hazard approach"* to national security.[169] Aimed to "systematically, and on a strategic level, to streamline government action on national security and coordinate it interdepartmentally" this new approach rather broadly defined national security as being at stake when "vital interests of our state and / or our society are threatened in such a way that there is (potential) social disruption".[170] These vital interests, which were even more broadly defined, were divided into five categories: (1) territorial security, encompassing the undisrupted functioning of Netherlands as an independent state in the broadest sense, or the territorial integrity in the narrow sense; the territorial integrity is in question, for example an impending occupation of the territory of the Kingdom by another state, but also by a terrorist attack (2) economic security, the undisrupted functioning of Netherlands as an effective and efficient economy; economic security for example, can be compromised in the event of a large-scale IT failure which renders (electronic) payments paralyzed (3) ecological security, having sufficient self-restoring ability of the environment; ecological security can be compromised for example by such disturbances in the management of surface water, but also by climate change (4) physical security, the undisrupted functioning of people in the Netherlands and its surroundings; physical security is at stake for example in the case when public health is threatened by the outbreak an epidemic, but also a major levee breach or an accident in a chemical plant and (5) social and political stability, the undisturbed

[166] Rijksoverheid, Rapport Herijking ICT Veiligheidsbeleid (2006), 6.
[167] Kamerstukken II, 2007/2008, 26 643, nr. 103.
[168] Kamerstukken II, 2006/2007, 30 821, nr. 1.
[169] Kamerstukken II, 2006/2007, 30 821, nr. 1.
[170] Kamerstukken II, 2006/2007, 30 821, nr. 1, 2–5.

survival of a social climate in which groups of people together can coexist within the framework of the democratic rule of law and shared values; the social and political stability can be compromised if changes occur in demographic community development (solidarity between generations), social cohesion and the degree of participation of the people in societal processes.[171] In short, it encompassed nearly every imaginable aspect of Dutch society.

The introduction of a new *all-hazard approach* in the form of the Project on National Security profoundly affected computer security discourse. Having developed from computer crime and computer abuse to ICT and critical infrastructure protection, it firmly established computer security as a securitizing concept into the highest arena of security, namely national security. Aimed at creating "an overarching strategy for national security," its broad definition of both national security and vital interests enabled the linkage of ICT and its security to an almost limitless array of referent objects. Articulated through such scenarios as digital paralysis, digital insecurity, and ICT-failure, the securitizing discourse developed in the specialized arena of national security, being added to the list of growing list of threats to national security, next to the more classical threats of violations of international peace and security, CBRN (Chemical, Biological, Radioactive and Nuclear), terrorism, and international organized crime.[172] In the following year, the context of this new approach, the Dutch government's official policy instrument for multi-hazard risk management was released. Intended to contribute to the prevention of societal disruption as a consequence of a (future) disaster or crisis in the Netherlands, this document further underscored the penetration of cybersecurity into national security concerns, defining "digital insecurity" as a socio-economic threat, and warning that "a failure of ICT can affect many sectors".[173]

Advancing through national security policy, another important milestone in Dutch cybersecurity policy was reached in 2009, with the submission of a political motion by House of Representatives members Knops (CDA), Voordewind (CU), and Eijsink (PvdA).[174] Marking the beginning of a comprehensive and coherent cybersecurity policy, this motion constituted cyber-attacks on computer systems and networks as "new type of threat", but also one which is not only posed by "organized crime or terrorist organizations", but also potentially from "military forces from other countries". As such, the motion called on the Dutch government not only for "the development of an interdepartmental governmental cybersecurity strategy", but also urged it to "actively participate in the thought process on

[171] Kamerstukken II, 2006/2007, 30 821, nr. 1, 3.
[172] Kamerstukken II, 2006/2007, 30 821, nr. 1, 5.
[173] Rijksoverheid, Strategie Nationale Veiligheid (2007), 12, 22
[174] Kamerstukken II, 2009/2010, 32 123-X, nr. 66.

cyber warfare in NATO context".[175] A few days later, the motion was accepted by a large majority of the Second Chamber.[176]

With the acceptance the parliamentary motion by Knops, the basis for the modern Dutch cybersecurity policy became established. Many of the classical threats to national security now gained their own cyber variants, with the prefix of cyber gradually becoming part of a discourse used to identify a wide array of ICT-related threats to national security, ranging from cyber-terrorism to cyber-attack and cyber-espionage.[177]This development was further compounded by both national and international developments. Internationally, the NATO Strategic Concept of 2010 entailed that each NATO member state, including the Netherlands, institutionally had to accept the risk of cyber-attacks as a high priority security concern. This document echoed much of the same discourse of the Project on National Security, stating that cyber-attacks were not only becoming "more frequent, more organized and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure", but also that their impact was rapidly expanding, with the potential to reach a threshold that "threatens national and Euro-Atlantic prosperity, security and stability".[178] Nationally, similar discourse was also evident, with cybersecurity discourse increasingly taking on a national security character. In 2010, as part of the new National Security Strategy, the inter-ministerial Advisory Committee on National Security released its first report titled "ICT-Vulnerability and National Security".[179] Requested by the Dutch government, this extensive report articulated the rapid proliferation of computer security as a securitizing concept, identifying a wide array of ICT vulnerabilities by highlighting threats such as cyber criminality, critical infrastructure, cyber-warfare, cyber-espionage, and even cyber-terrorism.[180]

In the same year, GOVCERT (the successor of CERT) also released the National Trend Report on Cyber Crime and Digital Security.[181] Based on existing reports by organizations including the national police service (KLPD), the National Coordinator for Counterterrorism (NCTb), Dutch intelligence services (AIVD and MIVD), the Independent

[175] Kamerstukken II, 2009/2010, 32 123-X, nr. 66.
[176] Handelingen II, 2009/2010, TK 34 34-3259.
[177] Rijksoverheid, Nationale Risicobeoordeling (2008); Rijksoverheid, Nationale Risicobeoordeling (2009), Algemene Inlichtingen en Veiligheidsdienst, Jaarverslag (2010); Militaire Inlichtingen en Veiligheidsdienst, Jaarverslag (2009).
[178] North Atlantic Treaty Organisation, Strategic Concept (2010), 11.
[179] Denktank Nationale Veiligheid, ICT-kwetsbaarheid en Nationale Veiligheid (2010).
[180] Denktank Nationale Veiligheid, ICT-kwetsbaarheid en Nationale Veiligheid, (2010), 14-15.
[181] Rijksoverheid, Nationaal Trendrapport Cybercrime en Digitale Veiligheid (2010).

Post and Telecommunications Authority (OPTA) and GOVCERT, and supplemented by the insights of a broad group of experts, this document identified so-called "trends in cyber crime and digital safety" and to relate these to each other.[182]

As part of the follow up on the political motion by Knops, the first ever Dutch National Cybersecurity Strategy was released in 2011.[183] This strategy, which became one of the most important policy documents in Dutch cybersecurity policy, contained one of the first governmental definitions of cybersecurity, combining all elements of the previous articulations of computer security as a securitizing concept. They defined it as:

> "(…) freedom from danger or damage caused by disruption, or failure of ICT, or by malignant use of ICT. The danger or damage caused by malignant use, disruption or failure can consist of restrictions of the availability and reliability of ICT, breach of confidentiality of the information stored in ICT, or damage to the integrity of this information."[184]

Moreover, in a similar cybersecurity discourse as used in the National Security Strategy, it posited ICT as being "essential to the community", linking it to various referent objects together, through such statements that: "…secure and reliable ICT is fundamental to our prosperity and wellbeing, and is a catalyst for (further) sustainable economic growth."[185] Additionally, the document announced the establishment of the Cybersecurity Council and the National Cybersecurity Center (NCSC) with the latter to replace GOVERCERT.[186]

With the implementation of the new *all-hazard approach* to (national)security policymaking, the securitizing concept of computer security moved into the highest arena of national security. Gaining a new prioritization due to its articulation as vital to national security, computer security developed once again, becoming referred to as *cybersecurity*. Set against the background of the newly developed comprehensive risk approach of the Dutch government, this led to the consistent development of a host of new policies and extensive strategy documents which included, to varying degrees, a focus on cybersecurity. This effectively established cybersecurity as an issue which was regarded with great importance for both the present and the future of national security.[187]

[182] Rijksoverheid, Nationaal Trendrapport Cybercrime en Digitale Veiligheid (2010), 7.
[183] Ministerie van Veiligheid en Justitie, Nationale Cybersecurity Strategie (2011).
[184] Ministerie van Veiligheid en Justitie, Nationale Cybersecurity Strategie (2011), 3.
[185] Ministerie van Veiligheid en Justitie, Nationale Cybersecurity Strategie (2011), 3.
[186] Ministerie van Veiligheid en Justitie, Nationale Cybersecurity Strategie (2011), 5.
[187] Kamerstukken II, 2010/2011, 30 821, nr. 12.

5.8 (Cyber) Securitization – Sub-conclusion III

In terms of the cyber securitization framework, the re-calibration of Dutch national security policy, in the form of the National Project on National Security, marked the inception of a securitizing move from *computer security* to *cybersecurity*. Technical discourse was now increasingly linked to the securitizing discourse developed in the specialized arena of national security, as computer security was transformed into a complex, securitizing narrative. This securitizing narrative drew in a wide range of referent objects and sectors through their discursive constitution as being reliant on the proper functioning of ICT which, upon failure, would lead to dramatic consequences for societal stability. As such, this securitizing discourse became pervasive in many aspects of (national)security policymaking.

It is here that a noted presence of the three grammatical modalities of the cyber securitization framework first became truly discernable within computer security discourse. For example, in term of hyper-securitization, failure or damage to "*the network"* or ICT, as it was more frequently referred, was continuously framed in both government letters and policy documents as leading to societal, financial, and military break-down, hence bringing in all other referent objects and sectors. A major contributing factor was the introduction of a broad definition of national security and vital interests which virtually encompassed every aspect of Dutch society. Drawing in a large number of referent objects and sectors, this enabled a discourse which consistently and repetitively, linked ICT failure to "the economy,"[188] "society" and "national defense".[189] Threats to these referent objects included "faltering power supply",[190] "cyber terrorism" and "cyber crime,"[191] and a host of many others, too voluminous to mention.[192]

In addition to such hyper-securitizing discourse, the grammatical modalities of technifications and everyday security practices (which draws upon and securitizes the lived experiences a citizenry may have) also became more prevalent throughout official discourse. For example, in a discourse characteristic of everyday security practices, many of the cybersecurity policies and strategic documents actively sought to secure the individual's partnership and compliance in protecting network security. This was often achieved by

[188] Rijksoverheid, Nationaal Trendrapport Cybercrime en Digitale Veiligheid (2010), 13.
[189] Ministerie van Veiligheid en Justitie, Nationale Cybersecurity Strategie (2011), 2-8.
[190] Rijksoverheid, Strategie Nationale Veiligheid (2007), 6.
[191] Denktank Nationale Veiligheid, ICT-kwetsbaarheid en Nationale Veiligheid (2010), 14-15.
[192] For an extensive overview of referent objects and threats, see: Rijksoverheid, Nationaal Trendrapport Cybercrime en Digitale Veiligheid (2010) and Strategie Nationale Veiligheid (2007); Ministerie van Veiligheid en Justitie, Nationale Cybersecurity Strategie (2011); Denktank Nationale Veiligheid, ICT-kwetsbaarheid en Nationale Veiligheid (2010).

framing cybersecurity as an issue that required active contribution was envisioned for all levels of society, including private citizens and businesses. The National Cybersecurity Strategy outlined the basics of this approach, which was essentially based on public-private partnership (PPP). This attributed a specific responsibility, or actual duty, to citizens to protect their own systems and networks in an adequate manner.[193] These responsibilities were summed up in the National Cybersecurity Strategy of 2011, which stated "all users (citizens, businesses, institutions and governments) [must] take appropriate steps to to protect their own IT systems and networks and to prevent security risks to occur for others. They are careful with storing and sharing of sensitive information and respect the information and the systems of other users".[194] A similar discourse was evident for the use of the Internet on which, according to the National Trend Report Cyber Crime and Digital Security, "citizens, businesses and government each have their own role to play in maintaining safety".[195] However, while such discourse established a vital role for ordinary citizens in cybersecurity, it did not, as Hansen and Nissenbaum hold, entail the "constitution of the individual as liability or indeed a threat".[196] Indeed, although an enlarging role as a responsible partner in fighting insecurity was articulated, this discourse featured no discernable framing of the individual as constituting a security risk.

With regard to technifications, much of the cybersecurity discourse from this period suggests a framing of the issue as a domain requiring advanced technical expertise that the public, and most politicians, did not have. In particular, this is evidenced from such measures as the creation of the NSCS, and the government's intended formation of expert groups and establishment of a register of experts for government, universities and industry, in order to share "scarcely available expertise".[197] Over time, such experts, although part of a remarkably small pool increasingly became securitizing actors which could distinguishing themselves from politicians and other political actors. Although initially remaining primarily in the background, these experts from various backgrounds, including the scientific and business communities and the government itself worked in close cooperation to create various important guiding policy documents and reports. Notable examples included the National Trend Report Cyber Crime and Digital Security, and the Report on ICT-Vulnerability and

[193] Ministerie van Veiligheid en Justitie, Nationale Cybersecurity Strategie (2011), 6.
[194] Ministerie van Veiligheid en Justitie, Nationale Cybersecurity Strategie (2011), 4.
[195] Rijksoverheid, Nationaal Trendrapport Cybercrime en Digitale Veiligheid (2010), 9.
[196] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1166.
[197] Ministerie van Veiligheid en Justitie, Nationale Cybersecurity Strategie (2011), 8.

National Security, both of which featured considerable contributions by experts.[198] Such contributions, through their significant importance in government cybersecurity policy, allowed for what Hansen and Nissenbaum refer to as a "particular constitution of epistemic authority and political legitimacy".[199] Indeed, the sheer fact that, at the highest level of national security, government policymaking actively involved input from experts located outside the political arena, clearly indicated the constitution of expert authority in cybersecurity policymaking with a privileged role as those who have the authority to speak about the unknown.

In terms of securitization, indications of a securitizing move now also appeared. Indeed, computer security, now falling under national security, was increasingly dealt with at an accelerated pace characteristic of securitization. The introduction of the *all-hazard approach* to national security, as well as the parliamentary motion by Knops, both exemplify a perceived necessity to create a (national)security framework to deal with what was then observed as a "greatly changing" and "diffuse" range of threats with "growing impact".[200] To mitigate this, great speed was employed towards the implementation of such a new approach, which essentially entailed large changes to the structure of (national)security policymaking. The impressive rate at which its relevant policy documents were formulated and released, arguably signify the importance of this issue, signifying that it was, to some degree, indeed handled at a securitizing pace. Moreover, the move of computer security into the arena of national security was hardly challenged, as most of the national and cybersecurity developments, although initially introduced in the Dutch House of Representatives, still remained confined to the purview of the various ministries and a small number of involved politicians.

Nonetheless, notwithstanding such indications, there was no evidence to suggest that the introduction of this approach, at any point, entailed the characteristic violation of legal and social rules of securitization. Indeed, as apparent from the parliamentary proceedings, the entirety of the introduction of this new approach completely followed established Dutch policymaking procedures. Moreover, and perhaps most importantly, although the move from computer security into national security considerations was largely uncontested, the scope of the issue remained the matter of much political debate. Indeed, as evidenced from deliberations in the House of Representatives, the scope of cybersecurity was continually

[198]Denktank Nationale Veiligheid, ICT-kwetsbaarheid en Nationale Veiligheid (2010), 4; Rijksoverheid, Nationaal Trendrapport Cybercrime en Digitale Veiligheid (2010), 47.
[199] Hansen and Nissenbaum, 'Digital Disaster, Cybersecurity, and the Copenhagen School', 1167.
[200] Kamerstukken II, 2006/2007, 30 821, nr. 1.

questioned by many Dutch politicians. This was especially valid of cybersecurity in terms of national security, a matter viewed as being distinct different from cyber crime.[201] Thus, while arguably now moved within the arena of national security, cybersecurity did remain a politicized issue. For example, as parliamentary member Gerard Schouw from the political party Democrats 66 (D66) noted during the general deliberations held on the 11 July entitled 'towards a safer society':

> "What exactly is the factual basis of the problem? That's the first question you should ask before embarking on a policy. How vulnerable are we and how often data is stolen and from whom? How often do nations conduct cyber-war with each other? Because figures are not available, the chosen strategy is too generic. We read that data on the extent of the problem is lacking. One consequence of the lack of detail is that it opens the door wide to unbridled governmental control on, for example, the Internet."[202]

Similar sentiments were also echoed by Tofik Dibi, a parliamentary member from the Green Party (GroenLinks), who, in addition to asking questions concerning the lack of clarity surrounding the issue, also commented on the danger of such unbridled governmental control and its consequences for civil liberties by stating that the potential of ICT to do harm "calls on governments not to simply on the basis of fear of sacrificing civil achievements, but to take effective and transparent measures based on calculated risks to ensure the protection of fundamental rights".[203] Such cautionary discourse was not only limited to oppositional parties, as even members of the largest coalition party, the People's Party for Freedom and Democracy (VVD), warned the Dutch cabinet not to "let ourselves be led by ghost stories and hypes" whilst deciding on the appropriate policy course.[204]

Such questions touched on an important issue during the introduction of the new *all-hazard approach* to national security, namely a substantial lack of clarity regarding the exact extent of the greatly changing and diffuse threats which were constituted as the main reason for initiating such significant changes to (national)security policymaking. Indeed, as the Report ICT-Vulnerability and National Security noted: "There is no party which possesses a comprehensive and balanced picture of the situation. This image is lacking both for threats and vulnerabilities, opportunities and capabilities of the various parties, as well as the

[201] Kamerstukken II, 2010/2011, 28684 nr. 323, 13.
[202] Kamerstukken II, 2010/2011, 28684 nr. 323, 4-5.
[203] Kamerstukken II, 2010/2011, 28684 nr. 323, 1.
[204] Kamerstukken II, 2010/2011, 28 684 nr. 323, 13.

legislative framework in which can and may be operated." [205] This lack of a comprehensive and balanced picture of the situation also affected many of the cybersecurity policies and strategic documents which were, at this stage, still in their infancy. For example, the National Cybersecurity Strategy in 2011 which was explicitly described as a "*work in progress*"[206] and consisted of only nine pages; a stark contrast with the exponentially more detailed, 45 pages long, National Cybersecurity Strategy of 2014.[207]

However, in the latter part of 2011, an important incident in the Netherlands presented politicians and policymakers with exactly the extent of the cybersecurity and its corresponding threats, in the form a new kind of disaster image or threat: the digital disaster. Decidedly impacting cybersecurity discourse, this threat image imbued cybersecurity with great sense of urgency, catapulting the issue to the top of Dutch political agenda.[208]

5.9 Digital Disaster

In the late summer/early autumn of 2011, an electronic break-in at DigiNotar, a Certificate Authority (CA) which issues digital certificates vital to the security, authenticity, and integrity of digital communication, compromised the security of several Dutch governmental online services including DigiD, an identity management platform which government agencies of the Netherlands use to verify the identity of Dutch citizens on the Internet, and the online services of Dutch tax department. Interrupting the regular Dutch television broadcasting schedule, an emergency press conference was immediately held by the Dutch minister of the Interior and Kingdom relations Piet-Hein Donner who issued a statement that the Dutch government could longer guarantee the security of sensitive/confidential information. Subsequently, the Dutch government reacted immediately, revoking all certificates issued by DigiNotar[209] and issuing specific instructions to the general public.[210]

The Diginotar incident signified an important development in computer security policymaking. Officially recognized by the Dutch government as a national crisis with

[205] Denktank Nationale Veiligheid, Rapport ICT-kwetsbaarheid en Nationale Veiligheid (2010), 44.
[206] Ministerie van Veiligheid en Justitie, Nationale Cybersecurity Strategie (2011), 8.
[207] Ministerie van Veiligheid en Justitie, Nationale Cybersecurity Strategie (2014).
[208] Kamerstukken II, 2010/2011, 26 643, nr. 174, 1.
[209] 'Donner: veiligheid sites overheid niet gegarandeerd', De Volkskrant, 3 September 2011, [http://www.volkskrant.nl/recensies/donner-veiligheid-sites-overheid-niet-gegarandeerd~a2887060/ accessed online 3 December 2015].
[210] 'Informatie over Diginotar', Rijksoverheid, 5 September 2011, [https://www.rijksoverheid.nl/documenten/brochures/2011/09/05/informatie-over-diginotar accessed online 3 December 2015].

potentially far-reaching consequences for society, the DigiNotar incident significantly affected cybersecurity discourse and the broader discussions of so-called cyber-attacks. The discussions, which had taken place amongst politicians and policymakers for several years already, but whose scope and guiding policies remained yet to be determined, took a decidedly different turn in terms of discourse.[211] A few months before, many of the opposition parties had previously advocated for a cautionary approach, especially in terms of government control due to fears regarding its consequences, they now openly advocated precisely the opposite. For example, political party D66, whose members had previously warned of "unbridled governmental control", now questioned whether the Dutch government was in fact "in control" when it came to reliability and security of ICT, warning the government "not to lose sight of security".[212]

A similar sentiment was echoed by the Labour Party (PvdA), who not only noted that ICT vulnerability had "not received adequate priority" by the Dutch government, but also, in a similar discursive manner as previous governmental policy documents, linked its importance to numerous topics as the increasing rate of cyber crime, the potential for societal disruption, and even terrorism.[213] However, the most surprising reversal came from the Socialist Party (SP). Referring the DigiNotar incident as "the biggest ICT problem in Dutch history" and a "digital doomsday scenario", the SP, having previously questioned the usefulness of investing both €90 million in cybersecurity for the military and the creation of a National Cybersecurity Center,[214] emphatically advocated for spending more money on cybersecurity through the formation of a "digital fire brigade" consisting of various digital experts.[215] This political discourse was further compounded by the increasing pressure emanating from a wide range of societal actors, in particularly the media. In the month following the incident, the Dutch Technology Website Webworld increased pressure on the Dutch government to address its difficulties in cybersecurity, by declaring October "the month of the privacy leak" or "Lektober" (a term which also found its way into the DigiNotar parliamentary debate).

During this month, the website vowed to expose a new privacy leak within either a public or corporate network every workday, prompting very concerned response from the

[211] See for example: Kamerstukken II, 2010/2011, 28 684, nr. 323; Kamerstukken II, 30 821, nr. 12
[212] Handelingen II, 2011/2012, 'DigiNotar Debat', vergaderingnummer 12, 3
[213] Handelingen II, 2011/2012, 'DigiNotar Debat', vergaderingnummer 12, 2
[214] Kamerstukken II, 2010/2011, 28 684, nr. 323, 6.
[215] Handelingen II, 2011/2012, 'DigiNotar Debat', vergaderingnummer 12, 1 – 4.

national association of Dutch municipalities.[216] Varying degrees of hyper-securitizations also featured prominently in international and national media. Key examples include an interview by the *New York Times* of computer security expert Calum MacLeod, the European director of internet security company Venafi, who likened the DigiNotar incident to a natural disaster, calling the incident "the Dutch equivalent of Hurricane Irene".[217] The *Telegraaf*, the most widely circulated newspaper in the Netherlands, called the incident "an act of cyber warfare"[218], with the political magazine Elsevier following suit, referring to the incident as "the first successful cyber-attack on Europe".[219]

The DigiNotar incident significantly affected government discourse on cybersecurity. Here, references to the incident featured prominently in the framing of digital information as essential for "the functioning of Dutch society"[220] as well as to "the functioning of the economy and the Dutch government".[221] For example, in a letter to the House of Representatives, Ivo Opstelten (VVD), the Minister of Justice and Security framed the issue as a pronounced example of the dangers of ICT failure, stating that "…in September 2011, the events at DigiNotar underlined to what extent the government and, by extension the whole of society, has become dependent on the undisturbed functioning of information and communication technology (ICT)".[222] The DigiNotar incident also instilled a new and greater sense of urgency amongst the Dutch government as noted at the general consultations on cybersecurity and the security of government websites, where the Minister of the Interior and Kingdom Relations Spies, noted that "we have all experienced the past few days how dependent we have become modern technology, ICT" and that "the DigiNotar situation, gave the government quite a wake- up call".[223]

By exposing the vulnerability of ICT systems, the incident had, for the first time, displayed the true implications of a failure of cybersecurity. As such, it underlined the need for increased technological knowledge and a restructuring of existing, as well as the

[216] '"Lektober": elke dag een ander privacylek', De Volkskrant, 3 October 2011,[http://www.volkskrant.nl/media/-lektober-elke-dag-een-ander-privacylek~a2944061/ accessed online 3 December 2015].
[217] 'Hacking in Netherlands points to weak spot in web security', New York Times, 12 September 2011, [http://www.nytimes.com/2011/09/13/technology/hacking-in-netherlands-points-to-weak-spot-in-web-security.html?_r=0 accessed online 3 December 2015].
[218] Alfred Monterie, 'Iraans hacken is oorlogsdaad', De Telegraaf, 5 September 2011, [http://www.telegraaf.nl/digitaal/article20819243.ece accessed online 26 December 2015].
[219] Afshin Ellian, 'De Iraanse cyberoorlog tegen Nederland', Elsevier, 5 September 2011, [http://www.elsevier.nl/Algemeen/blogs/2011/9/De-Iraanse-cyberoorlog-tegen-Nederland-ELSEVIER315601W/ accessed online 26 December 2015].
[220] Kamerstukken II, 2012/2013, 26 643, nr. 189, 1.
[221] Kamerstukken II, 2012/2013, 26 643, nr. 258, 1.
[222] Kamerstukken II, 2012/2013, 26 643, nr. 258, 1.
[223] Kamerstukken II, 2012/2013, 26 643, nr. 240, 21–22.

introduction of newer disaster and security strategies to deal with the implications cyber-attacks.[224] As a result of the breach, the Dutch government initiated a specialized three track cybersecurity approach based on (1) increasing the resilience against (deliberate) infringements (2) increasing resilience to unexpected success infringements and (3) structural system improvements on a global level. Key to this approach was the acceleration of multiple initiatives which had already been set up in previous years. These included many of the already ongoing initiatives such as the Cybersecurity Threat Analysis, the creation of the National Cybersecurity Center (NCSC) and the introduction of the E-ID (electronic identity), which were to be enhanced and continued following the newly gained insights as a result of the DigiNotar incident.[225]

5.10 (Cyber) Securitization – Sub-conclusion IV

In terms of a securitizing discourse, the subsequent cybersecurity initiatives announced by the Dutch government signified the influence of the Project on National Security on cybersecurity discourse. Indeed, the previously employed broad definition of national security ensured the seamless movement of cybersecurity between individual and collective security, between public authorities and private institutions, and between economic and political-military security, tying an ever increasing number of referent objects together. For example, echoing the now familiar discourse on cybersecurity, the necessity for an acceleration of such policy initiatives was underscored through a discursive constitution of the safety of the ‘‘network’’ as being vital to the referent objects of the ‘‘state’’ and ‘‘society”. Although evident in previous policy documents, such iterative statements were heavily reliant on ICT now gained new meaning and urgency. Key cybersecurity policy documents, such as the Cybersecurity Assessment, released shortly after the incident on December 2011, started to progressively make references to the DigiNotar incident, which was framed as being “a poignant example that ICT is vulnerable, that ICT can be abused and that our society is now very dependent on the proper functioning of ICT”.[226] This was again reiterated in the Cybersecurity Assessment of 2012, where the severity and scope of the DigiNotar incident was underlined through the statement that an attack on a third party can not only lead to serious consequences for its own operations, but also “exceed the organization, so that a

[224] Nicole van der Meulen, ‘DigiNotar: Dissecting the First Dutch Digital Disaster’, *Journal of Strategic Security* 6 (2013), 58.
[225] Kamerstukken II, 2010/2011, 26 643, nr. 189.
[226] Ministerie van Veiligheid en Justitie, Cybersecurity Beeld (2011) 11.

sector or, in the case of DigiNotar, the home country is affected".[227] This was also affirmed in the National Cybersecurity Strategy in 2014 which, through reference to the DigiNotar incident, stated that national security could jeopardized through "a large-scale cyber-attack on one or more private organizations".[228] This framing, which emphatically underlined the responsibility of the business sector in safeguarding national security, became a recurring feature of cybersecurity discourse, where it was increasingly defined as a "serious subject in which significant interests lie, which needed to be defended". [229] Moreover, these interests were not limited to information but extended to "all kinds of services that are vital for the functioning of Dutch society"[230] which, if subject to digital incidents such as DigiNotar, could lead to "social instability" and therefore "affect national security".[231]

This expansion of responsibility did, however, not only limit itself to the business sector. Following the incident, an agreement was established between all involved parties that some form of individual responsibility of citizens should become a necessary feature of cybersecurity policy.[232] Although such responsibility had previously been established with the publication of the first National Cybersecurity Strategy in 2011, this subject and the general vision behind cybersecurity policy, was still a matter of debate, with notable concerns being raised in the House of Representatives relating to the extent of the "self-reliance" and "personal responsibility" of the citizen.[233] In particular, such discussions pertained to the extent to which such responsibility was applicable, as a clear delineation between the responsibilities of the government and those of the Dutch citizen had not been established. Consequently, the government was continually requested to clarify the government's position in this matter, a request which was answered by the Minister of Justice and Security Ivo Opstelten (VVD) through a statement that "citizens and business owners are primarily responsible for their own safety and the government adds to this".[234] To relay message, it was, according to the Minister, crucial that "a broader debate within society was to be held about the fact that the first responsibility lies with the people themselves".[235]

In the period following the DigiNotar incident, a noticeable shift in cybersecurity discourse surrounding such responsibilities, and indeed the degree to which citizens

[227] Ministerie van Veiligheid en Justitie, Cybersecurity Beeld (2012) 30.
[228] Ministerie van Veiligheid en Justitie, Nationale Cybersecurity Strategie (2014), 23.
[229] Ministerie van Veiligheid en Justitie, Cybersecurity Beeld (2012) 8.
[230] Ministerie van Veiligheid en Justitie, Cybersecurity Beeld (2012) 8.
[231] Ministerie van Veiligheid en Justitie, Cybersecurity Beeld (2013) 98.
[232] Kamerstukken II, 2010/2011, 28 684, nr. 323.
[233] Kamerstukken II, 2010/2011, 28 684, nr. 323, 5–6.
[234] Kamerstukken II, 2010/2011, 28 684, nr. 323, 17
[235] Kamerstukken II, 2010/2011, 28 684, nr. 323, 17.

constituted a liability, occurred. Adopting a simultaneously educational and securitizing discourse, cybersecurity was constituted as an area in which "everyone should take his or her responsibility" an active policy was initiated towards securing the individual's partnership and compliance in protecting network security.[236] One manner in which this occurred was through so-called "*cyber awareness*" campaigns, such as Alert Online in 2012, which were aimed to create awareness amongst Dutch citizens regarding "the risks of using the internet and smartphones."[237] Developed by host of government and business actors, including such heavy security-orientated institutions as the National Coordinator for Counter-terrorism, the National Cybersecurity Center, and the Dutch civilian intelligence service, this campaign warned citizens to make "very deliberate choices when using, purchasing and maintaining ICT, both at home and at work" as "one click of the mouse can accidentally infect an entire network, or expose all your private and customer data to public view".[238] A similar discourse unfolded in policy documents, where it was implied that to act safely in the digital domain, it was important for citizens to actively participate in cybersecurity.[239] In the National Cybersecurity Strategy released in 2014, this principle was officially referred to as the "*competent citizen*", which expressed that "citizens are expected to apply some form of basic 'cyber hygiene' and skills in using ICT, like surfing the web. This includes carefully using personal information, installing updates, using good passwords and balancing functionality and cybersecurity".[240]

With regard to technifications, the DigiNotar incident also granted extensive legitimacy to experts. Lacking the technical expertise itself, the Dutch government contracted a company specialized in computer and network security, Fox-IT, which was to conduct an in-depth investigation into the computer systems of DigiNotar. The release of the preliminary report of this investigation on 5 September 2011 revealed that all servers were compromised, even those generating government certificates. This alarmed the Dutch government, which had originally only assumed that only sections of DigiNotar had been compromised. As a result, the potential damage caused by the breach was underestimated. The conclusions of Fox-IT had a significant impact on the government's handling of the breach, as its findings directly compelled the government to officially revoke the trust in all certificates issued by

[236] Kamerstukken II, 2011/2012, 30 821, nr. 16.
[237] 'About Alert Online', Alertonline, [https://www.alertonline.nl/over_alert_online/About-Alert-Online/index.aspx accessed online 15 December 2015].
[238] 'About Alert Online', Alertonline.
[239] Ministerie van Veiligheid en Justitie, Nationale Cybersecurity Strategie (2014) 19.
[240] Ministerie van Veiligheid en Justitie, Nationale Cybersecurity Strategie (2014) 20.

DigiNotar.[241] With the DigiNotar breach dominating the media, Fox-IT, through its investigative role, was immediately cast into center of attention, granting it a privileged role as the authority to speak about cybersecurity. Appearing in a host of national newspapers and television shows to talk about cybersecurity, its founder and CEO, Ronald Prins, was labeled as "the most powerful nerd in the Netherlands".[242] Prins' prominent presence in such media outlets established him as central figure and leading authority in matters of cybersecurity.[243] Fox-IT is currently one the most consulted cybersecurity company in the Netherlands, fulfilling a major role in the prevention, investigation, and reduction of the most serious cyber threats for government, defense, police and vital infrastructure. In addition, it now develops encryption and various other cyber tools for the defense sector.[244]

In the aftermath of the DigiNotar incident, the prefix of cyber once again proliferated throughout security discourse, being added to a host threats to signify their connection to ICT. For example, within the Dutch military intelligence (MIVD) and general intelligence (AIVD) agencies, warnings were increasingly issued regarding risks and threats with a "technological component" which can occur at "an unexpectedly rapid pace" and in "an unpredictable manner" and can have "a profound impact on national security."[245] Within the AIVD, one such threat with a technological component identified was *Cyber Jihadism* which was seen as a potential cyber threat to national security.[246] This finding was supported in the national cybersecurity assessment in 2013, which found that although not yet fully fledged, jihadists could pose "a cyber-threat to national security".[247] However, it appeared as though that even without the addition of cyber, ICT threats could be denoted, as the Internet also gained a new variant dubbed the "Jihadist Internet", which was defined as "the Nursery of Modern Jihad"[248] In the annual report of the MIVD, the topic of 'cyber' was added to such existing topics as proliferation, international terrorism and espionage.[249] During this period, cybersecurity also

[241] van der Meulen, 'DigiNotar', 49.
[242]Lex Boon, 'De Machtigste Nerd van Nederland', NRC Handelsblad, 5 September 2011, [http://www.nrc.nl/nieuws/2011/09/05/de-machtigste-nerd-van-nederland accessed online 25 December 2015].
[243] In the following years, Ronald Prins, through his role as expert would often advocate in favor of more cybersecurity, in a move which was defined by a journalist as a 'threat inflation': Maurits Martijn, 'Digitale Dreigingsinflatie', *De Correspondent*, 8 October2013, [https://decorrespondent.nl/125/Digitale-dreigingsinflatie/3844500-4c289220 accessed online 20 December 2015].
[244] Pim van der Beek, 'Defensie kiest Fox-IT voor encryptiebeheer', Computable, 4 March 2014, [https://www.computable.nl/artikel/nieuws/security/5019789/1276896/defensie-kiest-foxit-voor-encryptiebeheer.html accessed online 12 December 2015].
[245] Algemene Inlichtingen en Veiligheidsdienst, Jaarverslag (2011), 6.
[246] Algemene Inlichtingen en Veiligheidsdienst, Jaarverslag (2012), 26.
[247] Ministerie van Veiligheid en Justitie, Cybersecurity Beeld (2013), 22.
[248] Algemene Inlichtingen en Veiligheidsdienst, *Het jihadistisch internet Kraamkamer van de hedendaagse jihad* (2012).
[249] Militaire Inlichtingen en Veiligheidsdienst, *Jaarverslag* (2011)

gained new importance in the field of national defense, as the then incumbent Minister of Defense, J.S.J. Hillen, constituted 'cyber' as being, in addition to land, air, sea and space, the "fifth domain" for military action.[250] The Minister of Defense also announced substantial investments in cybersecurity which were aimed at strengthen existing, as well as develop, new cyber capacities.[251] These notable developments, which arguably mark the inception of some form of militarization of cyberspace in the Netherlands, also included discussions on 'cyber' warfare, which was defined as increasingly worrying issue for Dutch government due to the "increasing threat against national interests in the digital domain and the increase in the number of (complex) digital attacks".[252]

As the first digital disaster in the history of the Netherlands, the DigiNotar incident solidified an enlarging role for cybersecurity as increasingly important security issue in the national security agenda of Netherlands. Its substantial effects served as an important wake up call to virtually all politicians to the dangers they had so vehemently envisioned during many consecutive years of policymaking in the field of computer security, but seemingly not effectively prevented. By exposing many weaknesses which needed to be addressed in order to reduce the probability of future risk, it underlined the need for improved mitigation strategies, which were adopted at an accelerated pace compared to previous periods of policymaking. This acceleration of government initiatives, combined with a crucial impetus in cooperation amongst different government parties, advanced many of the cybersecurity developments of the previous years, developing them into a fully comprehensive and coherent modern cybersecurity framework as it currently exists in the Netherlands.[253]

[250] Kamerstukken II, 2011/2012, 33 321, nr. 1, 1.
[251] Kamerstukken II, 2011/2012, 33 321, nr. 1, 3.
[252] Rijksoverheid, kabinetsreactie op het AIV/CAVV-advies Digitale Oorlogvoering (2012)
[253] van der Meulen, 'DigiNotar', 57.

6 Conclusion

It has been the ambition of this thesis to chart the discursive constitution of computer security in security policymaking in the Netherlands and analyze how this constitution has corresponded to the cyber securitization framework. This analysis has focused on the complexities of various articulations of computer security throughout several decades of Dutch security policymaking, ranging from computer security's first emergence on the security agenda, to its modern embodiment in the coherent and comprehensive Dutch framework of cybersecurity.

In relation to the first part of the stated research question of this thesis regarding how computer security has been discursively constructed within security policymaking in the Netherlands, a notable development in articulations can be observed. Prompted by rapid technological advancements in the field of computer technology, computer security first emerged on the security agenda in the mid-1980s, when questions arose as to whether or not existing traditional criminal provisions still provided adequate protection under the law. This introduced new security concerns, in particular relating to the new capabilities of criminal acts using computers to impact traditional objects, and to protect incorporeal objects such as computer software. This was reflected in articulations of computer security which, although to a minor extent viewed as being potentially threatening to society, was framed primarily terms of a criminal/legal/technical issue. This framing was used as a justification for the need for new legislation, leading to the enactment of the first piece of legislation relating to the security of computers, the Computer Crime Act of 1993.

In the years following the enactment of this legislation, the discursive constitution of computer security was confronted by new, competing articulation of (in)security. Now encapsulated in the larger framework of ICT, computer security, through the potentially devastating effects of Y2K, became conceptualized as a problem of (system) vulnerabilities — the singling out of particular systems and framing of their functions as being 'vital' or 'critical' due to the fact that their unavailability holds the potential for a political and social crisis. Framed as vital to the proper functioning of Dutch society, discourse on the matter now reiteratively stressed the implications of network break-downs for other referent objects such as ''society'', "the state", or ''the economy". This constitution of computer security became particularly prevalent in the area regarding the protection of critical infrastructure, where it gained increasing political importance through such connections to these collective referent objects.

With the implementation of the new *all-hazard approach* to (national)security policymaking in 2006, the discursive constitution of computer security moved into the highest arena of security of national security. Prompted by means of an almost all-encompassing definition of national security, computer security became commonly referred to as *cybersecurity*, gaining a prominent place on the security agenda through its articulation as being vital to national security. This resulted in the formulation of a wide array of new security policies and extensive strategy documents, each dealing with this new domain. However, this articulation of computer security also remained the subject of continual political debate in the House of Representatives, where its subsequent policies were repeatedly challenged.

The occurrence of the DigiNotar breach provided a critical impetus of urgency, necessity, to interpretations of cybersecurity. As its consequences became apparent, the aforementioned contestation of cybersecurity policies remarkably diminished. Cybersecurity now assumed an expanding role on the political agenda and although some questions as to the normative desirability of certain cybersecurity remained, its articulation as constituting something which affects all layers of society, ranging from government, to the private entities, to the individual citizen became solidified within Dutch security policymaking.

Focusing on the second part of the research question, pertaining to the degree to which this discursive constitution has corresponded to the cyber securitization framework, the aforementioned changes in articulations of computer security in Dutch security policymaking present an observable amount of parallels with the three grammatical modalities of hyper-securitizations, everyday security practices and technifications.

With reference to the first grammatical modality of hyper-securitizations, a gradual increase is evident. During its initial emergence onto the security agenda, computer security, although framed as a potential threat to Dutch society, did not initially involve the identification of large-scale instantaneous cascading disaster scenarios. However, a noticeable changed occurred during the advent of Y2K. Computer security, now conceptualized as a problem of (system) vulnerabilities, became increasingly characterized by a discursive emphasis on the existence of a great chain dependency of collective referent objects. This dependency enabled the emergence of hyper-securitizations, as the vital importance of the proper of functioning of ICT was framed as holding the potential for large-scale political and societal crisis. With the reimagining of (national)security policymaking in 2006, such hyper-securitizations became a central feature of securitizing discourse in Dutch cybersecurity policymaking, as an ever enlarging number of referent objects were discursively framed as

being essentially inter-connected through ICT. As a result, failure of ICT constituted a significant security issue, as it would result in a cascading disaster scenario affecting all layers of society. This view was further solidified in the wake of the DigiNotar incident.

With regard to the second grammatical modality of everyday security practices, a similar incremental increase in discourse is also evident. Indeed, the initial framing of computer security as a criminal/legal/technical issue involved no discernible effort to secure the individual's partnership and compliance in protecting network security. The limited occurrence of computer crime and abuse, combined with a lack of familiarity and unavailability of computers to many, effectively simply meant that no linkage to experiences familiar from everyday life could be made. Nonetheless, in the following years, everyday security practices gradually emerged as a significant component in computer security discourse. Elements of this grammatical modality, albeit in a very minor form, first emerged during the Y2K, where mitigating efforts often included active involvement of a wide range of societal actors who were informed of the looming danger of large scale ICT failure. This was often done by linking such dangers to experiences familiar to everyday life, through a range of risk scenario's which were articulated as affecting various societal sectors. However, here only a minor role was attributed to the individual, as the mitigation of the Millennium Bug was primarily seen as a task for government and the business community (for which the consequences were seen as being the most significant). The adoption of the *all-hazard approach* to (national)security policymaking marked the advent of an articulation of computer security in which an increasingly active role for the individual as an important partner in the security of the network was conceptualized. This role was further expanded in the aftermath of the DigiNotar incident when the individual also became constituted as a potential liability, or even a threat, to the security of the computers/network.

The third and final grammatical modality of technifications also experienced a remarkable development within articulations of computer security. Starting from the initial policymaking process of the Computer Crime Act, a variety of experts has consecutively played an integral role in the discursive constitution of computer security in security policymaking. Appearing in discourse during Y2K through the prominent role the Millennium Platform and, later years, through the formation of expert groups and the contracting of external cybersecurity companies, Dutch computer security policy is characterized by continuous constitution of an epistemic community of authoritative experts which are granted political legitimacy through the Dutch government actively seeking their involvement. Increasingly, and facilitated by varying degrees of media attention, such experts have

acquired a privileged role as an authority to speak to both to the broader public, as well as to the government, about cybersecurity. As such, these experts have, to a certain extent, effectively managed to become securitizing actors which, through their ability to distinguishing themselves from the politicking of politicians and other political actors, have been able to facilitate the framing of cybersecurity as politically neutral or even unquestionably normatively desirable.

In an age in which ongoing technological advancement is progressively influencing security policies, it is vital that more understanding is gained regarding the specific processes which underline their formulation. When set against the historical background of cyber security policymaking in the Netherlands, a more detailed picture is formed in relation to the main empirical claim of the cyber securitization framework regarding the emergence of new a conception of computer security which is articulated by specific constellation of securitizing actors and which differentiates itself from a technical conception through a linkage to national security. While initially only corresponding in a weak manner to the cyber securitization framework articulations of computer security within Dutch security policymaking have gradually seen an increasing prevalence of the three grammatical modalities. Throughout several decades, each articulation has imbued computer security with new meaning, which correspondingly affected the manners in which computer security could be framed. By setting the boundaries of its reach further each time, this has gradually increased the extent to which such articulations corresponded to the cyber securitization framework through the three grammatical modalities. Consequently, a large extent of interconnectedness between such articulations, and this theoretical framework can be discerned.

That being said, it is worth nothing that deviations are also evident. Here, the most notable discrepancy with the theoretical framework is formed by the grammatical modality of hyper-securitizations, which is marked by a significant lack of its constituting element of historical analogies. Although theorized as an important part of this grammatical modality, they are practically inexistent within Dutch articulations of computer security. Indeed, when analyzing the entirety of Dutch debates, deliberations and policy documents on cybersecurity, not a single historical analogy can be detected. Although admittedly speculative, one possible explanation for this absence perhaps lies in the socio-cultural history of Dutch political system and the specific manner in which political discourse in the Netherlands can be characterized. Another, more practical, potential explanation lies perhaps in the simple fact that Dutch history simply does not present opportunity for such grandiose historical analogies as an “electronic Pearl Harbor”. Perhaps the only historical analogy which could lend itself to

such similar framing is the Watersnoodramp of 1953, a large-scale flooding disaster in the Netherlands, which is still considered the biggest disaster in Dutch history. However, such a framing is likely a bit too heavy-handed in the context of cybersecurity for most politicians and policymakers, let alone the general public. Nonetheless, whatever the particular explanation may be, this element of the hyper-securitizing modality has remained absent from any sort of discourse in the Netherlands on cybersecurity.

Notwithstanding such deviation, the cyber securitization framework does present an invaluable empirical tool. Understanding the cyber sector of security as working from a discursive, Copenhagen School-inspired perspective, that is, as a distinct sector with a particular constellation of threats and referent objects, allows for an analysis of the ways in which inter-subjective representations of perceived digital threats become discursively constituted as an issue of national security. Indeed, the interplay of the three grammatical modalities of hyper-securitizations, everyday security practices, and technifications, provide a compelling insight into the extent to which multi-discursivity has linked referent objects, threats, and securitizing actors together. Over the course of several decades, this has effectively constituted cybersecurity as something in which a great chain dependency exists, which affects all layers of society, ranging from government, to the private entities, to the individual citizen. Given the power that emanates from such a securitizing discourse, the question that asks whether security is desirable shifts to how it can be effectively contested. Since when it comes to the digital sphere, it is hard to escape the fact that everyone is vulnerable.

Discussion

For purposes of scientific thoroughness, this thesis acknowledges the existence of a number of limitations to its findings. The first of these is that, in a similar fashion as Hansen and Nissenbaum's seminal paper, this thesis is based on a single case study analysis. Naturally, this limitation introduces several concerns, including the inter-related issues of external validity, methodological rigor and subjectivity of the researcher. The second of these limitations is located within the more specific overlaying theory of securitization. Notwithstanding the criticism already discussed in a previous section of this thesis, Securitization Theory remains a theory which is essentially split between different factions, each with their own view of how securitization research should be conducted. While too numerous to mention, it suffices to note that the Copenhagen School's interpretation of securitization, which has been employed in this thesis, still faces a number of important empirical challenges, including inherent tensions in its main theoretical assumptions and the validity of its claims of a universal logic of security. Through its inter-related theoretical connections, this also affects the cyber securitization framework, which raises questions as to the applicability of this framework in different contexts. The third limitation pertains to the employed methodology of discourse analysis. Here, a similar observation can be made as with Securitization Theory, as discourse analysis constitutes a methodology which is inherently split between different approaches, each with its own merits and demerits.

It is in relation to such limitations into account, several avenues for further research can be discerned. Limiting these to those specifically relevant to the scope and goal this thesis, further empirical testing of the cyber securitization framework, especially in different contexts, or comparatively are amongst the first which come to mind. This also applies in relation to the specifics grammatical modalities of the cyber securitization framework themselves which, in a comparative perspective between this thesis and Hansen and Nissenbaum's paper reveals that their specific constitution and prevalence varies across cases analyzed. As such, the specifics of these modalities in different contexts warrants further research.

References

Government/Parliamentary Sources:

Algemene Inlichtingen en Veiligheidsdienst – all cited sources:

Het jihadistisch internet Kraamkamer van de hedendaagse jihad (2012).

Jaarverslag (2011)

Jaarverslag (2012)

Commissie Computercriminaliteit – all cited sources:

Informatietechniek en Strafrecht (1987).

European Union – all cited sources:

Council of Europe, Recommendation, No. R (89) 9.

House of Representatives (Tweede Kamer der Staten-Generaal) – all cited sources:

(all sources accessed through https://zoek.officielebekendmakingen.nl/)

Handelingen (listed chronologically):

Handelingen I, 1980/1981, 25 November 1980

Handelingen II, 1995/1996, nr. 1647.

Handelingen II, 1997/1998, Nr. 49, 3767-3769.

Handelingen II, 2009/2010, nr. 34, 3259.

Handelingen II, 2011/2012, nr 12, 99.

Kamerstukken (listed per dossier):

Dossier 21 504 - Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering en enkele andere wetten ter verruiming van de mogelijkheden tot toepassing van de maatregel van ontneming van wederrechtelijk verkregen voordeel en andere vermogenssancties

Kamerstukken II, 1989/1990, 21 504, nr. 3.

Dossier 21 551 - Wijziging van het Wetboek van Strafrecht en van het Wetboek van Strafvordering in verband met de voortschrijdende toepassing van informatietechniek (Wet computercriminaliteit):

Kamerstukken II, 1989/1990, 21 551, nr. 2; Kamerstukken II, 1989-1990, 21 551, nr. 3.

Dossier 24 175 - Beheersing informatiebeveiliging:

Kamerstukken II, 1994/1995, 24 175, nr. 2.

Dossier 24 565 - Elektronische snelwegen:

Kamerstukken II, 1997/1998, 24 565, nr. 7

Dossier 25 000 - Vaststelling van de begroting van de uitgaven en de ontvangsten van het Ministerie van Binnenlandse Zaken (VII) voor het jaar 1997:

Kamerstukken II, 1996/1997, 25 000-VII, nr. 41.

Dossier 25 674 - Millenniumvraagstuk:

Kamerstukken II, 1997/1998, 25 674, nr. 15; Kamerstukken II, 1998/1999, 25 674, nr. 34.

Dossier 25 894 - Oprichting Stichting Millennium Platform:

Kamerstukken II, 1997/1998, 25 894, nr. 261

Dossier 26 643 - Informatie- en communicatietechnologie:

Kamerstukken II, 1998/1999, 26 643, nr. 1; Kamerstukken II 2000/2001, 26 643, nr. 20.

Kamerstukken II, 2000/2001, 26 643, nr. 30; Kamerstukken II, 2002/2003, 26 643, nr. 39.

Kamerstukken II, 2003/2004, 26 643, nr. 47; Kamerstukken II, 2007/2008, 26 643, nr. 103.

Kamerstukken II, 2010/2011, 26 643, nr. 174; Kamerstukken II, 2010/2011, 26 643, nr. 189.

Kamerstukken II, 2012/2013, 26 643, nr. 240; Kamerstukken II, 2012/2013, 26 643, nr. 189.

Kamerstukken II, 2012/2013, 26 643, nr. 240; Kamerstukken II, 2012/2013, 26 643, nr. 258.

Dossier 28 648 - Naar een veiliger samenleving:

Kamerstukken II, 2010/2011, 28 684, nr. 323

Dossier 30 821 - Nationale Veiligheid:

Kamerstukken II, 2006/2007, 30 821, nr. 1; Kamerstukken II, 2010/2011, 30 821, nr. 12.

Kamerstukken II, 2011/2012, 30 821, nr. 16.

Dossier 33 321 - Defensie Cyber Strategie:

Kamerstukken II, 2011/2012, 33 321, nr. 1.

Dossier 32 123 X - Vaststelling van de begrotingsstaten van het Ministerie van Defensie (X) voor het jaar 2010:

Kamerstukken II, 2009/2010, 32 123-X, nr. 66.

Militiaire Inlichtingen en Veiligheidsdienst – all cited sources:

Jaarverslag (2009).

Jaarverslag (2011)

Ministerie van Veiligheid en Justitie – all cited sources

Computercriminaliteit (1987)

Cybersecurity Beeld (2011)

Cybersecurity Beeld (2012)

Cybersecurity Beeld (2013)

Nationale Cybersecurity Strategie (2011)

Nationale Cybersecurity Strategie (2014)

Ministerie van Verkeer en Waterstaat – all cited sources*:*

Interactieve videotex in Nederland Standpunt van de regering met betrekking tot het Eindrapport van de Stuurgroep ter begeleiding van de PTT-praktijkproef met viewdata (1984)

North Atlantic Treaty Organization – all cited sources

Strategic Concept (2010)

Rijksoverheid – all cited sources

Rapport Herijking ICT Veiligheidsbeleid (2006)

Strategie Nationale Veiligheid (2007)

Nationale Risicobeoordeling (2008)

Nationale Risicobeoordeling (2009)

Nationaal Trendrapport Cybercrime en Digitale Veiligheid (2010)

Kabinetsreactie op het AIV/CAVV-advies Digitale Oorlogvoering (2012)

Secondary Sources

Arquilla, John and Ronfeldt, David. 'Cyberwar is Coming!', *Comparative Strategy* 12 (1993), 141-165.

Arquilla, John and Ronfeldt, David. *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, 2001).

Bada, Maria and Sasse, Angela. 'Cybersecurity awareness campaigns: Why do they fail to change behaviour?', Global Cyber Security Centre (2014), [https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Awareness%20CampaignsDraftWorkingPaper.pdf accessed online 23 December 2015].

Balzacq, Theirry. 'The Three Faces of Securitization: Political Agency, Audience and Context', *European Journal of International Relations* 11 (2005), 171-201.

Balzacq, Thierry. *Securitization Theory: How Security Problems Emerge and Dissolve* (London, 2011).

Bendrath, Ralf. 'The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection', *Information & Security* 7 (2001), 80-103.

Buzan, Barry. *The United States and the Great Powers: World Politics in the Twenty-first Century* (Cambridge, 2004).

Buzan, Barry; Waever, Ole; and de Wilde, Jaap. *Security: A New Framework for Analysis* (Boulder, 1997).

Cavelty, Myriam Dunn. 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', *International Studies Review* 15 (2013), 105-122.

Cavelty, Myriam Dunn. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (London, 2008).

Corry, Olaf. 'Securitzation and Riskization: Two Grammars of Security', working paper prepared for Standing Group on International Relations, 7th Pan-European International Relations Conference, [http://www.eisa-net.org/be-bruga/eisa/files/events/stockholm/Risk%20society%20and%20securitization%20theory%20SGIR%20paper.pdf, accessed online 28 December 2015].

Der Derian, James. *Antidiplomacy: Spies, Terror, Speed, and War* (Oxford, 1992).

Eriksson, Johan. 'Cyberplagues, IT, and Security: Threat Politics in the Information Age', *Journal of Contingencies and Crisis Management 9* (2001), 211-222.

Greenwood, Royston; Oliver, Christine; Suddaby, Roy; and Sahlin-Andersson, Kerstin. *The Sage Handbook of Organisational Institutionalism* (Thousand Oaks, 2008).

Gutteling, Jan and Kuttschreuter, Margot. 'The role of experise in risk communication: laypeople's and expert's perception of the Millennium Bug risk in The Netherlands', *Journal of Risk Research* 5 (2002), 35-43.

Hansen, Lene and Nissenbaum, Helen. 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly* 53 (2009), 1155-1175.

Hansen, Lene. 'Theorizing the Image for Security Studies: Visual Securitization and the Muhammed Cartoon Crisis', *European Journal of International Relations* 17 (2011), 51-74.

Hansen, Lene. *Security as Practice: Discourse Analysis and the Bosnian War* (Oxford, 2006).

Huysmans, Jef. *The Politics of Insecurity: Fear, Migration, and Asylum in the EU* (London, 2007).

Koops, Bert-Jan. 'Cybercrime Legislation in the Netherlands', *Electronic Journal of Comparative Law* 14 (2010), 595-633.

Latham, Robert (ed.). *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security* (New York, 2003).

Laustsen, Carsten Bagge and Waever, Ole. 'In Defence of Religion: Sacred Referent Objects for Securitization', *Journal of International Studies* 29 (2000), 705-739.

Lawson, Sean. 'Putting the "War" in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States', *First Monday* 17 (2012), [http://www.firstmonday.org/ojs/index.php/fm/article/view/3848/3270 accessed online 15 December 2015].

Lipschutz, Ronnie (ed.). *On Security* (New York, 1955).

Mollema, Kornelis, *Computercriminaliteit: de wetgeving, gevolgen voor bedrijven en de accountant* (Deventer 1993).

Muller, Erwin; Rosenthal, Uri; Helsloot, Ira; and van Dijkman, Erwin. *Crisis: Studie over crisis en crisisbeheersing* (Deventer, 2009).

Muller, Erwin; van der Leun, Joanne; van Calster, Patrick. *Criminaliteit en criminaliteitsbestrijding in Nederland* (Alphen aan de Rijn, 2010).

Nissenbaum, Helen. 'Where Computer Security Meets National Security', *Ethics and Information Technology* 7 (2005), 61-73.

Parker, Ian. *Discourse Dynamics: Critical Analysis for Social and Individual Psychology* (London, 1992).

Peoples, Columba and Vaughan-Williams, Nick. *Critical Security Studies: An Introduction* (London, 2010).

Phillipps, Nelson and Hardy, Cynthia. *Discourse Analysis: Investigating Processes of Social Construction* (Thousand Oaks, 2002).

Phillips, Nelson and Brown, John L. 'Analyzing Communication In and Around Organizations -- A Critical Hermeneutic Approach', *Academy of Management Journal* 36 (1993), 1547-1576.

Phillips, Nelson; Lawrence, Thomas; and Hardy, Cynthia. 'Discourse and Institutions', *Academy of Management Review* 29 (2004), 635-652.

Salter, Mark. 'Securitization and Desecuritization: Dramaturgical Analysis and the Canadian Aviation Transport Security Authority', Journal of International Relations and Development 11 (2008), 321-349.

Shapiro, Michael. *The Politics of Representation: Writing Practices in Biography, Photography, and Policy Analysis* (Madison, 1988).

Sieber, Ulrich. 'Legal Aspects of Computer-Related Crime in the Information Security', report generated for the European Commission (1998), 24-26, [http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf accessed online 12 December 2015].

Stritzel, Holger. 'Towards a Theory of Securitization: Copenhagen and Beyond', *European Journal of International Relations* 13 (2007), 357-385.

van der Meulen, Nicole. 'DigiNotar: Dissecting the First Dutch Digital Disaster', *Journal of Strategic Security* 6 (2013), 46-58.

van Dijk, Teun. *Discourse as Structure and Process* (Thousand Oaks, 1997).

van Perzie, Mischa. *ICT en Recht* (Wolters Kluwer, 2008).

Veraart, Frank. 'De domesticatie van de computer in Nederland, 1975-1990', *Tijfschrift voor Wetenschaps-en Universiteitsgeschiedenis* 1 (2008), 145-164.

Wiemans, F. (ed.). *Commentaren op het wetsvoorstel computenline rcriminaliteit* (Maastricht, 1991).

Wiemans, F. *Onderzoek van gegevens in geautomatiseerde werken* (Nijmegen, 2004).

Williams, Michael C. 'Words, Images, Enemies: Securitization and International Politics', *International Studies Quarterly* 47 (2003), 511-532.