CONSENSUAL HALLUCINATIONS

THE POLITICS OF IDENTITY IN DUTCH CYBER SECURITY POLICY

by

HANS JOZEF ADRIAAN MARIE SIMONS

Student number: 0614122

Supervisor: Dr. G.C. van der Kamp-Alons

A Thesis Submitted in

Partial Fulfillment of the

Requirements for the Degree of

Master of Science

in Political Science

at

Radboud University Nijmegen

July 9, 2014

ABSTRACT

Cyber security is currently at the top of the Dutch political agenda, and regarded as the newest domain for military operations. Threats in and through cyberspace are considered to be threats against national security and the functioning of Dutch society. The depoliticized character of the language used in the cyber security debate suggests that this is the only acceptable way to talk about this matter; that is to say, the debate appears to be securitized. Still, while securitization theory can reveal how a (perceived) threat can be securitized through discourse, it says little about *why* one particular (security) discourse becomes dominant rather than another. This thesis examines this question, using a poststructuralist approach to analyze the cyber security debate in the Netherlands. It shows how the debate has transitioned from a technical computer security discourse in the late 1990s to the cyber security discourse of the present. Building on the works of earlier poststructuralists, it argues that identity and policy are mutually constitutive. The link between the two is characterized as an equilibrium that is premised on the idea of state sovereignty: a country's identity must be protected in a world full of dangerous Others. Therefore, this thesis concludes that the "choice" between discourses is based on the consideration of which discourse is better compatible with state sovereignty.

KEYWORDS: cyber security, identity, securitization, poststructuralism, discourse analysis

Cyberveiligheid staat momenteel bovenaan de Nederlandse politieke agenda, en wordt beschouwd als het nieuwste domein voor militair optreden. Dreigingen in en via cyberspace worden gezien als dreigingen tegen de nationale veiligheid en het functioneren van de Nederlandse samenleving. Het gedepolitiseerde taalgebruik in het cyberveiligheidsdebat suggereert dat dit de enige acceptabele wijze is waarmee over het onderwerp kan worden gepraat; dat wil zeggen, het debat lijkt te zijn *securitized*. Hoewel *securitization* theorie kan laten zien hoe een (gepercipieerde) dreiging kan worden *securitized* door middel van discours, zegt het weinig over *waarom* één bepaald (veiligheids)discours dominant wordt in plaats van een ander. Deze scriptie onderzoekt deze vraag, en gebruikt hiertoe een poststructuralistische benadering om het Nederlandse cyberveiligheidsdebat te analyseren. Het laat zien hoe het debat is overgegaan van een *technical computer security* discours in de late jaren negentig naar het huidige *cyber security* discours. Voortbouwend op het werk van eerdere post-structuralisten wordt beargumenteerd dat identiteit en beleid wederzijds constituerend zijn. De verbinding tussen de twee wordt gekarakteriseerd als een evenwicht dat steunt op het idee van statelijke soevereiniteit: 's lands identiteit moet worden beschermd in een wereld vol gevaarlijke Anderen. Om die reden concludeert deze scriptie dat de "keuze" tussen discoursen is gebaseerd op de overweging welk discours beter aansluit bij statelijke soevereiniteit.

KERNWOORDEN: cyberveiligheid, identiteit, *securitization*, poststructuralisme, discoursanalyse

ACKNOWLEDGEMENTS

This thesis is the result of a writing process of more than a year, filled with ups and downs along the way. Foremost I dedicate this thesis to my parents, who supported me unconditionally in a time when I needed it the most. As I already noted in my first master's thesis, I have tested their patience throughout the years. I also wish to thank the following people who graciously helped me out when I asked for their assistance: Nienke Bos, for being my sounding board during our long discussions; Claudia Beijen, for translating a number of Latin phrases; and dr. Gerry van der Kamp-Alons, for her insightful comments about and assistance with earlier versions of this thesis.

NIJMEGEN

June 30, 2014

LIST OF ABBREVIATIONS

ARPANET	Advanced Research Projects Agency Network
AIV	*Adviesraad Internationale Vraagstukken* (Advisory Council on International Affairs)
AIVD	*Algemene Inlichtingen- en Veiligheidsdienst* (General Intelligence and Security Service)
CERN	European Organization for Nuclear Research
CNA	computer network attack
CSNET	Computer Science Network
CSR	*Cyber Security Raad* (Cyber Security Council)
CST	cyber-space-time
CYBERCOM	US Cyber Command
DARPA	Defense Advanced Research Projects Agency
DCC	*Defensie Cyber Commando* (Defense Cyber Command)
DCS	*Defensie Cyber Strategie* (Defense Cyber Strategy)
DDoS	distributed denial of service (attack)
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
ICT	information and communications technology
IR	international relations
IT	information technology

IVS	*Internationale Veiligheidsstrategie* (International Security Strategy)
JWICS	Joint Worldwide Intelligence Communications System
MFC	Member of the First Chamber (Dutch Senate)
MILNET	Military Network
MIVD	*Militaire Inlichtingen- en Veiligheidsdienst* (Military Intelligence and Security Agency)
MSC	Member of the Second Chamber (Dutch House of Representatives)
NCSC	*Nationaal Cyber Security Centrum* (National Cyber Security Center)
NCSS	*Nationale Cyber Security Strategie* (National Cyber Security Strategy)
NGO	non-governmental organization
NHTCC	National High Tech Crime Centre
NIPRNET	Nonsecure Internet Protocol Router Network
NSA	National Security Agency
NSF	National Science Foundation
NSFNET	National Science Foundation Network
PCC	Permanent Chamber Committee (*Vaste Kamercommissie*)
re.	regarding
RMA	Revolution in Military Affairs
SIPRNET	Secret Internet Protocol Router Network
UCLA	University of California, Los Angeles
URL	uniform resource locator
UK	United Kingdom (of Great Britain and Northern Ireland)
US	United States (of America)
WWW	worldwide web

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION: THE ROAD NOT TAKEN

The information revolution continues to change international politics. Inextricably linked with globalization, it facilitated the blurring of the boundaries between the national and the international, and challenges the concept of sovereign rule. The information revolution has empowered non-state and transnational actors seemingly at the cost of the nation-state. As a result, in Joseph Nye's words, it has had "decentralizing effects" on society, effects that will seep through to the foreign policy of governments (2004a: 82).

One may logically conclude, then, that the nature of conflict is also undergoing change. Arquilla and Ronfeldt argued precisely that: "Cyberwar is coming!" they exclaimed in 1993. The two authors, writing for the RAND Corporation, predicted that as the world would become both more dependent on and interdependent through information and communication systems, the possibility of cyber war was increasing by the day. While the information revolution may have greatly benefited society as a whole, it also made states more vulnerable to attacks. Science fiction novels and movies abound depicting terrorists or rogue states creating chaos by taking out critical infrastructures through cyber attacks.

Almost twenty years later it seems that their doomsday scenarios have played out the way they anticipated them. As Arquilla himself notes, "[c]yber war is here, and it is here to stay" (2012: 1). Indeed, his views appear to be vindicated by a number of events in recent years. In April 2007, Russian cyber attacks were launched against Estonia in "retaliation" of the latter relocating a Soviet war memorial. Naturally, Russia claimed it was not responsible.

In any event, being one of the most networked countries in the world, Estonia's online activity was almost completely halted after a large distributed-denial-of-service (DDoS) attack (Landler and Markoff, 2007).[1] One year later, during the brief Russia-Georgia War, cyber attacks made Georgian government and media websites inaccessible, which some claimed was a prelude to the actual armed conflict. Russia again denied any involvement (Markoff, 2008). The most-cited example of cyber attacks is undoubtedly Stuxnet. Stuxnet, a cyber worm, specifically targeted the Iranian nuclear development program, infecting thousands of computers and (allegedly) setting back the program by a number of years. Speculations about who was responsible quickly surfaced following the attack. In 2011, the German control system security consultant Ralph Langner (2011) argued that it could only have been carried out by a "cyber superpower," namely the US. It was later confirmed that president Obama indeed ordered the attacks (Sanger, 2012).

It should not be surprising that throughout the years governments have responded to such threats by introducing policies aimed at securing cyberspace, and, more recently, to start increasing their offensive cyber capabilities. President Obama considers cyber security as "one of the most serious economic and national security challenges [the US faces] as a nation" (National Security Council, 2010). In 2009, the US government created a special division, US Cyber Command (CYBERCOM), which reached full operational capability in October 2010. CYBERCOM's mission statement declares that it is

> responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations)

[1] A DDoS attack makes websites, servers, and/or internet services unavailable by overloading them with communications requests.

> in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries. (US Strategic Command, 2011)

Arriving relatively late on the scene, the Dutch government issued a cyber security strategy in 2011, in which it announced to establish two new agencies, the *Cyber Security Raad* (CSR) and the *Nationaal Cyber Security Centrum* (NCSC), which were operational by June 2011 and January 2012 respectively (Ministerie van Veiligheid en Justitie, 2011). One year later, the Dutch ministry of Defense released the *Defensie Cyber Strategie* (DCS). Recognizing "the dependence of the armed forces on digital technology," it explicitly mentions "the development of [offensive] military capabilities to conduct cyber operations" as one of its main goals (Ministerie van Defensie, 2012: 4-6).

More recently, the Netherlands has emerged as an internationally recognized player in the cyber security industry, an image the Dutch government carefully cherishes. The Hague is now home to the so-called "Hague Security Delta," a security cluster of some four hundred security companies of which a large portion is devoted to cyber security (De Lange, 2014). In 2015, The Hague is hosting the fourth International Conference on Cyberspace, one of the largest of its kind when it comes it cyber security. Another sign of the Netherlands' growing prominence in cyber security is the decision by NATO to move all of its activities in the field of information and communications technology (ICT)—which includes the security of its digital networks and missile defense systems—to The Hague. The Hague's growing cyber security industry was cited as an important reason for NATO's decision (De Lange and Jonker, 2014).

The fact that decision makers oftentimes think in terms of security when it comes to cyberspace speaks volumes. Most discourse simultaneously emphasizes looming threats coming from non-state actors and the possibility of a full-blown cyber war between states.

Cyberspace is thus linked to national and economic security. This suggests, as some authors have already noted, that cyberspace has been securitized (Barnard-Wills and Ashenden, 2012; Dunn Cavelty, 2007; for an earlier account see Eriksson, 2001), which in turn gives legitimacy to the introduction of sometimes far-reaching policies. After all, the stakes are high: a state's survival is on the line. Yet the more interesting observation, here, is that cyberspace turns out to be a *space* that can in fact be securitized. Seemingly, it is a domain comparable with air, sea, and land. If that is the case, then all the laws, norms, rules, and regulations of the "real world" must also apply to the virtual world of cyberspace (see for example Lynn, 2010). Once policymakers have accepted that "cyberspace" fits in with existing discourse, it is not very surprising anymore that policy worldwide with regards to cyber security converges over time, as several international relations (IR) theories teach.

Intuitively, this sounds like a plausible explanation. Yet, even if discourse and policy with regards to cyberspace, cyber security, and more recently cyber warfare show remarkable similarities in many countries, it still leaves open one fundamental question. Why was this particular discourse chosen and *not* another? Since the worldwide web, according to one author, is moving from Web 2.0 to a Web 3.0 in which physical and virtual lives become more integrated everyday (Carr, 2012: 204), it is crucial to examine this question in order to improve our understanding of this apparently "natural" policy convergence. It is therefore all the more surprising that this question as of yet has received so little attention from IR scholars because the choice of discourse has major implications as to how future policy and research will develop. There are latent forces at play that guide and have guided the cyber security debate down a specific road, which is already betrayed by the fact that the world is talking about a cyber *security* debate in the first place.

Returning to the previous observations, the supposed continuity in terms of discourse belies the dialectical undercurrent taking place in international relations (theory) and politics.

As noted above, the information revolution has put the idea of sovereignty under pressure. Today policymakers (are trying to) adapt to the digital age within the confines of known territory—both figuratively and literally—that is, a security framework. More and more it appears that we are arriving at the peculiar situation in which the Westphalian system of sovereign states is being replicated in cyberspace, a space which was presumed borderless. A similar trend is occurring in academia: scholars, particularly IR scholars, are still trying to figure out how to fit in concepts such as 'information revolution" and "cyberspace" into existing theories (Eriksson and Giacomello, 2006, 2007; Junio, 2013; Nye, 2004a). The problem remains, however, that those efforts are primarily aimed at problem-solving: the problem of how to reconcile theory with the puzzles posed by the information revolution, within the parameters set by well-established scientific paradigms. These parameters guide the direction into which research will go. Since the "grand theories" in IR are mostly concerned with questions of security, it is only logical that a new phenomenon like cyberspace will be viewed through the same lens. This is not to say that such research is not useful; what matters here is that this kind of research does not critically reflect upon *itself*. Like many policymakers, a lot of scholars take for granted a certain "given" order of things, for instance that it is "natural" to think about international politics in terms of security. To put it differently, both they and policymakers start from the assumption that their framework of analysis is universal, i.e. applying equally throughout space and time and thus also to later, new phenomena such as cyberspace.

This thesis questions this assumption because it ignores or outright denies that discourse is dynamic. Though discourse may appear fixed or show continuity, as established above, it is still built on earlier struggles between competing discourses (Cox, 1981). Following from this, the main research question is "*Why did the current cyber security discourse become dominant rather than another?*" Using poststructuralist theory and

discourse analysis, the aim of this thesis is to show that the path cyber security discourse has gone down is not as natural as it seems. Rather, it is *logical* that it went down this particular path and not another because existing paradigms (inevitably) pushed it into that direction. From that point of view it then becomes easier to understand why cyber security policies in different countries have converged.

Outline

In order to answer the research question this thesis analyzes cyber security policy in the Netherlands. With its focus on discourse in those policies, it places itself at the nexus of several academic fields. The following chapter explores these fields, providing the necessary background for subsequent parts. It looks in particular at the historical development of cyberspace, information revolution literature, and cyber security literature in the broadest sense of the word.

Chapter 3 then discusses earlier attempts by IR scholars to integrate the cyber security debate into the existing literature. Many of these attempts fall within the boundaries of conventional IR theories, primarily realist and constructivist thinking. With the insights gained from these fields it moves on to introduce poststructuralism as an alternative to account for the rise of cyber security discourse. It argues that (state) identity and (foreign) policy are interlinked: they produce and reinforce each other. Moreover, the link between identity and policy is constituted by state sovereignty. Boundaries in cyberspace are theorized to be an ontological necessity in order to preserve state identity.

Chapter 4 concerns methodology. It explains how the ideas of the previously mentioned two alternatives are “translated” into measurement tools, and also includes a reflection on some of the consequences this will have for the research conducted in this thesis. In addition, it addresses case selection, and provides justification with respect to the

selected case. As mentioned, this thesis conducts a single case-study on the Netherlands. Additionally, it will explain the choices made in terms of source material. As will be seen, publicly available documents are the primary objects of analysis.

The fifth chapter contains the empirical part of this thesis. With the methodological tools of the preceding chapter it analyzes several Dutch policy documents and reveals how the language used in those documents gradually moves from a technical computer security discourse to a cyber security discourse. More important, it will also treat the *why*: why were particular policy choices made and how were those choices made possible through discourse? As seen, this thesis attempts to answer this question from a poststructuralist point of view. To that end, the expanded foreign policy debate *vis-à-vis* cyber security will also be analyzed.

This thesis rounds off with concluding thoughts and will provide suggestions about which direction future research could go. On a final note, it must be underscored that this thesis is not about other aspects of cyberspace, such as e-democracy, the "digital divide," open access, and so on. Although a poststructuralist analysis could have much to say on such matters, it falls outside the scope of this thesis, which is first and foremost security oriented.

CHAPTER 2

CYBERSPACE AND THE CYBER SECURITY DEBATE

Discourse is contestable and inherently unstable, which is especially salient in the case of cyber discourse. Everyone has some intuitive feeling what is meant by terms such as "cyberspace," "cyber security" or "cyber warfare." Still, there is no real consensus as to their definitions. This is also underscored by the fact that there even is no agreement how to *write* these terms. With the notable exception of "cyberspace," authors use variations of terms with the prefix "cyber" interchangeably: cyber security, cybersecurity, cyber-security.[2] In any case, the more pressing problem is that prefixes like "cyber" or "information" are often slapped on to existing terms without giving any real thought to conceptual clarity. As a result, Dunn Cavelty notes, these terms now "have so many meanings and nuances that the words quickly become confusing or lose their meaning altogether" (2007: 21). Before continuing with the more substantive part of this chapter, it therefore merits to discuss how one is to understand such "cyber lingo." The way in which a term like "cyberspace" is explained usually tells a great deal about the actor doing the explaining, how they diagnose problems, and their proposed solutions. If anything, the discussion is a first step in answering the main question guiding this research. Former US Deputy Secretary for Defense William J. Lynn III, for example, espoused the view of his department, the Pentagon, that cyberspace "is a new domain of warfare. . . . [I]t has become just as critical to military operations as air, land, sea,

[2] As the reader will have noticed, this thesis opts for the format "cyber [space] noun/verb," e.g. "cyber warfare." In line with existing literature, the only exception to this rule is the term "cyberspace."

and space. As such, the military must be able to defend and operate within it" (2010: 101). Lynn's conclusion that militarization of cyberspace is warranted logically follows from his premise that cyberspace is indeed a military domain.

This chapter provides the background against which this thesis is situated, presenting the cyber security debate from multiple angles. The following section fleshes out the discussion about cyber terms. It briefly traces the genealogy of the term "cyber" and its offspring before moving on to discussing how this thesis (and other scholars) conceptualizes cyberspace. The second section looks at the history of the Internet. It explains how from its inception the Internet was built with openness, expedience, and transparency in mind. Lastly, moving on to the third part, it is shown that a security discourse emerged in response to the (supposed) weaknesses of the Internet. This discourse heavily emphasizes the insecurities that arise from the design choices of the Internet (and cyberspace). While the Internet was envisioned as an "open commons," the call for more control and regulation has now become far more acceptable among politicians and policymakers.

The difficulties of things "cyber"

The prefix "cyber" finds its origins in the term "cybernetics," which comes from the Greek *κυβερνήτης* (*kybernētēs*), meaning "steersman" or "governor." The modern conception of cybernetics has its roots in the cybernetic theory established by Norbert Wiener (1948: 19), who defined it as the study of control and communication in the machine or in the animal. "Cyber" thus has the connotations of control and guidance. Today, however, the meaning of "cyber" has far removed from its original meaning, being mostly associated with the "virtual" or the "digital." As will be seen later, especially the connotation with control is becoming more and more salient again. Many policies with regards to cyber security are at the very least attempts at regulating or controlling cyberspace.

The term “cyberspace” itself was popularized by the science fiction author William Gibson, in his 1984 novel *Neuromancer*. In it, he described cyberspace as a

> consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts… A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light in the nonspace of the mind, clusters and constellations of data. Like city lights, receding. (1984: 69)

Since then, the use of “cyberspace” has become widespread in both academic and non-academic circles, and many of them have given it different definitions. One author defined cyberspace as

> a man-made environment for the creation, transmittal, and use of information in a variety of formats. . . . Cyberspace consists of electronically powered hardware, networks, operating systems, and transmission standards. (Rattray, 2001: 65)

More recently, Kramer, Starr and Wentz (2009) proposed that

> cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies. (2009: 28)

The list of definitions goes on much longer than the three quoted here,[3] but the red thread throughout all of them highlights a number of aspects: artificialness, information and communication systems, and electronics.

Notably absent in these definitions is any reference to control. Perhaps this is because it is self-evident: if there is a space yet unclaimed, someone (or something) is bound to attempt to control it, lest it falls into anarchy. In addition, the control of cyberspace is implied by the term itself. After all, as was seen, the prefix "cyber" has the connotation with control. To elucidate the foregoing a little further, one also has to keep in mind that, in the end, cyberspace is man-made. The information in cyberspace is stored on servers because people make it do so. The servers are in turn stored in data centers which are maintained by living and breathing IT persons. And, in the most extreme case, many different institutions are (easily) able to monitor the information in cyberspace, as was revealed by whistleblower Edward Snowden in 2013. All told, at various points in the "cyber chain" we might discern different measures of control. We might even *expect* that some levels of control are exerted over cyberspace regardless of whether it is visible or not.

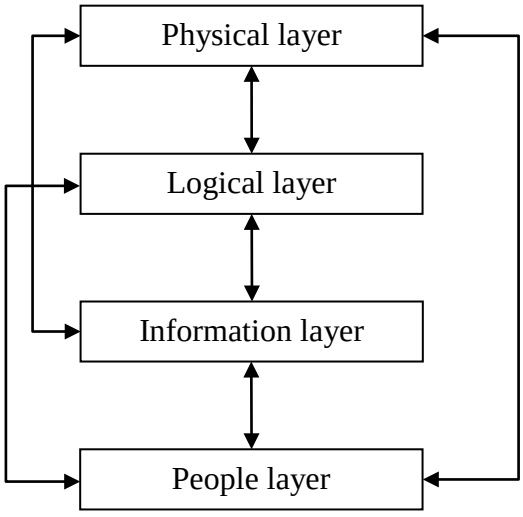
In order to bring the control aspect back in, this thesis adheres to the model created by David Clark (2010) that characterizes cyberspace with four interconnected layers. These layers are a) the physical layer upon which cyberspace is built such as PCs and servers, b) the logical layer which has to do with the design choices for platforms like the Internet, c) an information layer that contains, as the name suggests, all the information in cyberspace, and

[3] For a comprehensive overview of definitions, see Kramer, Starr and Wentz (2009), pp. 26-27. Another author has claimed that the term "cyberspace" is misguided (Carr, 2012). Drawing from theoretical physicist Basarab Nicolescu, he instead puts forward "cyber-space-time" (CST) as a more accurate name, because it reflects that it is simultaneously artificial *and* real. Nicolescu originally explains that the "information that circulates in CST is every bit as material as a chair, a car, or a quantum particle. Electromagnetic waves are just as material as the earth from which the calculi were made: it is simply that their degrees of materiality are different. In modern physics matter is associated with the complex relationship: substance-energy-information-space-time" (2002: 77). Elsewhere, Nicolescu argued that CST is a completely different level of reality "on par with organic systems" (Carr, 2012: 204).

d) a people layer, because it is ultimately the people who make and shape cyberspace. With this model, we can better grasp at which point and to what extent cyberspace can be controlled, and, more important, see how discourse gives meaning to cyberspace—we will see this particularly in the first and second section of the empirical analysis in Chapter 5. This is quite a different but useful approach to understanding cyberspace because it can put into perspective what policymakers and/or politicians actually have in mind when they talk about cyberspace. The model also calls attention to the fact that cyberspace is more than simply "the virtual" and that it is indeed very real as well. As Clark explains, "It is not the computer that creates the phenomenon we call cyberspace. It is the interconnection that makes cyberspace—an interconnection that affects all the layers in our model" (2010: 1). Figure 1.1 depicts a graphic representation of the model.

Other cyber terms are a function of cyberspace. Cyber security is the security *of* cyberspace. Cyber warfare is warfare *in* or *through* cyberspace. Yet if cyberspace is conceived as a layered space, we also need to revisit those other concepts like cyber security and cyber warfare. What exactly are we securing when we talk about cyber security? In and against which part of cyberspace can war be waged, if at all? Elsewhere in this thesis, we will

Figure 1.1. A layered conceptualization of cyberspace.



see that many policy documents and debates do not take these considerations into account or simply take them for granted. The following two sections, however, will go along with the established discourse in order to represent the cyber security debate as it currently stands.

Cyber insecurity

With a term like cyber security it must also mean that there is cyber *in*security. If the design of cyberspace were infallible, then there would be no need to secure it in the first place. We thus have to ask what the source of this insecurity is. The sources are manifold, and have to do with the way cyberspace and in particular the Internet was envisioned.[4] In order to understand this better, it is necessary to discuss the historical development of the Internet.

The Internet as we know it today began as a military program that has its early roots in the 1960s (Leiner et al., 2009). It developed out of ARPANET, which was the result of a computer research program funded by DARPA, an agency of the US Department of Defense.[5] In September 1969, the first message between two host computers at UCLA and the Stanford Research Institute was transmitted. It would take a number of years before ARPANET fully matured into the Internet, with access to the network remaining limited to academic and military circles. In the early 1980s, the Defense Department adopted various standard network protocols, which in the following years became global standards many of which are still in use today. This allowed the splitting off of the military community from ARPANET, resulting in MILNET in 1983. It should be noted that by then ARPANET had become a subnet of the Internet. But as Leiner et al., who were all directly involved with the development of ARPANET, note, this was precisely the way Internet was intended to be:

[4] In everyday language "cyberspace" and "the Internet" are often, erroneously, equated or used interchangeably. The Internet is only part of cyberspace, but undoubtedly the most important one.

[5] The Defense Advanced Research Projects Agency, originally named ARPA, changed its name multiple times from ARPA to DARPA and back throughout its existence. Here it will be referred to by its current name, DARPA.

> The Internet as we know it embodies a key underlying technical idea, namely that of open architecture networking. In this approach, the choice of any individual network technology was not dictated by a particular network architecture but rather could be selected freely by a provider and made to interwork with the other networks through a meta-level "Internetworking Architecture." (Leiner et al., 2009: 24)

These ideas would turn out to be crucial in the subsequent development of the Internet, which will be discussed in more detail later in this chapter.

As seen, access to ARPANET (and various other networks in *inter alia* British universities) was limited, and was rapidly becoming obsolete. The American university community soon expressed its desire for all scientific communities, regardless of discipline, to be connected to a single network (Flichy, 2007; Leiner et al., 2009). After another network (CSNET) bridged the period between 1981 and 1983, the US National Science Foundation (NSF) launched the NSFNET program in 1983, becoming fully operational in 1985. NSFNET provided the so-called national Backbone to which regional networks could connect; local university networks in turn connected to the regional networks. By 1989, NSFNET had taken over all of ARPANET's functions, resulting in the latter's decommissioning. This marked an important occasion in the development of the Internet: with the role of the military ending, the Internet came under civilian control (Abbate, 1999).[6]

Three subsequent developments then proved decisive in the way the Internet became part of everyday life. First, the network infrastructure was privatized. Most of the networks connected to NSFNET were funded by the NSF itself. Steve Wolff, who became head of the NSFNET program in 1986, realized that further development of network infrastructure

[6] The US Department of Defense to this day operates its own private networks, namely NIPRNET for non-classified information, SIPRNET for secret information, and JWICS for top-secret information. These networks are in turn part of cyberspace.

needed to become independent from government funding. Moreover, the national NSFNET Backbone precluded any uses other than those related to research and education, much to the dismay of commercial network service providers. This "Acceptable Use Policy" was necessary, since Congress did not want government funding to go to commercial uses (Abbate, 1999: 196). Starting from 1988, the NSF pursued strategies with the goal of privatization in mind, such as sponsoring "The Commercialization and Privatization of the Internet" conference at Harvard's Kennedy School on Government. The strategy paid off. By 1995, the NSFNET Backbone was defunded, because private investments had led to the creation of numerous long-haul networks privately owned by commercial network service providers (Leiner et al., 2009). With the retreat of government the acceptable use issue was now rendered moot.

The second crucial development was the creation of the World Wide Web (WWW). While working at CERN in Geneva, nuclear physicist Tim Berners-Lee concluded that too much project information was lost as a result of frequent personnel turnovers. Already in 1989 he proposed a "'web' of notes with links" which he "hope[d] would . . . allow a pool of information to develop which could grow and evolve" (Berners-Lee, 1989: 2). One year later, together with Robert Cailliau, he reiterated this view, and explained how information could be accessed through a browser on a client machine (i.e. a personal computer) (Berners-Lee and Cailliau, 1990). The revolutionary part was that the WWW could also store images and other multimedia, in a time period in which the Internet was still primarily oriented towards basic text. Berners-Lee released the necessary software in 1991, including the programming language HTML that is still used today and well-known other protocols such as HTTP and URL. The software naturally ended up on the Internet, which permitted other physicists and programmers around the world to pick it up as well and create software of their own (Abbate, 1999; Flichy, 2007). The rest, as the saying goes, is history.

Lastly, the Internet was rapidly commercialized in the second half of the 1990s. This had everything to do with the two previous developments. The invention of the WWW coincided with the privatization of the Internet. Where the privatization opened up the possibilities for commercial uses, the WWW popularized and made access to the Internet easier. Companies could reach millions of customers within their homes, a huge marketing potential. In the closing years of the previous millennium these huge expectations led to the infamous dot-com bubble. Because internet startups were expected to make huge profits, their shares were highly overvalued. When the bubble burst, many of these companies had to file bankruptcy. In the years since then, companies have developed more feasible business models which usually revolve around advertisement revenues and subscription fees.

What is so remarkable about the development of the Internet is how fast it was adopted by the general public and commercial parties. The keyword as to why is "*open*." A 1994 National Research Council report which was very influential on the Clinton administration emphasized this idea and described the way of the future with a high level of accuracy:

> [A]n Open Data Network includes the following characteristics:
>
> *Open to users:* It does not force users into closed groups or deny access to any sectors of society, but permits universal connectivity . . .
> *Open to service providers:* It provides an open and accessible environment for competing commercial or intellectual interests. . . .
> *Open to network providers:* It makes it possible for any network provider to meet the necessary requirements to attach and become a part of the aggregate of interconnected networks.

> *Open to change:* It permits the introduction of new applications and services over time. It is not limited to only one application, such as TV distribution. It also permits the introduction of new transmission, switching, and control technologies as these become available in the future. (National Research Council, 1994: 3-4, emphasis in original)

Given the origins of the Internet in academic and research communities this emphasis is not surprising. Its architecture was designed with expedience and efficiency in mind, permitting open access and knowledge sharing. And here we find the main source of cyber *in*security: security did not have priority. Dunn Cavelty (2012a) correctly refers to this as a legacy problem, because in the early days of the Internet there were simply not that many computers connected to the various incipient networks. She identifies three factors why today's cyberspace is so vulnerable, namely "the same basic network technology (not built with security in mind), the shift to smaller and far more open systems (not built with security in mind), and the rise of extensive networking at the same time" (Dunn Cavelty, 2012a: 363).

What we thus need to take away from this section is the conditions that make cyber insecurities possible. In domains like air, space, water, and land, insecurities arise over territorial boundaries, natural resources, and countless other things. Some of this also applies to cyberspace. But unlike those physical domains, the architecture of cyberspace itself is not watertight. Physical domains came into existence through gradual, natural processes, and we can hardly say that nature's *architecture* is fallible or open to hostilities. Even if sometimes we do not like the way nature works, there is still not much we can do about it. At best we can do what mankind always has done: learn to live *with* nature. Cyberspace, by contrast, is entirely man-made. The architecture of cyberspace, as seen in the model, relies on multiple layers that one way or another requires some human input. If the architecture of cyberspace is

fallible—which it is—it is because man *made* it fallible, whether or not consciously. Moreover, technological choices concerning the architecture are not value-neutral, a point that will return in the third chapter. Here, we already see the interplay between agency and structure. Cyberspace was originally open-natured because the scientists behind cyberspace *believed* that it *should* be open. On the flipside, these scientists were located in a society, the US, which greatly values such liberal norms. Combined with the open nature of cyberspace we can now begin to see the contours of cyber threats and the people behind them.

Cyber threats and threat perceptions

Undeniably, the creation of cyberspace and the Internet has had many positive effects. Its blurring of boundaries has brought the world closer together; it provided a platform for groups that previously had severe difficulties getting their voices heard; information is more accessible; to name but a few. Overall it has and still is radically changing international politics. The paradox, however, is that the open nature of cyberspace is simultaneously its biggest weakness. It is indeed open to everyone, including those who want to use it to do harm. Still, while this threat is very real it is also important not to overstate the problem. Later in this chapter we will see that there is a considerable gap between perception and reality. The next paragraphs first explore the different types of cyber threats identified primarily by authors in the field of strategic studies.

Cyber threats can be put on a ladder with an upward scale in terms of gravity. By and large there are three categories of threats to the security of cyberspace, all of which are not without complicating factors. They are cyber crime, cyber terrorism, and cyber warfare, respectively (Klimburg, 2011). *Cyber crime* is by far the most common and prevalent threat and is committed by an amalgam of actors. As in the real world, cyber crime can vary from theft, to fraud, to espionage. Examples of such crimes abound. Most users of the Internet will

probably have had some experience with so-called phishing emails. Such emails, which often look as if they are sent by genuine companies, try to trick users into providing personal information such as a credit card number. The US, in another case, has accused China multiple times of stealing American intellectual property through cyberspace (Sanger, 2013). A more ambiguous form of cyber crime is "hacktivism," which can be compared to civil disobedience. The difference lies in motivation. Whereas the previous examples are (mostly) economically motivated, hacktivism is politically motivated. Oftentimes, such hacktivists deface websites or try to make websites unavailable with for instance DDoS attacks. A well-known example is the 2008 attack by Anonymous, a leaderless hacker collective, against the website of the Church of Scientology (Singel, 2008). As might be expected, cyber crime comes with a high price. Reports by Symantec and McAfee, both companies in the antivirus industry, claimed that the global costs of cyber crime run into the hundreds of billions of dollars. These figures are criticized by others on the grounds of some questionable methodology used in the reports and the companies having clear commercial interests (Maass and Rajagopalan, 2012). Still, such reports are often quoted by politicians and policymakers nonetheless. The role of the private cyber security industry in these debates is certainly an interesting one and worth studying, but falls outside the scope of this thesis.

The second category is *cyber terrorism*, which is an infinitely more complicated type of cyber threat than cyber crime. Where cyber crime is still relatively easy to identify, this is certainly not the case for cyber terrorism. We first have to ask what kind of cyber attacks qualify as cyber terrorism. From the conventional terrorism literature, we can deduce that such attacks must be a violent act committed (or threatened to commit) by a clandestine actor that at least contains a political motivation and an objective to instill fear in a particular targeted group (Schmid and Jongman, 1988; Weinberg, Pedahzur and Hirsch-Hoefler, 2004). Cyber terrorism is then, obviously, the confluence of cyberspace and terrorism: inflicting

harm through the means of computer networks (Denning, 2001). With the previous section in mind it is certainly plausible that network attacks can lead to serious harm. Much of the critical infrastructure (e.g. power plants) in today's world relies on computer networks which in theory can be attacked by anyone. To date, however, no act of cyber terrorism that led to loss of life has taken place.

The cyber terrorism debate is therefore not without controversy. As Dunn Cavelty (2007) notes, the debate has fallen into two groups of authors which she refers to as the "hypers" and "de-hypers." The first group of authors argues that due to the vulnerabilities of cyberspace a destructive act of cyber terrorism is imminent and indeed inevitable (Arquilla and Ronfeldt, 2001; Bhalla, 2003; Carr, 2012). An early 1991 report asserted that "Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb" (National Research Council, 1991). Oftentimes authors use "cyber doom" scenarios to get their point across. It is only a matter of time before the US will witness an "electronic Pearl Harbor" or "cyber 9/11" (Arquilla, 2009). The other group is critical of these claims, pointing out *inter alia* that, as said, there has so far been no instance of cyber terrorism. Lewis (2002), for instance, questions whether cyberspace really is as vulnerable as the "prophets" of cyber doom purport it to be. Some argue that the gap between cyber security rhetoric and reality is born from a fear of the unknown and the fear of technology-out-of-control (Barnard-Wills and Ashenden, 2012; Lawson, 2013; Stohl, 2006; Weimann, 2005). Weimann notes that "from a psychological perspective, two of the greatest fears of modern time are combined in the term 'cyberterrorism'. The fear of random, violent victimization segues well with the distrust and outright fear of computer technology. An unknown threat is perceived as more threatening than a known threat" (2005: 131). It is hardly a surprise that especially after the terrorist attacks of September 11 the fear of cyber terrorism dramatically increased.

Lastly, and most relevant to this thesis, the third cyber threat is *cyber warfare*. The cyber warfare debate shows many similarities with the previous debate. Even more so than cyber terrorism, cyber warfare is not easy to conceptualize. There is no general consensus as to how to define cyber warfare or, more specifically, what constitutes an act of cyber war—more on this momentarily. Cyber warfare is usually mentioned in the same breath as the so-called "Revolution in Military Affairs" (RMA), an idea that gained momentum after the Gulf War of 1990-1991 (Arquilla and Ronfeldt, 1997). As seen, advances in ICT changed the way information was gathered, disseminated, and used to one's advantage (or the other's disadvantage). The Gulf War showed that the vast US superiority with respect to information and technology added to the resounding defeat of the Iraqi forces. Military thinking thus accepted that information would become more important and even decisive in future conflicts, and that military theory and strategies had to change accordingly (Berkowitz, 1997; Davis, 1997).

In their paradigm-setting article "Cyberwar Is Coming!" Arquilla and Ronfeldt (1993) proposed to separate cyber warfare from the RMA debate because the latter focused primarily on changes in organization and management theory (e.g. in the military). To them, cyber war

> refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems . . . on which an adversary relies to "know" itself . . . It means trying to know all about an adversary while keeping it from knowing much about oneself. It means turning the "balance of information and knowledge" in one's favor, especially if the balance of forces is not. It means using knowledge so that less capital and labor may have to be expended. (1993: 145)

Elsewhere they note that, in line with their definition, cyber war is exclusively reserved to the military realm and that it involves nation-states pitting their military forces against each other as in traditional wars (Arquilla and Ronfeldt, 1997).[7] Richard A. Clarke, who was the Special Advisor to president George W. Bush on cyber security, echoes this sentiment in his definition that is now widely used. Cyber war "refers to actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke and Knake, 2010: 6). Both definitions are problematic because they focus exclusively on nation-states. It ignores the fact that a plethora of non-state actors—which in turn might be *sponsored* by an enemy government—can launch cyber attacks against a nation's critical infrastructures.

The biggest problem of conceptualizing cyber war, like all cyber threats, is that it has become more and more abstract in the twenty years since the term's introduction. This is especially apparent in definitions such as Carr's ("inspired by the writings of Sun Tzu") who suggests that "Cyber Warfare is the art and science of fighting without fighting; of defeating an opponent without spilling their blood" (Carr, 2012: 2). It virtually turns any (potentially) disruptive or destructive use of computers by anything or anyone into an act of cyber war. And as Dunn Cavelty (2012b) corroborates, it is exactly this development that adds to insecurity among many governments, which become convinced that they have to step up their cyber security game in terms of cyber defense, cyber offense, and cyber deterrence.

Some critical voices in the field of security studies have recently tried, to borrow Dunn Cavelty's terminology, to "de-hype" the cyber war debate. Liff (2012) rightly argues

[7] Arquilla and Ronfeldt distinguish cyber war from what they call "netwars." Netwars are defined as "an emerging mode of conflict (and crime) at societal levels, short of traditional military warfare, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age" (2001: 6). Netwar tactics may include propaganda, public diplomacy with intent to change public opinion, and "efforts to promote a dissident or opposition movements across computer networks" (1993: 144). The use of social media during the 2011 Arab Spring would fall within the definition of "netwar."

that authors who adopt such definitions make the mistake to assume that cyber warfare exclusively takes place in cyberspace. This "risks leading analysts to exaggerate seemingly novel and disturbing aspects of CNA [computer network attacks] (e.g. plausible deniability) and restrict their analyses to the most unlikely, and in some cases fantastical scenarios" (2012: 405). He explains that cyber warfare at best can serve as a force multiplier of traditional military force or may increase the frequency of conventional kinetic wars (see also Libicki, 2009). Even more outspoken is Rid (2012), who claims that as of yet cyber war has not taken place and that it probably never will. Similar to Liff, he draws his arguments from a Clausewitzian approach to warfare, who argued that war contains three elements. First, war has a violent character. An act of war is lethal or at least has the potential of being lethal. Secondly, war is instrumental in that it is a means to an end, namely to force the enemy to accept your will. Lastly, war is politically motivated, as Clausewitz's most famous adage summarizes: "War is a mere continuation of politics by other means." Rid concludes that no single cyber incident has met all three criteria. Even Stuxnet, the US-Israeli cyber attack against Iranian nuclear facilities which was hailed as a game changer for cyber warfare, is at most cyber *sabotage*. Admittedly, one may level the criticism against Rid that he is playing with words: according to *his* (stringent) definition, no cyber war has taken place so far. It does underscore the problem, however, of lack of consensus. Neither group really takes each other seriously.

Criticism notwithstanding, why then do so many opinion makers assume that cyber warfare is such a threat to the stability of the international system? It again has to do with the open nature of cyberspace, leading to the problems of *asymmetry*, *attribution*, and *volatility* (Clarke and Knake, 2010; Libicki, 2009). Cyber warfare is said to be asymmetrical: if a balance of forces is disadvantageous for one country *vis-à-vis* another, the country can use a cyber attack to surmount this disadvantage (cf. Arquilla and Ronfeldt, 1993). Since cyber

attacks are relatively cheaper to conduct, a (weak) country might be more willing to start a conflict. Moreover, geographic distances between countries are irrelevant in cyberspace. Cyber operatives can attack the networks of a country on the other side of the world from the safety of their compounds back home. Next, in cyberspace it is easy to remain anonymous. Sophisticated cyber warriors are usually able to cover their tracks, thus making it difficult for other countries to trace the location of origin and culprit of a cyber attack. A country may therefore launch a cyber attack because it knows it can deny involvement or shift the blame to individual hackers. In other words, because attribution of cyber attacks is difficult, countries are able to appeal to plausible deniability. An example of this is the 2007 cyber attacks against Estonia. Most experts agree that Russia is most likely the culprit, yet Russia denies any responsibility (Landler and Markoff, 2007). Lastly, cyberspace is volatile, meaning that it is perpetually evolving. The assumption is that cyber defense always lags behind, because a clever cyber warrior can always find some gap in cyberspace that he can exploit for a cyber attack—Chapter 5 shows that this is also a very vivid sentiment in Dutch cyber security policy. From this point of view, the best defense is a good offense. A country that feels threatened by a certain other country may have incentive to launch a "preemptive" cyber strike. (One may wonder, though, about the efficacy of such a strategy. As Thomas Rid (2013: 87) rightly notes, "designing [for example] the next Stuxnet will not make the U.S. energy grid any safer from digital attacks.") The upshot of all this is that many authors believe that in the future most conflicts will be fought in and through cyberspace and that cyber war is indeed inevitable (McGraw, 2013).[8]

Summary

This chapter provided the background for the subsequent chapters. It first discussed how the term "cyberspace" and related terms originally developed. In order to bring back in the

[8] For a critical review of these assumptions, see Liff (2012).

control element of prefix “cyber” it then adopted a layered model of cyberspace. The second part looked at the history of cyberspace, and specifically the Internet. It demonstrated that both were invented with quite liberal ideas in mind. This was then followed by the third section, which showed the current state of the cyber security debate. The debate has become dominated by a discourse based on threats, varying from cyber crime, to cyber terrorism, to cyber warfare respectively.

The development of the cyber security debate from a “liberal” to a more “realist” school of thought has not eluded scholars, which is the focus of the following chapter. Some authors use traditional IR theory, such as (neo)realism, to account for this development, while others view it from a constructivist point of view. Both schools of thought offer competing explanations, yet remain silent on the question as to *why* it is that the realist discourse became dominant rather than another. For this, as will be seen, we need an altogether different approach, namely poststructuralism.

CHAPTER 3

CYBER SECURITY AS PRACTICE

Compared to other forms of security, cyber security is still relatively new to the scene. However, it is abundantly clear that the debate is dominated by older, existing rhetoric. Two dominant bodies of literature within IR are reviewed that attempt to account for this development. Although they provide useful insights, they have a number of limitations that prevent them from elucidating the full picture. The second through fourth section of this chapter introduce an alternative approach to IR: poststructuralism. Poststructuralism looks *inter alia* at the discourses that link identity and politics, which it argues are mutually constitutive. What matters more is that it theorizes that power-knowledge constellations are inherent to discourse: it enables and constrains both identity and policy. In addition, discourse is relational. A discursive subject is always positioned with reference to someone or something else. We already saw some of these aspects earlier when it was suggested that since we speak about cyber security there must also be cyber insecurity, and that the way an actor conceptualizes cyberspace has consequences for the range of possible policy options. Crucially, this does not only apply to policymakers but also to other authority figures such as academics.

Cyber security and IR theory

At this point the reader will have noticed two trends. First, the last part of the previous chapter uses a lot of “coulds” and “mights,” especially in the parts about cyber terrorism and

cyber war. There is much uncertainty surrounding cyber threats, except the apparent certainty that cyber terrorism and/or cyber war *will* happen. Second, much of the specialist cyber (security) literature focuses on policy, governance, organization, and management, and is usually written by security experts and computer scientists. They describe the various cyber phenomena, how to cope with them, and propose countermeasures. Still, many of these articles are not informed by theory. Given the open, transnational character of cyberspace and its impact on the international system one would thus expect that the field of international relations theory has much to say on the matter. Yet as some other scholars have noted as well, this is surprisingly not the case (Choucri, 2012; Eriksson and Giacomello, 2006, 2007; Manjikian, 2010; Reardon and Choucri, 2012). A number of articles have been written on cyberspace in general, but few attempts have been made to view the roles of cyberspace and cyber security in particular through an explicit IR (theory) lens (Reardon and Choucri, 2012).[9] Those authors that did can roughly be divided into two distinct groups that follow the dominant paradigms in IR: realists and constructivists.

The first group adopts a clear realist point of view, which is not surprising given the fact that the studies of security and power in IR have historically been dominated by the realist paradigm. In general, they research the impact of cyberspace on the stability of the international system. More important, these authors underline that despite processes of globalization the international system is anarchic and that states are still the most important actors in IR. Liff (2012), for instance, points out that cyber war is part of a political bargaining process, because no country will launch a cyber war *ex nihilo*. He concludes that the impact of cyber warfare capabilities on the frequency of interstate war is limited: “in most cases, it is unlikely to significantly increase the expected utility of war between actors that

[9] Reardon and Choucri (2012) found 49 articles in 26 academic journals for the period 2001-2010 about the role of cyberspace in international relations. Only 19 articles specifically treated cyber security. The four other major issue areas are global civil society, governance of cyberspace, the effect of cyberspace on authoritarian regimes, and economic development.

would otherwise not fight" (2012: 408). In terms of power, Joseph Nye (2011) also adheres to the view that states will remain the key players in the future. Cyberspace diffuses power to smaller states and non-state actors, but it will not undermine the power of large states entirely: the "relative reduction of power differentials is not the same as equalization. Large governments still have more resources. On the Internet, all dogs are not equal." What is more, "[b]ecause the physical infrastructure of the Internet remains tied to geography and governments are sovereign over geographical spaces, location still matters as a resource in the cyberdomain" (2011: 132-134). Ultimately, Forsyth (2013) therefore concludes that great powers will inevitably create an international cyber regime that will govern cyber behavior.

The most likely reason that realist IR theorizing with regards to cyberspace (and cyber security) remains limited is that cyberspace is often regarded as simply another variable in the equation: how does/did the introduction of cyberspace (variable *x*) influence the global balance of power (variable *y*)? Another complicating factor is that many IR theorists focus on information rather than cyberspace in particular. Indeed, much literature has been written about the "information revolution" and its impact on security. These authors usually conclude that information will be the most crucial source of "soft power" in the future. States that control information resources will see the balance of power tip in their favor (Keohane and Nye, 1998; Nye, 2004b; Nye and Owens, 1996). Newmyer (2010), for example, reveals how China is attempting to use the information revolution to mitigate US global preponderance. Yet, information also constrains states in their actions when it comes to security—both on the offense and defense—because non-state actors can counter raw power with information power (Rothkopf, 1998).

What unites the aforementioned authors is their ontology. Cyberspace, as said, is another external factor that has to be taken into account in the security equation. To put it differently, cyberspace is an exogenous cause that shapes the actions of particular actors

(effects). Cyberspace is, to be sure, both literally and figuratively a man-made construction, but now it is "out there" in the world existing independently of an observer. It has become, so to say, an objective fact. It independently causes certain effects, which states may attempt to use or mitigate. The second group of authors, by contrast, goes entirely counter to this logic, subscribing to a constructivist ontology. As the term suggests, for them reality is a social construct, meaning so much as that we give meaning to objective matter through social interaction (Wendt, 1999). An important term in this regard is intersubjective agreement, a shared understanding between actors of a certain phenomenon. A threat does not become a threat until we agree that it *is* a threat. The textbook example is the case of nuclear proliferation (and deterrence). Nuclear weapons as physical objects *by themselves* are not a threat; they do not take sides. Rather, the real threat is how we perceive those who control these nuclear weapons. One (potential) nuclear weapon in the hands of North Korea is viewed as far more threatening to international security than the entire nuclear arsenal of the US. It is for the same reason that people tend to be far more afraid of "the" Chinese hacker than US cyber military operatives.

Constructivist IR theorizing about cyber security thus often refers to the idea that cyberspace and the Internet are quite literally social constructs. It was invented as a university network by computer scientists who had in mind open access in the broadest sense of the word. And by itself this is already an example of intersubjective agreement. It implies that this particular group of people agreed that openness and transparency are desirable—even morally superior to their respective opposites given the spirit of academia—making cyberspace by definition *not* value-neutral. So, as Deibert corroborates, "cyberspace is not an empty vessel or neutral channel. How it is structured matters for identity, human rights, security, and governance" (2013: 6). In other words, the way cyberspace is structured tells much about the views (and interests) of those who created it, and of those who now try to

transform it. Different groups have a different view on cyberspace, or it is perhaps the first group that changes its initial view to something else. What is more, an altogether new group may bring in yet another view.

If we extend these last points to the case of cyberspace we can see that, especially after Stuxnet, the security discourse has come to dominate the cyber security debate (hence the term "cyber *security* debate") and is indeed militarizing. This trend has not eluded a number of scholars in the constructivist tradition, who argue that the case is well-suited for analysis with a subjective ontology. These authors tend to take threat perception as a starting point, and how such threats are framed (Bendrath, 2001; Eriksson, 2001; Helms, Costanza and Johnson, 2012; Stohl, 2006; Weimann, 2005). Due to a number of factors—such as fear, the influence of the media, politicians trying to promote a certain agenda, and plain ignorance—they argue that cyber threats are (willingly) exaggerated, leading to extreme measures in many different countries.

A more recent school of thought within the constructivist cyber security literature uses securitization theory (Barnard-Wills and Ashenden, 2012; Hansen and Nissenbaum, 2009; Lawson, 2013). Securitization theory, based in particular on the Copenhagen School, describes the process of bringing a certain (political) issue into the security domain. This process contains three elements: the agent who does the securitizing, the issue that is being securitized (the referent object), and the audience which has to be convinced of the issue's (existential) threat to society (Buzan, Wæver and de Wilde, 1998). It is a form of depoliticization that enables the securitizing agent to introduce extreme measures to counter the threat. The most prominent work has been delivered by Myriam Dunn Cavelty (2007, 2008, 2013). Using threat frame analysis, she shows how policymakers and politicians use diagnostic and prognostic framing to forge a link between cyberspace and national security. They diagnose the problem by (excessively) playing into insecurities about the vulnerability

of cyberspace and by reinforcing the fear of a "dangerous Other" who might attack the nation's critical infrastructure through cyberspace, using rich metaphors throughout their discourse. Dunn Cavelty argues, though, that the prognostic frame, i.e. the solutions put forward by the securitizers, is actually more important. And it is here where she draws a notable conclusion: securitization of cyberspace has failed. Because of the decentralized nature of cyberspace, the proposed countermeasures to cyber threats are downloaded to private actors. Contrary to the diagnosis, the prognostic part is not fully linked to national security; that is to say, no extreme measures are being taken at the *national* security level, which is exactly a criterion for successful securitization (Dunn Cavelty, 2007). Nevertheless, her article was written in 2007, and since then much has changed.

All in all, existing IR literature about the cyber security debate is useful, but has its limitations. Realist literature treats cyber security as another external factor that nation-states have to take into account in their national security policies, constrained by pressures at the global level. In fact, it even goes a long way in explaining why cyber security policy is similar in so many countries. Waltz (1979) already famously pointed to the forces of interstate competition and socialization. Still, while it is certainly true that some aspects of cyber security are bound to national territory—e.g. server parks, cables, and other physical infrastructure—it ignores the transnational character of cyberspace itself. As was already shown, there are several complicating factors that make a strict realist approach untenable: threats and opportunities through cyberspace more often than not come from various non-state actors who can hide behind the anonymity of cyberspace. Moreover, from this perspective, actors and policies are primarily reactive in nature. They simply respond to structural pressures, giving little room for agency. Even if an actor has deviating ideas, she or he will eventually return to the fold, or risk ostracism.

The constructivist cyber security literature, by contrast, convincingly shows how a wide range of actors use several ploys to get cyber security at the top of the political agenda. It demonstrates that such actors use a particular flavor of discourse in an attempt to frame the cyber security debate in such a way that it is almost exclusively about threats rather than opportunities. In other words, the cyber security debate and the resulting policies are quite agency-driven. Actors act proactively rather than reactively. The problem here, however, is that it underestimates the dynamics at the international level. Actors may deliberately choose a particular rhetoric, but it is still in response to structural pressures. Their choices are limited by "material constraints such as costs, range of technological options, path dependencies, or intended consequences" (Fritsch, 2011: 39).

On the surface, the most pressing problem is the apparent incommensurability between the two bodies of literature. Realist accounts hardly focus on discourse at all, whereas the constructivist accounts are fixated on unraveling one version of cyber security discourse without offering alternatives. Authors in the constructivist tradition argue that realists are (deliberately) exaggerating cyber threats, whilst on the other hand realist authors respond by saying that constructivists are not taking the cyber threat seriously enough. This is unfortunate, because the groups can learn a lot from each other. The material reality of cyberspace—which may sound like an oxymoron—is given meaning by the social reality of cyberspace, and *vice versa*. That is to say, they are mutually constitutive.

If this is the case, then both schools of thought must be researching an underlying factor that co-constructs both realities, and which thus far has not been examined in-depth. This factor is, perhaps counterintuitively, the *instability of discourse*. After all, both bodies of literature have in common that neither asks the *why* question. Why was this particular discourse chosen over another? The existing literature is inconclusive. Realists argue that cyber security discourse is a natural response to a natural order of things: security discourse is

taken for granted and assumed to be static. Yet constructivists only show how this discourse made it to the top of the political agenda. They are correct to argue, however, that the connection between cyberspace and national security is anything but natural. Still, it implies that there is a "causal" link between *a priori* existing identities and cyber security policies in the sense that the former largely determines the latter. This is a questionable assumption because it does not take into account that policies produce and reproduce certain identities. In the case of cyber security policy, it builds on existing foreign policy from other fields of security, which in turn are the result of earlier competing discourses. The following section explores these considerations further.

A poststructuralist approach to cyber security policy

To analyze the relationship between identity and cyber security policy this thesis uses a *poststructuralist* approach. It is important here to emphasize the word "approach": poststructuralism is not a theory *per se*, in that it is uses models to explain and/or predict various processes in the world. It is not, in other words, a problem-solving theory: foreign policy is not merely the outcome of factors *x*, *y*, and *z*. This would assume that such factors exist independently of an observer. Poststructuralism within the field of IR rejects this assumption, and instead views foreign policy as discursive practice. It argues, explains Hansen, that "foreign policy discourses articulate and intertwine material factors and ideas to such an extent that the two cannot be separated from one another" (2006: 1). To say for instance that "the international system is anarchic" is a *representation* of the world. The world does not independently present objective categories to the observer, rather the observer interprets the world through a lens that is constituted by the identity of that observer. Foreign policy, such as cyber security policy, based on that particular interpretation of the world will then reinforce that identity. The poststructuralist focus on language and discourse thus bears

some resemblance to constructivist literature. What sets the two apart, however, are their respective conceptualizations of language and discourse, as will be elaborated upon throughout the remainder of this chapter and the next.

Poststructuralism employs a linguistic ontology. It is through language that we construct reality and imbue it with an identity. Language is thus not a tool to "objectively" describe reality but an inherently social and political medium (Shapiro, 1989: 13-14). It is *social* in that individuals collectively share a common knowledge of (linguistic) conventions that enable them to understand each other. We know that the sound "table" is connected to the object "table." Language is *political* because it is the "site for the production and reproduction of particular subjectivities and identities while *others are simultaneously excluded*" (Hansen, 2006: 16, emphasis added). What follows from this is that not only do we understand a concept by particular signs but also by what it is *not*. Hansen (ibid.) refers to this as processes of linking and differentiation. She illustrates, for example, how a man is described as rational and intellectual while a woman is portrayed as emotional and motherly. Both pairs of words connote positively with their respective gender (*linking*), but at the same time the pairs are negatively juxtaposed (*differentiation*). In binary pairs such as these one term is always valued higher than the other. Consequently, the man is privileged and considered more capable to lead the public sphere, while the woman is relegated to the domestic sphere. In itself this portrays another juxtaposition: rationality is seen as morally superior to emotionality. More egregiously, however, we can see how this enabled the exclusion of women from the public sphere for such a long time. The previous also means that language, apart from being structured through linking and differentiation, is simultaneously unstable and thus prone to change over time.

In Chapter 2 we already asked the question how to understand cyber security. The conclusion drawn then was that cyber security was the security *of* cyberspace. The more

fundamental question should be, however, how to understand the meaning of the term *security*. The most common understanding in IR is security as the absence of any form of foreign coercion. It seems so obvious that it is nearly irrefutable. But, as R.B.J. Walker (1990) shows, this too is an historical construct that gradually congealed over the past centuries. The concept of security is tightly linked with state sovereignty. After the breakdown of feudal hierarchical societies with monarchs legitimizing their rule through divine rights, Walker claims that state sovereignty became the resolution to "the apparent contradiction between centralization and fragmentation, or, phrased in more philosophical language, between universality and particularity" (1990: 10). State sovereignty therefore creates and reconciles many binary oppositions. It implies that there is one world but many communities. More important, in his later seminal work *Inside/Outside: International Relations as Political Theory*, Walker (1993) notes that the concept of state sovereignty suggests spatial and temporal demarcations. Within the state, justice and other virtues can be pursued; outside the state, only relations are possible. Within the state, one can make progress; outside the state is only chaos and backwardness. Thus, Campbell (1992) writes, "securing an ordered self and an ordered world – particularly when the field upon which this process operates is as extensive as the state – involves defining elements that stand in the way of order as forms of 'Otherness'" (1992: 55). Security therefore becomes an ontological necessity, because a state's identity depends on it, and thereby also legitimizes the necessity of violence (Hansen, 2006: 30; Walker, 1990: 12).

From the preceding discussion two conclusions can be drawn. First, poststructuralism argues that there is no extra-discursive reality that presents itself independently to the observer. This does not mean, it must be emphasized, that it denies that there is a *material* reality. A machine gun is very real and very deadly. The point is, however, that the machine gun as such is meaningless without a discursive structure. For some, e.g. supporters of gun

rights in the US, it can be viewed as a tool to defend yourself; others, e.g. politicians, can construe it as a tool of coercion when in the hands of a (perceived) enemy. Ideas and materiality cannot go without each other. Second, it follows that discourse requires political agency, both in the literal and figurative sense. A political actor has to spell out, through discourse, what (national) identity exactly comprises. And, more important, political actors have to propose policies that construct objects, subjects, problems, and actions to engage these problems in response (Hansen, 2006: 19).

Hence, foreign policy cannot be understood as merely a product of a pre-given, stable identity. Like ideas and materiality, identity and policy imply each other. Looked at it from this perspective, as Campbell (1992) aptly put it, and which is worth quoting at length, foreign policy

> shifts *from* a concern of relations *between* states which takes place *across* ahistorical, frozen, and pregiven boundaries, *to* a concern with *the establishment of the boundaries* that constitute, at one and the same time, the "state" and "the international system." Conceptualized in this way, foreign policy comes to be seen as a political practice that makes "foreign" certain events and actors. . . . The construction of the "foreign" is made possible by practices that also constitute the "domestic." In other word, foreign policy is "a specific sort of *boundary-producing political performance*." (1992: 69, emphasis in original)

Here we get to the crux of the matter: there is power in discourse. The domestic-foreign dyad constructs identity through inclusion and exclusion, through creating a Self and Other. Discourse represses and marginalizes opposing views, yet is also productive. Foucault

(1977/1991) referred to this as “productive power”: “it produces reality, it produces domains of objects and rituals of truth. The individual and the knowledge that may be gained of him belong to this production” (1977/1991: 194). Discourse thus *disciplines* identity, by virtue of knowing what identity we are not. Moreover, it simultaneously disciplines the appropriate range of responses (policy).

What, then, is the purpose of foreign policy *discourse*? From a poststructuralist point of view it is about creating a stable link between identity and policy. Hansen (2006: 26) characterizes this link as an equilibrium. If it goes out of balance, it will try to rebalance itself, either on the identity side or the policy side. Therefore, an identity-policy construction requires, first, internal stability, in that it must be consistent. In addition, internal stability is situated within a political context: it is supported or contested by other discourses. Second, Hansen writes, an identity-policy construction is faced with external constraints. These include the partially structured nature of discourse. As seen above, discourse disciplines identity. But it also includes material factors than constrain policy, such as technology, military capabilities or pressures from the media. These do not exist though, Hansen underscores, objectively, but are “situated within, or products of, older and competing discourses” (2006: 27).

Returning to the heart of the matter of this thesis, we can observe that a number of discourses about cyberspace and cyber security have come and gone. Cyberspace and the Internet were envisioned as an open commons, but are now on the brink of, in the words of worldwide web creator Tim Berners-Lee, becoming “balkanized” (Kiss, 2014). Nissenbaum, moreover, already in 2005 identified two competing discourses with regards to computer security. On the one hand, the computer science and engineering community propagated a “technical computer security” discourse, which focused on individual systems and networks. On the other hand, the “cyber security” discourse focuses on collective security, and was

situated within government and corporate circles (Nissenbaum, 2005: 63). By now it is clear that the cyber security discourse gained the upper hand, which is evidenced by the fact that this thesis too almost exclusively speaks of cyber security. The question remains, however, why "cyber security" and not "technical computer security" discourse became dominant, or for that matter any other discourse.

In order to find an answer, we must combine the insights provided by Hansen and those by Campbell and Walker. Hansen argues that foreign policy discourse wants to maintain the equilibrium between identity and policy. Next, we can deduce from Campbell and Walker that the equilibrium is underpinned by state sovereignty. State sovereignty requires boundaries, and foreign policy discourse creates just that. As we have seen, this is ontologically necessary: a state requires boundaries in order to secure its identity, to know what its identity is (Self) and what is not (Other), and to produce commensurate policy frameworks. From this perspective, the reason why one foreign policy discourse is chosen over another is because it is (ostensibly) better capable of maintaining the equilibrium between identity and policy.

We currently live in a world ordered by political communities that we call nation-states. This is a socially constructed reality based on the premise that state sovereignty resolves the contradiction between the universal and the particular, as seen above. By contrast, cyberspace and specifically the Internet, assuming for the moment that it is a space or domain comparable to the physical world, were designed to be borderless. It was based on the liberal ideas of free choice and open networks (Leiner et al., 2009).[10] This constituted a universalizing move, because it paid little heed to the particularities of the international system of nation-states. Yet, a universalized cyberspace challenges conventional sovereignty-based identity-policy constructions. A sovereign state necessarily has to secure its identity—

[10] It is worth mentioning here that technology too is far from value-neutral. Discourse produces certain technological choices, which in turn is based on a particular understanding of identity (cf. Foucault, 1977/1991: 194).

an identity constituted by boundaries through foreign policy discourse. But there were, and for now, still are, no boundaries in cyberspace. What is most important here is that this upsets the balance between identity and policy. Identity can manifest in and through cyberspace, but policy has not yet caught up. In more concrete terms, identity was defenseless—insecure—in cyberspace. Thus, in order to reorganize the "*status quo*" a policy discourse had to be adopted that at least has the appearance of creating boundaries in cyberspace. It is not surprising then that the cyber security discourse was chosen over the technical computer security discourse. The cyber security discourse is far more compatible with the state sovereignty discourse in a way that the technical computer security discourse is not. The latter secures individual systems and networks, whereas cyber security discourse is aimed exactly at securing a collective identity. The existing security discourse excludes technical computer security discourse as a feasible alternative.

Moreover, as Hansen (2006) noted, identity-policy construction also has to keep in mind external constraints. It was underscored earlier that a poststructuralist approach does not lose track of material factors: cyber criminals, hackers, and other individuals or entities up to no good are undeniably real. When faced with such a new (external) phenomenon such as cyber crime, it makes sense for policymakers (and, for that matter, IR theorists) to first try to fit in the phenomenon within the existing, most compatible discourse. A cyber security discourse can clearly accommodate such factors much better than a technical computer security discourse, when viewed through the lens of state sovereignty.

Epistemology of poststructuralism

In the preceding section it was argued that poststructuralism subscribes to a linguistic ontology. Identity and policy are constituted and reproduced through language, and there is no extra-discursive reality that presents itself objectively without the need for discourse.

Consequently, poststructuralism adopts a *discursive epistemology* whose analytical focus lies on how identity and policy are articulated (Hansen, 2006: 20-21). Discourse is then the "structured totality" that arises from such articulations (Laclau and Mouffe, 1985: 105). However, it was argued as well that discourse is only partially structured yet also unstable. It is never completely fixed or, to stay with Foucault, discursively unified (Foucault, 1969/2002). He concludes that a discourse cannot be grouped by statements about objects, statements sharing similarity in style, statements about concepts involved, or statements about a thematic, because these are subject to all kinds of transformations or incompatibilities over time. Rather, he proposes, a discourse is unified, paradoxically, by "forms of division," or differently put, "*systems of dispersion.*" The goal of a discursive epistemology is thus to analyze "discursive formations," which he defines as "[w]henever one can describe, between a number of statements, such a system of dispersion, whenever, between objects, types of statement, concepts, or thematic choices, [one finds] a regularity (an order, correlations, positions and functionings, transformations)" (Foucault, 1969/2002: 41). A good metaphor to understand this concept comes from Radford (2003). One should imagine standing in front of a library bookshelf. On the shelf, various groups of books are ordered by a certain criterion, e.g. author or subject. Following the spines of the books, we travel from the texts at the heart of the discursive formation to the texts on the margin. At a certain point, we have arrived at another discursive formation, for instance we have moved from texts about US foreign policy to US history. Sometimes the "cut-off point," i.e. boundary, is clear; at other times, we may have moved between categories without even fully realizing it. Now, the ordering of books will also be subject to certain criteria. These are what Foucault called the "rules of formation" (1969/2002: 42). What Foucault then proposes to study is not so much the contents of books on the shelf, but rather the question why they are arranged in this particular way. More important, it raises the question where these divisions come from. And, as Radford notes,

"What are the grounds for their legitimacy? How might they be challenged and transgressed?" (2003: 4).

Before exploring this in more detail, it adds to the understanding of the argument to show how poststructuralism differs from constructivism. Although both agree that material reality only acquires meaning through discourse, the crucial difference is, however, how poststructuralists and constructivists, especially the Wendtian kind, conceptualize identity. Poststructuralists believe that identity is relational—it is constructed through processes of linking and differentiation. The Self can only know the Self by also knowing what it is not, i.e. the Other. Wendt (1999), by contrast, suggests that identities need not be relational *per se* but can be intrinsic to an individual or an entity, say a state. He refers to this as "type identities" (1999: 225), which is an identity that has certain traits or characteristics regardless of whether it is recognized by another. Concretely, as Wendt puts it, teenagers have certain traits that make them teenagers even if they are not recognized as such by someone else, and, similarly, "a state can be democratic all by itself" (ibid.: 226). This supposes that identities may be pre-social. As far as poststructuralists are concerned, Hansen (2006: 22) notes, this is impossible, because "being" a democratic state is part of that state's self-understanding, which is constituted through discourse. A state understanding itself as democratic excludes, by definition, opposing self-understandings, i.e. it differentiates. The point is that it does not matter that the Other recognizes the Self as being the Self; what matters is that the Self recognizes *itself through differentiation from the Other*. To clarify this further, let us assume the hypothetical situation in which there is one single democratic state in a world system of otherwise non-democratic states. It may be the case that the single democratic state is not recognized as such by the other non-democratic states, but the single democratic state itself still knows beyond question that it is democratic because it is certainly *not* non-democratic.

Assuming that identities are pre-social reveals another characteristic of constructivism that poststructuralism takes issue with. Although they share that identity has a constitutive effect on policy and political behavior (i.e. they both "endogenize" politics), the constructivist argument that identities are intrinsic means that they are also deterministic in nature. To put it black and white, a "democratic" identity necessarily leads to "democratic politics," just as a "dictatorial" identity must lead to "dictatorial politics." It is exactly this kind of causality, which is grounded in a positivist epistemology, which poststructuralism rejects. To recapitulate, poststructuralism believes that identity and policy are ontologically linked: they both constitute and reproduce each other through discourse. For a constructivist like Wendt discourse is static with fixed meanings. It has to be, otherwise a concept like identity cannot be used to "explain" certain outcomes or tested against other variables.

Yet here we arrive at a problem for poststructuralism, at least from a positivist perspective. As Campbell observes, a positivist epistemology subscribes to *epistemic realism*, the idea that there is an external world with meaning independent of observance and thought, and to *correspondence theory of truth*, the idea that the "facts" of the world can be captured in objective statements that are true or false (2010: 218). It therefore demands that theories hypothesize. So how can a poststructuralist analysis "explain" the world? It cannot, in any case not in the strict sense of causality that a positivist epistemology envisions. The point is, however, that poststructuralism does not claim to do so. It is "concerned with the manifest political consequences of adopting one mode of representation over another" (ibid.: 232). The research question of this thesis, why did a collectivized cyber security discourse become dominant over the more individual technological computer security discourse, is thus not so much about *explaining* which *factor* leads to the choice between discourses as it is about *understanding* why one discourse within a range of possible discourses became dominant. And even if, hypothetically, an analyst could narrow down *the* one specific factor which

informed a decision-maker's choice, then still that factor is historically produced and situated within a particular discursive formation. Moreover, it still says very little about the appropriateness of the chosen discourse within this particular situation. While it may be good to know that factor *x* "caused" decision *y*, we still do not know why decision *y* should be, or is constructed to be, the most appropriate response to factor *x*. Again, this requires understanding the historic and discursive specificity of the situation (Hansen, 2006: 30).

Poststructuralism, in short, goes against positivist foundationalism that underpins causality. It does not accept that there are ahistorical, universal rules that exist independently of the observer. Yet here, then, poststructuralism seemingly faces a paradox. If it argues that nothing is universal, then by definition everything must be particular. But then that must mean that if everything is particular, there in fact does exist a universal rule independent of thought and observance, namely that everything is particular. That, in turn, means that actually *not* everything is particular. Poststructuralism responds to this, recalling Foucault, by positing that groups of statements are unified through dispersions. Should one accept the previous line of reasoning, then that means assuming that the universal and the particular are mutually exclusive. It implicitly accepts that the meaning of the two are fixed and absolute. A poststructuralist, such as Ashley (1987), would argue however that the paradox exactly underwrites their point. The universal and the particular need each other to stabilize their existence. The crux is that something, e.g. national identity, can take on the appearance of being universal, thereby obscuring its particular origins. Returning to international politics, discourse thus tries to *create* stability, but it never fully can. Since this is the case, Hansen further observes, then it is possible to analyze the *relative* stability of discourse. It is for this reason that this thesis subscribes to what Hansen calls a *theoretical model of combinability*: foreign policy discourse "constructs identity and policy by mutually adjusting the two. . . . One might think of this model as a system of equilibrium: . . . if there is an imbalance in the

construction of the link between identity and policy there will be an attempt to make an adjustment to recreate stability through modification of either the construction of identity or the proposed policy" (2006: 26). The same model may be applied to the construction of identity itself, which is the focus of the next section.

Performative identities

With the heavy focus on identity, it is paramount to discuss how poststructuralism understands it. We already established on multiple occasions that identity is created by and constituted through discourse. This meant that discourse was simultaneously social and political, and that discourse contains productive power. Although the processes of differentiation and linking were mentioned briefly earlier, what has not been addressed thus far is along which dimensions these processes then enable the construction of identity. What follows, first, is a discussion on how poststructuralism conceptualizes identity, and, second, how poststructuralism understands the construction of identity.

The concept "identity" within poststructuralism can be summarized in four key terms: it is discursive, social, relational, and political (Hansen, 2006). That poststructuralism understands identity as *discursive* is by this point self-explanatory. Identity is constituted through discourse. It was already argued that identities do not exist independently in an extra-discursive reality; that is to say, identities are not pre-social, as some constructivists claim. A consequence of this is that identity cannot be used as a "variable" in the positivist sense or that it can be tested against other variables. Since identities are discursive, and discourse itself was viewed as inherently unstable, it means that identities too are contestable. This reveals the *social* nature of identities. They are established "through a set of collectively articulated codes . . . constituted within and through a collective terrain" (ibid.: 6). This can be compared to what constructivists call "intersubjective agreement" (Wendt, 1999). Actors understand

themselves through the beliefs in their heads with regards to identity (subjectivity), and understand each other because they share those ideas collectively (*inter*subjectivity). Crucially, however, identities must in addition refer to what they are not, i.e. they are *relational*. This sets poststructuralism decisively apart from constructivism. While they agree that identity is articulated within and through a group, poststructuralism argues that this is still meaningless unless actors know what differentiates their identity from another. Lastly, poststructuralism conceptualizes identities as *political*, because ultimately it is a choice who or what belongs to a certain identity and what does not. Identities thus produce boundaries that lead to the inclusion of certain aspects and the exclusion of others. Here again we see the productive power of discourse: it creates a particular reality and disciplines the knowledge deemed appropriate in it.

It follows that identities always articulate a Self and a range of different Others, in the case of this thesis through foreign policy discourse (Campbell, 1992). In classic security discourse, the Self, a political community within a well-ordered national domain, has to be guarded against the disorder, ambiguities, and dangers from without, the dangerous Others. Still, it is not so much that these dangers exist objectively as that they are ontologically necessary for the construction of the Self. Campbell locates this necessity in Christian thinking. Whereas earlier the church provided salvation for its followers so as to escape the danger of an "unredeemed death," the state similarly legitimizes itself by offering security to its denizens who would otherwise face "manifold dangers;" both thereby "engage in an evangelism of fear to ward off internal and external threats" (1992: 56). Viewed from this perspective, international politics becomes a "knowledgeable practice of statecraft," Ashley concludes, "that functions to produce the effects of modern domestic societies . . . [It] is a practice of the inscription of the dangerous, and the mobilization of populations to control these dangers—all in the name of a social totality that is never really present" (1989: 304).

Identities are thus *performative*: they are "constituted by the very 'expressions' that are said to be its results" (Butler, 1990/2006: 34). It is no accident that poststructuralism argues that the "state" and the "international system" emerged "coeval[ly]" (Campbell, 1992: 69). Neither the state nor the international system existed prior to one another, but is rather the outcome of the dialectic between identity and policy.

Having argued that identity results in the articulation of Selves and Others, we must now, lastly, turn to *how* identities are constructed. Hansen (2006: 41-45; see also Walker, 1990) again provides a useful framework. While identity constructions are founded on a complex web of linking and differentiation, in general their signs can be viewed through three different analytical dimensions: spatiality, temporality, and ethicality. None have ontological precedence over the other, but rather have equal status and imply each other. Each will be addressed below.

To construct identity *spatially* is to subscribe to the view outlined above that identities are relational and produce boundaries. Identities may be delineated by boundaries that circumscribe a physical (i.e. territorial) space, but may also comprise abstract spaces. In terms of the former, the most common way to construct spatially an identity is the nation-state. A population is referred to as e.g. "Dutch," "Belgian," or "Luxembourgian." Still, such territorially bounded identities need not be absolute. If anything, such identities tend to be fluid, transcending the national borders. The Netherlands, Belgium, and Luxemburg often present themselves as the "Benelux," a group of likeminded countries different from, say, their French neighbors in the south and their German neighbors in the east. On an even higher scale, the Benelux countries claim to be European through and through; the list of possible spatial identities is anything but exhaustive. Here we also find the saliency of identity's relational aspect: spatial identities are so easily recognized because they always differentiate

from something else. Within the Netherlands, for instance, inhabitants from the provinces of Limburg or Friesland often claim to be culturally different from the rest of the country.

As noted, an identity may also be delineated along an abstract spatial axis. To put it differently, such identities are grouped by certain subjectivities, and are usually politically and/or socially motivated. Examples of this are identities centered around discourses about "barbarians," "the people," "homosexuals," "civilization," and so on. In addition, such political subjects, Hansen points out, are often mixed with territorial identity. In March 2014, the Dutch politician Geert Wilders, for example, infamously called for "fewer Moroccans" in the Netherlands. By thus referring to Moroccan Dutch citizens simply as "the Moroccans" he not only turned them into political subjects but also invoked a territorial connection with Morocco. From his perspective, they are different from "the Dutch," and, what is more, he removes their link with the Netherlands as a nation-state.

Secondly, identity is *temporally* constructed. To that end, themes such as change vs. continuity or progress vs. stasis play an important role in discourse. Similar to above, we can discern a territorially bounded and an abstract construction of temporal identity. Poststructuralism's emphasis on the coeval emergence of the state and the international system shows how such spatial entities are historically produced. Walker (1990, 1993) locates this development primarily in the principle of state sovereignty. The principle makes a temporal distinction, he writes, "between the progress toward universalizing standards possible within states and the mere contingency characterizing relations between them" (1990: 12). Economic, cultural, or political progress is possible within states, whereas between states relations are sadly doomed to the recurrence of power politics, so (classic) realist discourse goes.

Foreign policy discourse also constructs temporal identity in a more abstract sense. Again, the Self/Other dichotomy plays an important role. Specifically, Hansen (2006: 43)

observes, the temporal Self is constituted with reference to a temporal Other. It asks whether the Other has a capability for changing (or not) and whether the Other is inferior (or superior) to the Self. Note here that the latter contains an ethical component, more on this momentarily. The Self may present itself as "modern" or "developed," as opposed to a "primitive" Other. Should the Other be fortunate enough, in the eyes of the Self, to be capable of changing, the Other may be designated as "developing" or being "in transition." Should this not be the case, then the Other is "backwards" or "savage." During the early phases of 2011 Arab Spring, president Obama praised Tunisian demonstrators, who showed that "the will of the people proved more powerful than the writ of a dictator" (Lizza, 2011). The democracy aspiring Tunisian "people" were distinguished from "the dictator" who still preferred the old ways. Whereas the people demanded democratic change (superior), the dictator backwardly tried to hold on to power through repression (inferior). In addition, the reverse is also possible: the Self could also present *itself* as inferior to the Other. When negotiations started for the 2004 EU enlargement, many Central and Eastern European governments used a "return to Europe" rhetoric to emphasize that they had always belonged to Europe, but that they had been held back by the post-World War II communist rule (Schimmelfennig, 2001).

Lastly, as was hinted at above, identity is constructed *ethically*. The previous paragraphs revealed how identities are always relational, and that one term within a dichotomy is deemed superior to the other term. A return to Europe is normatively preferable to remaining in a communist-laden past. It is better to have democratic aspirations than to live under the yoke of dictatorship. In the end, the goal of foreign policy discourse is to legitimize foreign policy. It needs support of a receptive audience (which may vary depending on the situation). Constructing, then, identity in terms of good and bad, of what is proper and what is improper, is to invoke tremendous moral force. In 2003, in an attempt to justify the military intervention in Iraq, president Bush claimed that Saddam Hussein was producing weapons of

mass destruction that would inevitably pose a threat to (American) liberal democratic values, making invasion a right and proper response. A similar line of reasoning, although less explicit, based on classic security discourse can be found in the cyber security debate. The lone wolf, terrorist organizations, and even foreign governments are threatening national and economic security through cyberspace. In order to protect liberal values, the introduction of various measures—expanding offensive military capabilities, increasing cyber surveillance, and so on—appear justified. All told, the ethical construction of identity returns to what early poststructuralists like Campbell (1992), Ashley (1989), and Walker (1990, 1993) had already theorized: the universalized identity of the nation-state has to be guarded against the contingencies of the international system.

Poststructuralism's construction of identity as spatial, temporal, and ethical emphasizes the dynamism of identity. It is constituted by discourse, which is theorized to be inherently unstable. Hansen (2006: 45) explains that changes in one of the three dimension puts pressure on the other two. Policy adjustments (or continuity) tend to follow. Such changes in, and choices between, discourses can be traced.

Summary

Although much has been written on cyber security, surprisingly few studies have been informed by theory. Of those scholars that did try to account for developments in cyber security discourse, we saw that they analyzed the question along the well-known paradigmatic lines of IR. They either look at how cyber threats will affect the international system (realists) or how cyber threats became constituted as threats to national security (constructivists).

Still, the existing literature has not yet answered why this particular cyber security discourse was chosen over another. The second section therefore introduced poststructuralism

as an approach to address this gap. It argued that identity and policy are ontologically interlinked, and that the link is constructed by foreign policy discourse based on the concept of state sovereignty. This discourse was characterized as an equilibrium: it has to balance identity and policy. If the identity-policy constellation goes out of balance, it was deduced, then the discourse that is more compatible with state sovereignty discourse will be chosen to restore the balance.

The last two sections discussed epistemological considerations concerning poststructuralism. It argued that identities do not exist pre-socially but are socially constructed. Moreover, it explained that poststructuralism did not subscribe to a positivist conception of causality, using a model of combinability instead. This model suggested that identity and (foreign) policy are mutually adjusted to each other. Next, since identity is a crucial concept in poststructuralism, the chapter explored how identity is conceptualized. Poststructuralists argue that identity is constructed along a spatial, temporal, and ethical dimension. More important, identity is theorized to be performative: identities are constituted by the very effects they are said to "cause."

Adopting a poststructuralist approach is not without its complexities. Because of its more meta-theoretical nature, it will be clear by now that it is necessarily more abstract than a theory like structural realism. One complexity was already touched upon: poststructuralism rejects causality. This does not mean, however, that it is impossible to empirically analyze whether the above expectation holds. These and a number of other methodological consequences in terms of analysis and research design will be addressed in the following chapter.

CHAPTER 4

ANALYZING CYBER SECURITY DISCOURSE

Analyzing the cyber security debate through a poststructuralist lens requires a method that places discourse at its center and is sensitive to the ways identity and policy are articulated. Moreover, a method has to be epistemologically sound: adopting a poststructuralist method means choosing to accept a number of assumptions that are different from conventional positivist scientific research. The previous chapter described that poststructuralism rejects causality (in social sciences), an idea central to positivist research. This does not mean that it is impossible for poststructuralist research to "explain" how the world works, but rather that it asks a different set of research questions.

The following section delves deeper into some of methodological considerations mentioned above. It first introduces the concepts of intertextuality and genealogy. These concepts are at the core of the type of discourse analysis that this thesis uses in the empirical chapter, and are in line with the discursive epistemology mentioned previously. Next, it discusses predicate analysis as research method to analyze the discursive link between identity and cyber security policy. The second section then turns to the practical matters of this thesis, discussing research design, case selection, and sources, respectively. Studying discourse necessarily relies on analyzing texts. To that end, an intertextual model created by Hansen (2006) is used to narrow down the *scope* of texts and which *type* of texts are selected, to which a number of selection criteria are added to decide which documents will be analyzed.

Methodology of discourse analysis

The main argument of this thesis is that discourse attempts to stabilize the link between identity and policy and that this link is constituted by the concept of state sovereignty. Foreign policy creates boundaries through discourse. Such constitutive moves instigate dispersions of knowledge of power across spatial, temporal, and ethical dimensions, which, as Foucault reminds us, is exactly what unites them. New (discursive) challenges like cyber security are thus subjected to older, existing discourses, and then transformed. Studying these transformations means that we have to analyze how newer discourses relate to older ones. This has three methodological implications, each of which will be discussed below; their analytical consequences are discussed at the end of this section.

First, the notion of *intertextuality* is crucial in a poststructuralist discourse analysis. Intertextuality, a term coined by Julia Kristeva, suggests that "any text is constructed as a mosaic of quotations; any text is the absorption and transformation of another" (1980: 66). Each text is unique but always situated in an existing textual space. Texts refer back to older texts, which in turn refer back to even older ones. They add to history and are simultaneously a product of history. Texts are constructed to have authority, but not every type of authority is exactly alike. Moreover, authority is located in different locations, viz. the author, the text itself, and even the audience. A text may be authoritative because its author is (or appears to be) knowledgeable, or because a text is (perceived to be) a key text within a certain field. For instance, many if not all scholars of cyber security studies refer to Arquilla and Ronfeldt's seminal article "Cyberwar Is Coming!" (1993), in much the same way as most IR theory scholars at one point, whether they want to or not, probably turn to Waltz's *Theory of International Politics* (1979). This also underscores the productive power of discourse, and that power is dispersed across discourses (Doty, 1993). More important, it shows the partially structured nature of discourse. Intertextuality emphasizes that texts are part of an ever

expanding complex web of texts, but the exact position of a text within the web is largely dictated by what is considered appropriate given a certain discourse. The cyber security discourse guides new texts to a part of the discursive web that is characterized by concepts such as sovereignty, national security and "cyberrealism" (Manjikian, 2010). This suggests that the authority of a text also derives from power: existing discourses discipline how new texts will fit in, thereby including some narratives but excluding or marginalizing others. Again, the question arises where this type of authority is located. The author of an important text may see his power position increasing in subsequent texts. Others may read his text not so much because of the text itself but because of who wrote it. Yet the flipside of the coin is that a particular audience, e.g. a group of academics in the field of cyber security, has recognized a text as *being* authoritative (either because of the text itself which is deemed knowledgeable or because of the author wrote it). In sum, a text invokes the authority of preceding texts, which will reflect positively on the newer narrative (and by the same token negatively on deviating narratives).

Intertextuality comes in different forms. Explicit references are the most visible, usually direct quotations or references to existing texts. As discussed, these older works have authority, and have to be assessed or criticized. The bulk of intertextuality, however, tends to be more subtle. Hansen (2006: 51) identifies conceptual intertextuality and the use of catchphrases as *implicit* forms of intertextuality. Authors and texts often refer to older concepts so as to appeal to their history, thereby gaining legitimacy. What is more, Hansen notes, creating such an intertextual link is a two-way exchange. Not only does the concept gain legitimacy because it invokes the authority of an older concept, but, in reverse, the older concept also obtains more legitimacy by virtue of being used. Using a term like "cyber security" or "cyber warfare" relies on earlier bodies of text about "conventional" security. The same applies to using catchphrases, such as "cyber Pearl Harbor."

The second methodological implication is that a poststructuralist discourse analysis adopts a *genealogical* approach. This is a method of historical studies that does not view history as a linear progression towards an end point but rather sees history as moving forward through series of contingencies. It "record[s] the singularity of events outside of any monotonous finality" (Foucault, 1977: 139). A genealogical study "asks how what we 'know' now has become the understanding of history" (Hansen, 2012: 105). It thus focuses on and makes problematic dominant discourses, and traces how other discourses have been excluded (Milliken, 1999). A conceptual history of, say, cyber security examines how the current understanding of the term is rooted in historical contingencies. It questions the "objectivity" of the term to which many authors mentioned in the previous chapter subscribe, and shows how things could have been different if the term was interpreted in another way. As Hansen (2012: 106) rightly points out, a genealogical study shifts research away from the question of what we know something *is*, to what *role* a particular (historicized) understanding of a concept like cyberspace plays in legitimizing policy.

In a way, intertextuality is thus genealogical at its core: texts are theorized to absorb and transform older narratives, thereby both gaining legitimacy. A genealogical study would then draw attention to the contingent nature of the two-way exchange described above. The referencing to or quoting of an original text in a new narrative is always a rereading or reinterpretation of said original; the meaning of original texts is thus never fully reproduced (Hansen, 2006: 51). New narratives are products of their time just as much as older texts are products of theirs. That is to say, both are disciplined by the respective terms and conditions of their time rather than stemming from an elusive origin that reverberates into the present. Authors pick and choose texts, concepts, and catchphrases because it is opportune for them to do so. In true Foucauldian fashion, they are part of power-knowledge constellations. Texts are constructed to have authority, yet the authority of those texts depends on the dominant

discourse. Consequently, alternative discourses have less or no authority as a result, and tend to be marginalized, excluded, or simply not taken seriously. What is more, older texts will be viewed through a new lens. We have seen and will see in the next chapter for example that policymakers often rely on metaphors like cyberspace as being lawless—echoing the lawlessness of the old American West—or predicting a "cyber 9/11," a metaphor which needs little explanation. Mobilizing particular readings of history, in short, enables and constrains the range of policy options.

Lastly, a poststructuralist discourse analysis has to make a number of choices with regards to its methodological toolbox. Genealogy and intertextuality highlight the unstable nature of discourse. Poststructuralists argue that discourses are never completely fixed, which leaves room for variation and contestation among discourses. Methodologically speaking, the *level* of analysis must then be discourse. However, it is not the discourses *per se* that are being analyzed. Here, we briefly have to take one step back and return to the concept "discursive formation" that was introduced earlier, which was defined as a series of regularities between objects, subjects, types of statements, et cetera. A discourse, according to Foucault, is then "a group of statements in so far as they belong to the same discursive formation; . . . it is made up of a limited number of statements for which a group of conditions of existence can be defined" (1969/2002: 131). This suggests that a discursive formation may either contain multiple, contradicting and/or competing discourses at the same time or that one discourse has completely supplanted an older discourse. This thesis asks the question how a choice between competing discourses is made, putting us on the level of agency. Therefore, the *object* of analysis is the discursive *practices* that constitute discourses. Such discursive practices, another important concept for Foucault, are "the body of anonymous, historical rules, always determined in the time and space that have defined a given period" (ibid.: 131). Moreover, adds Doty, "[they are] not traceable to a fixed and

stable center . . . Discursive practices that constitute subjects and modes of subjectivity are dispersed, scattered throughout various locales" (1993: 302). Additionally, she explains elsewhere, discursive practices "put into circulation representations that are taken as 'truth'" (1996: 5).

In order to "measure" discursive practices, this thesis uses *predicate analysis*, a method which "enables [one] to get at how discursive practices constitute subjects and objects and organize them into a 'grid of intelligibility'" (Doty, 1993: 306). Predicate analysis uses three analytical categories: predication, presupposition, and subject positioning. It focuses, first, as the name suggests, on how terms are predicated through the verbs, adjectives and adverbs that are attached to them. That is to say, it looks at the labels that construct the meaning of certain things (Milliken, 1999). For instance, the Dutch National Cyber Security Strategy asserts that "ICT is of fundamental importance for our society and economy" (Ministerie van Veiligheid en Justitie, 2011: 3). This *predication* constructs ICT as a subject with societal and economic qualities. Next, a predicate analysis looks at *presuppositions* made in texts. Every text employs background knowledge that is assumed to be "true." Without such background knowledge, it is nearly impossible to make sense of the meaning of a text. A statement like "In cyberspace, the offense has the upper hand" (Lynn, 2010: 99) assumes that cyberspace is comparable to physical domains, that a logic of offense/defense applies, that conventional strategic thinking also works in cyberspace, and that the author is in a position authoritative enough to make this claim. Third, texts produce a reality by positioning a subject or object *vis-à-vis* another. This *subject positioning* is comparable to Hansen's processes of linking and differentiation. To recapitulate, we know something by knowing what we are not, i.e. the relational quality of discourse. Two terms are juxtaposed, with one being dominant over the other. Speaking of "cyber war" means that there must also be "cyber peace." Moreover, to both terms various qualities are ascribed:

cyber war as characterized by aggression or potential loss of lives, cyber peace as non-aggression or amicability. Note that presupposition and predication are simultaneously at work here.

Keeping in mind the conceptualization of discursive practices as an historically bounded body of rules that gives rise to representations with a claim to truth, we may interpret, to quote Doty, "what [these] discursive practices *do*" (1993: 305, emphasis in original). That is to say, once we have mapped out the different discursive practices that are present in texts, we can see how they construct identity, and, in turn, how policy reproduces identity. Since poststructuralism adopts a genealogical approach, we have to analyze how identity-policy construction *vis-à-vis* cyberspace has developed throughout time. Furthermore, the intertextual component of poststructuralism analyzes the productive power present in such identity-policy constructions: the several discursive practices used in texts invoke the authority of existing, earlier texts. Combined, the two components should shed light on the process of why a transition in discourse took place. Most likely, the discursive practices either changed in response to actors (endogenously) changing their views with regards to computer security or because of changes in the context (influenced by an "exogenous" event). As always, at the core of these practices is a particular (historicized) representation of identity. Subsequently, readjustments in the discursive formation should take place, followed, in turn, by policy changes in order to adapt to these readjustments. After all, the link between identity and policy has to remain stable. With this in mind, the following section elaborates upon the research design.

Research design: cases and sources

The genealogical nature of poststructuralist discourse analysis implies that discourses are situated within an infinitely large and expanding web of other discourses. Consequently,

different discourses—and the choices made between them—may also be found in an infinite amount of texts. Studying every text even within a clearly outlined field is obviously impossible, meaning that choices have to be made as to which texts to choose for analysis. A common criticism against poststructuralism is that "anything goes," but Hansen (2006, 2012) has convincingly shown that although it disagrees with the assumptions of (conventional) positivist research, it does not mean that a poststructuralist analysis does not use (or need) guidelines for research design. Hansen outlines, first, three intertextual models that guide which kind of texts should be used in an analysis. These three models progressively widen their analytical scope starting from official discourse (e.g. government policy documents, statements by heads of state), to including wider foreign policy debate (e.g. statements by oppositional groups, media institutions), to including cultural representations (e.g. popular culture such as fictional books or movies) and/or marginal political discourses (e.g. statements by social movements or NGOs).

The research in the next chapter uses the second intertextual model. The choice for this model was made on several grounds. First, to analyze which discourse is dominant in cyber security policy, it makes sense to start with official discourse issued by government institutions or persons of authority. In the previous chapter, we saw that the goal of (foreign) policymakers is to produce policies that appear "legitimate and enforceable to its *relevant* audience" (Hansen, 2006: 25, emphasis added). Therefore, publicly available policy documents are the primary source material, which have "official" status or are official responses to questions or criticisms. In addition, it was argued that identity and policy are interlinked. Policy documents, from this point of view, then become the site where identity is produced and reproduced. The link must, however, appear consistent. What matters more is that in such official documents we may find an understanding of how governments envision national identity, and how it came to be that it is this particular representation that is

articulated and not another. Second, to determine if there are multiple discourses in competition, the analysis will also include discourse by oppositional voices, for instance coming from political parties.

In order to further narrow down the analytical scope, we then have to make choices with regards to the number of "Selves," the temporal dimension, and the number of events.[11] The *number of Selves* simply refers to who or what one wishes to analyze, for example states or other foreign policy subjects. Subjects, here, should be understood as entities with an identity. This can be a single Self, or multiple ones, depending on the analytical goal. Here, the goal is to compare how the Dutch government produces and reproduces identity in cyber security policy. Thus, this is a single Self study: its primary focus is on Dutch cyber security discourse. It analyzes whether there are different discourses, and the choices made between them. The empirical analysis will attempt to identify dominant discourses, and whether there are competing discourses. The latter in particular will certainly not be an easy task. If we ask the question why this cyber security discourse became dominant and not another, then that seems to imply that policymakers are able to pick and choose from an "archive" of discourses. The reality is obviously much more complicated, in which it is difficult to discern where one discourse "begins" and another one "ends."

With regards to the case selection itself, in the introductory chapter it was noted that the Netherlands is an increasingly important player in the field of cyber security, which in itself is an interesting development given its more limited resources compared to countries like the US, the UK or Germany. At the root of this development, as will be seen, is the desire to preserve Dutch identity. Still, the next chapter will also show some degree of intertextuality between US and Dutch cyber security discourse. The US has historically been a leading nation in the development of cyberspace and cyber security policy, with many other

[11] For a detailed overview of setting up a poststructuralist research design, see Chapter 5 in Hansen (2006), pp. 65-82.

nations, including the Netherlands, following their example. It will be argued however that even this course of action by the Netherlands is motivated by the wish to preserve Dutch national identity in cyberspace.

Second, the *temporal* dimension asks whether a study looks at a single moment in time or an historical development. It was already made clear that this study uses a genealogical approach, thus looking by definition at a longer historical period in time. Cut-off points in a certain time span are always somewhat arbitrary (especially from a genealogical point of view which rejects the idea of linear progression of history), but obviously not every historical moment or period is as relevant. Following Hansen's (2006: 70) suggestion, this thesis focuses on discourse centered around key moments of political importance. These are moments between the post-9/11 period until late 2013, ending with the "fallout" of Edward Snowden's leaks on global surveillance.

Lastly, and related, the study must decide whether to look at one or more *events* within a given period. "Event" can be broadly defined from as large as "war" to a more specific foreign policy issue as the construction of cyber threats, and can be related by time or space. What matters is that the events have saliency (or consequences) for the development of discourse. This study looks at the construction of cyber security discourse over time, and how this one particular discourse became to dominate rather than another. It was already argued that identities produce and are reproduced by policy, suggesting that a study of cyber security discourse has to look at the construction of "dangerous Others" *vis-à-vis* the Self in texts produced at the time of politically important events. These events include, among others, the negotiating, signing, and implementation of the Convention on Cybercrime, Stuxnet, and, specifically for the Netherlands, the DigiNotar affair.

With the previous considerations in mind, one must finally select the texts. Two criteria that apply are, writes Hansen (2006: 73-74), first, that texts (obviously) date from the

period of time under study, and, second, that these texts serve as "nodes" that structure a discourse. These texts tend to be quoted or referred to often, or carry a certain authoritative weight in the debate. The sources here are mainly official policy documents or strategies issued by the government, and texts produced by oppositional voices (e.g. statements by opposition leaders).

In the end, 44 texts were consulted for the period 1998-2013;[12] of these texts, predicate analysis was applied to a total of 29. All texts were gathered from the government website for official announcements and parliamentary documents.[13] These documents were searched for terms like "cyber," "digital," and "electronic." A list of the used documents can be found in Appendix A. Predicate analyses were applied to these documents, following the example of Doty (1993) and Milliken (1999). The results of these analyses are presented in Appendix B.

Along with the selection criteria mentioned above, a number of other guiding principles were also used. First, "follow the money": implementation of cyber security policy is not free, meaning that every euro spent on it has to be accounted for, and, more important, legitimized. The starting point to look for identity-policy constructions was therefore in the *Memories van toelichting* (Explanatory memorandums) attached to the annual budget proposals for the years 2001-2013 of the ministries of Defense, Foreign Affairs, Security and Justice, and Interior and Kingdom Relations.[14] Second, in order to capture the wider foreign policy debate, the analysis also looked at plenary debates that took place in the *Tweede Kamer* (Second Chamber, House of Representatives), and in the *Algemene Overleggen* (General Meetings) of Permanent Chamber Committees. It is in these debates where the legislative branch has the possibility to review legislative proposals and actions by the

[12] Originally, as explained above, the time span was 2001-2013. During data collection, however, five documents from the years 1998 to 2000 showed up that were relevant enough to include.
[13] https://www.officielebekendmakingen.nl/. All texts were in Dutch, and translated by the author.
[14] In October 2010, the ministry of Justice was renamed to the ministry of Security and Justice, due to its taking over public safety duties from the ministry of the Interior and Kingdom Relations.

government. In plenary debates, members of the Second Chamber (MSC) may, for instance, introduce motions to urge the government to take a certain action, or to refrain from one; in a General Meeting, MSCs have the opportunity to exchange thoughts with one of more members of the government about certain policies. Special attention is paid to members of opposition parties, because it is reasonable to argue that they are the ones who voice competing discourses. The third type of document that was investigated were letters from (relevant) members of the government (ministers and/or state secretaries). In these letters, members of the government answer questions from or respond to requests from MSCs, give progress reports about new legislation, inform parliament about specific developments, et cetera. These letters were included because they might logically be the location where competing discourses meet. Last, the research analyzed a number of reports by government security and intelligence agencies, and two official cyber strategies released by the Dutch government. These strategies present the government's vision about cyber security, threats and opportunities, and how to deal with them in the long term.

On a final note, the data selection does not include sources outside the (parliamentary) debates regarding cyber security. The goal of this thesis is to explain why one discourse became dominant, rather than another, among politicians and policymakers; the study therefore does not explicitly analyze, for instance, media coverage of certain cyber events. Although it can certainly be argued that politicians and policymakers may change their views in response to public opinion, this for now falls outside of the analytical scope. Still, this limitation is not likely to cause a bias in the analysis. We may assume—presuppose, to use Doty (1993)—that politicians and policymakers will always act in the best interests of the people. It is reasonable to argue that they anticipate possible public reactions to events anyway, thereby mitigating the influence of the media. Moreover, we *cannot* assume that the media (or other institutions) automatically speak on behalf of the general public. Analyzing

media coverage would at best "measure" public opinion by proxy, whereas the documents used in this analysis express the views of politicians and policymakers directly.

Summary

This chapter treated methodological questions. It began with a discussion on intertextuality and genealogy. Intertextuality is the idea that all texts are part of an ever-expanding mosaic of texts. Genealogy is a type of historical study that traces how certain understandings or representations of history have become dominant. Predicate analysis was then introduced as method to analyze discursive practices. This method is based on three analytical categories: predication (the language attached to words), presupposition (the background knowledge behind statements), and subject positioning (how the Self is positioned *vis-à-vis* the Other).

The last section outlined the case selection and the sources used in the study. Official policy documents and the wider foreign policy debate in the Netherlands from the period 1998 to 2013 will be examined. The selected texts will, furthermore, center on a number of key events within that period. All told, the analysis should show that identity is mobilized to reestablish the link with state sovereignty. Cyberspace is borderless, leaving identity defenseless. In order to make up for the insecurity of identity in cyberspace, cyber security policy will create boundaries in cyberspace.

CHAPTER 5

CYBER SECURITY POLICY IN THE NETHERLANDS

This chapter presents the empirical analysis of the various documents outlined previously, and is divided into several sections. The sections correspond with three time periods, each ending with a major event in Dutch cyber security policy. This is in line with Hansen's approach to focusing discourse analysis around politically salient events. Conveniently, it also helps with presenting, in an ordered fashion, the historical context of the development of Dutch cyber security policy over time.

The first section treats the period between 1998 and 2006, which covers some of the early policies with regards to cyber security, even though it was not referred to as such in those days. Most debates centered on how to handle cyber crime—an almost entirely new phenomenon at the time. The cut-off point lies at the end of May 2006, with the simultaneous passing of the *Wet Computercriminaliteit II* (Law Computer crime II) and the ratification bill of the Convention on Cybercrime by the *Eerste Kamer* (First Chamber, Senate), some of the first major pieces of legislation with regards to cyber security. The second section covers the remainder of 2006 until September 2011. In this period, the then ruling coalitions shifted the tone of the debate from repression of cyber crime to prevention. In those years, debates about cyber terrorism also gain more prominence. The second section ends with the DigiNotar affair, a major cyber security event that changed the way the Dutch government handles information security. The third and final section looks at the aftermath of the DigiNotar affair, starting in October 2011, and runs roughly until the end of 2013, with the "fallout" of

the Snowden leaks about surveillance in cyberspace by government intelligence agencies. Crucially, in this period cyber security and worries about cyber warfare skyrocket to the top of the Dutch political agenda.

1998-2006: a new phenomenon on the rise

Characteristic for this early period is the sense of uncertainty and even bewilderment among politicians and policymakers. Many policy documents draw parallels with existing policies and/or earlier debates having to do with combating crime and maintaining the public order in society. ICT is always developing at a "tempestuous" or "stormy" speed, with the government always appearing to be one step behind. Although the main focus of this part will be on the passing of the Law Computer crime II, it was not the first legislation on cyber security in the Netherlands. As the name suggests, before its passage there came the first Law Computer crime. This first law was passed in 1993, and was primarily aimed at giving law enforcement agencies the legal authority to search and/or investigate automated systems, i.e. (personal) computers and computer networks. More important, it added the term "*computervredebreuk*" to the penal code, which was derived from the existing term "*huisvredebreuk*." The latter means so much as the "breaching of domestic peace," and makes punishable the unlawful trespassing in or breaking and entering of a dwelling (such as a house or any other type of privately owned dwelling). *Computervredebreuk* is then the breaching of "computer peace," which the penal code defines as "the purposeful and unlawful entry into an automated system or one of its parts."[15]

The first Law Computer crime rapidly became outdated due to "tempestuous" developments in information technology, to use the language of the explanatory

[15] Dutch Penal Code, article 138ab. *Computervredebreuk* is punishable up to one year in prison or a monetary fine of the fourth category (a maximum fine of €20,250 in 2014).

memorandum to the Law Computer crime II (*Kamerstuk* 26 671, nr. 3, 1999).[16] Interconnected computer networks among companies, universities, and so on already existed at the time, but it was not foreseen how incredibly fast the use of (personal) computers and especially the Internet would spread to people's homes in the years to come. In light of these developments politicians and policymakers agreed that a revision of the Law Computer crime was in order.

The first concrete proposals to update computer crime legislation were made in 1998, which is where this analysis starts. The memo "Legislation for the electronic highway" (*Kamerstuk* 25 880, nr. 1-2, 1998) of February 12, 1998 assessed the consequences of the "informationalization" of Dutch society for legislation and the government's role in it. It outlined several policy proposals for new legislation, which, it explicitly stated, would also serve as the future Dutch input for possible international negotiations on this topic. The most important idea introduced by the memo, however, can be found in the phrase

> As starting point, the cabinet chooses – given the current level of development of the electronic highway – that legal norms from the physical world should also be applicable to the electronic environment: what applies "off line" should also apply "on line." (*Kamerstuk* 25 880, nr. 1, 1998: 1)

This phrase contains a number of discursive practices that produce a particular kind of reality that will recur in many documents regarding cyber security in later years. First, similar to the term "cyberspace," these documents refer to the virtual realm as a "highway" or an "environment;" that is to say, they are predicated on spatial terms. To put it differently, the virtual is constituted as a subject with the quality of being spatial. Furthermore, it

[16] Official documents of the Dutch parliament are referred to as "*kamerstukken*," roughly translated as "chamber documents."

presupposes that Dutch law has jurisdiction in cyberspace. This makes sense if we accept that cyberspace is a space similar to the physical world: the relation between the physical and the electronic environment is one based on similarity rather than, as one may expect, opposition. Thus, the phrase "legal norms from the physical world should also be applicable to the electronic environment" constitutes a discursively produced norm in and of itself.

On July 8, 1999, then minister of Justice Korthals sent the proposal for the Law Computer crime II to the Second Chamber, which in part was based on the findings of the earlier memo. In the accompanying explanatory memorandum the government notes that "[t]he informationalization of society has not left the government's role unaffected" (*Kamerstuk* 26 671, nr. 3, 1999: 2). Moreover, it emphasizes that

> On the one hand the government's possibilities for control and guidance, especially at the national level, are becoming smaller, whereas on the other hand the government's responsibility for maintaining the orderly course of traffic among citizens gives rise to adapting that order to the changed circumstances, so that everyone's justified interests retain as much legal protection as possible. (ibid.)

Here we see an explicit use of the word "control," which fits with the "offline is online" norm. In this context, "control" does not refer to keeping citizens "*under* control" in a kind of coercive manner, but rather to maintaining the public order in cyberspace. This is underlined by the phrase "traffic among citizens," which in turn can be derived from the "electronic highway" analogy. On a physical highway, rules and norms are put in place so as to make sure that traffic goes in an orderly and safe fashion, and are enforced by law enforcement agencies. The same applies to the electronic highway: the government has to maintain the

orderly conduit of data traffic among citizens, which is to say that the government's main responsibility is maintaining the integrity of computer systems. It logically follows that within this responsibility also falls making sure that computer systems are available (i.e. access to computer systems and networks should be open to everyone and not interrupted by people or organizations with malicious intentions), and, as the explanatory memorandum proposes, giving electronic mail the same measure of legal protection as letters or phone calls (ibid.: 3). Recalling Clark's (2010) layered conceptualization of cyberspace, what the government thus appears to be "securing" is the physical and logical layers. All of these measures point to a *technical computer security* discourse, as coined by Nissenbaum (2005) in her study of conceptions of computer security in the US, which can be summed up with the words integrity, availability, and confidentiality.

What matters more is that this approach presupposes a conception of Dutch identity that is buttressed on open, liberal values. In this specific case, identity is constructed along spatial and ethical lines. There is a clear (abstract) spatial separation between the government and the Dutch citizenry: the government maintains the public order and ensures the safety of its citizens, but does not intrude into the domestic sphere. Moreover, in terms of ethicality, it is appropriate to the liberal discourse precisely that government stays out of people's homes. If we read between the lines, we might also even argue that identity, here, is constructed temporally. The government noted, for instance, that the "informationalization" of Dutch society had not left its role "unaffected," suggesting a break with the past. What it thus seems to be saying is that it does not want to stand in the way of progress, but that older conventions must be respected.

The sense of restraint on the part of the government comes back when the Netherlands was negotiating the Convention on Cybercrime, the first international treaty that attempted to combat computer crime. These negotiations pushed back the Law Computer crime II for

several years, but many of the proposed measures determined the Dutch stance towards the Convention (recall that this is in accordance with the 1998 memo). In the letter of December 23, 1999, Justice minister Korthals informed the Second Chamber about these negotiations. He explained that there was international consensus about behaviors that the signatory countries had to make punishable, which included "on the one hand behaviors aimed against the confidentiality, the integrity, and the availability of computer systems and the stored and transferred data in it." Here the intertextual links with earlier documents are abundantly clear, and subscribe to the technical computer security discourse. More problematic during the negotiations was, "on the other hand, content-related behavior. The fundamental right to freedom of expression plays a role" (*Kamerstuk* 23 530, nr. 40, 1999: 3). If we thus look at the letter from the perspective of the four layers of cyberspace, we also find a failed attempt to extend security to the information layer, in addition to the physical and logical layer that did receive security from the Convention (and previously in Dutch legislation). Although there was widespread agreement to combat child pornography in cyberspace, there was no consensus about other content. For instance, a number of European countries, including the Netherlands, have laws against incitement of racial or ethnic hatred. This met with opposition from some countries, most important the US, which argued that the freedom of expression took precedence.

We find another prominent example of identity politics in a document from October 16, 2000. In this letter, minister of the Interior and Kingdom Relations De Vries presents the cabinet position towards the final advice of the Committee "Constitutional rights in the digital age." This committee was tasked with researching and advising on how to make the Dutch constitution ready for the twenty-first century. Its most important conclusions was to make the phrasings of the constitution "technology-independent" and that Dutch constitutional rights offered more protection than international rights. The then ruling cabinet

largely took over the Committee's conclusions, as seen in the following passage which is worth quoting at length, and which displays some of the most visible subject positioning thus far:

> Notwithstanding increasing internationalization and Europeanization, the Netherlands remains a separate nation in which a great value is attached to our own norms and values. Precisely in the current multicultural society, in which there is no such thing as a shared history and background, are constitutional rights, guaranteed by a national constitution, of great importance. They constitute the formal *acquis* of our society. As the Committee notes, the level of constitutional rights in international arrangements can never be more than the largest common denominator of the different levels that the states concerned want to employ. Our national constitutional rights indicate the standard that our own society has reached in terms of, among others, culture and justice. (*Kamerstuk* 27 460, nr. 1, 2000: 7)

Although the advice never got a follow-up—the Dutch constitution did not change in response to the advice—it shows again a number of discursive practices that are embedded in earlier practices and that reproduce identity. Importantly, these discursive practices neatly fit in with Hansen's three dimensions of identity construction. In terms of subject positioning, the cabinet rates Dutch constitutional rights as superior to international ones, i.e. the cabinet positions itself ethically. Moreover, it underwrites both Walker's (1990) claim that identity is temporally constructed, even in cyberspace, and Campbell's (1992) claim that foreign policy *produces* borders. Logically, this also reveals that the identity is constructed spatially. Within the Dutch nation-state progress and cultural development is possible; outside of the border

there is only contingency. Had the constitution been changed according to the proposals in the cabinet's response, then articles concerning the integrity of the domestic sphere, the right to anonymity, and the right to confidential communication would have been rephrased to be independent of technology, i.e. also applicable to cyberspace. This coheres with the presupposition (and identity) that the government has a task to maintain an open, liberal society.

Almost a full year after minister of Justice Korthals sent his letter on the Convention on Cybercrime negotiations, the Permanent Chamber Committee (PCC) on Justice[17] filed a long list of questions regarding these negotiations to which it received answers on November 27, 2000. Most questions were concerned with the phrasing and interpretation of the Convention, repercussions for Dutch legislation (the Dutch constitution stipulates that international law trumps national law), and the government's efforts during the negotiations. Still, although critical, by and large they displayed widespread agreement and support for the government. It is actually a number of answers that are more interesting. To a question about why the final text of the Convention did not include a prohibition on incitement of racial hatred and pornography (in general), the government replied that "Regarding racism and pornography, the countries in question did not accept that such an international norm would implicitly suggest they were morally lacking" (*Kamerstuk* 23 530, nr. 45, 2000: 10). Nevertheless, the government noted that they would still enforce legislation against racial hatred at the national level. We see again that identity shapes policy, and we see it even more in response to a question that asks whether it is not "sensible" for the government to obligate computer users to follow certain security standards:

[17] Permanent Chamber Committees are composed of members of the Second Chamber from both coalition and opposition parties, and are *inter alia* tasked with reviewing legislation and/or current events with members of the government.

> It appears wrong that security standards should be prescribed by the government. Just as anyone needs to decide for himself which lock he puts on his back door and carries the risks of failing to do so, lawmakers should similarly restrain themselves in taking away the personal responsibility of companies and citizens to secure their data (for example company secrets). (ibid.: 12)

The technical computer security discourse based on liberal values renders this policy option impossible. Through the analogy of the back door, the government is saying that its role is to maintain the public order, but to stay out of the private sphere (cf. the earlier discussion on *huisvredebreuk* and *computervredebreuk*). If citizens or companies freely choose not to secure themselves, knowing full well the risks, then that is their responsibility. Even the right to make unwise decisions falls within the rights of an open society.

In terms of new, major computer security legislation, the years 2001 to 2004 were rather uneventful. The Convention on Cybercrime was signed on November 23, 2001 by thirty-eight countries, including the Netherlands, and went into force on July 1, 2004.[18] The Netherlands waited with ratification until 2006, which in part had to do with European directives on ICT that were issued around the same time period, more on this momentarily. As far as national policies were concerned, the government launched projects like the National High Tech Crime Centre (NHTCC) and the National Registration Point for Cyber Crime. These had the goal of improving online law enforcement, in line with the "offline is online" norm. For a more detailed overview, see predicate analyses [6], [9], and [10] in Appendix B.

[18] The Convention stipulated that it went into force three months after at least five ratifications, three of which had to be Council of Europe member states (Council of Europe, 2001).

More important, what did change was the more heavy emphasis on terrorism in security debates, obviously influenced by the terrorist attacks of September 11. It is in this context that cyber warfare first enters the lexicon of Dutch politicians. In a General Meeting on November 4, 2004, the PCC on Defense discussed the 2003 annual report of the MIVD (*Militaire Inlichtingen- en Veiligheidsdienst*, Military Intelligence and Security Agency). There, member of Second Chamber (MSC) Haverkamp of the centrist Christian Democratic party asked Defense minister Kamp how the MIVD could combat cyber warfare. Kamp noted that there were "indications that terrorists are using or preparing to use cyber warfare. Its goal is to disrupt information structures of countries like the Netherlands" (*Kamerstuk* 29 800 X, nr. 55, 2004: 4). He promised to inform the Second Chamber further at a later time, which he did with the next MIVD annual report of 2004. In it, the MIVD called cyber warfare "an underestimated phenomenon" and a potential threat against Dutch national security (MIVD, 2005: 19). Cyber warfare remained a low-key issue the following years, only to reappear in the 2008 MIVD annual report (and subsequent years) and the 2009 Defense budget. The next section will discuss this in more detail.

In 2005, the more substantial debate *vis-à-vis* computer security picked up speed again. In May, the PCC on Justice reported its preparatory research for the ratification bill of the Convention on Cybercrime. The PCC members generally showed agreement with the government's position and approval for the Convention, using similar rhetoric like "in principle, what is punishable in the 'normal' world should also be punishable in the virtual world" and that the international character of cyber crime "also requires an international approach" (*Kamerstuk* 30 036 (R 1784), nr. 6, 2005: 1). The biggest concern, however, was the Convention's inclusion of data preservation, a quick "freeze" of 90 days' worth of computer data (which may include metadata) if ordered to by a legal authority as part of a criminal investigation. Some PCC members believed this constituted a breach of the domestic

sphere. Indeed, such powers seem incompatible with the technical computer security discourse focusing on availability, confidentiality, and integrity of computer systems. In any event, since the text of the Convention had already been in force since 2004, the bill ratifying the Convention was adopted without a plenary session and without a formal vote in the Second Chamber on September 15 (*Handelingen* TK 107, 2004-05: 6417).[19]

Similar concerns *were* expressed in the Second Chamber plenary debate of September 13 on the revised Law Computer crime II, which was heavily adapted following the signing of the Convention, and also anticipated the implementation of European Directive 2006/24/EC, which obligated member states to store citizens' telecommunications data for at least six months. MSC Vos of the GreenLeft party—the only party that would vote against the Law Computer crime II—was especially critical: "My party finds this proposal pretty scary, because does this mean a blank check to search data files to one's heart's contents? . . . Supervising this appears very difficult to me, so the ministry of Justice might very well be doing that which is punishable as *computervredebreuk*" (*Handelingen* TK 105, 2004-05: 6355). Minister of Justice Donner dismissed her criticism, citing potential terrorist threats.

Throughout the debate, we see that technical computer security discourse has slightly shifted compared to the years before. Many MSCs still agree that citizens carry a personal responsibility to secure themselves, and that the government has a task to maintain the public order. Crucially, however, minister Donner veiled the "offline is online" in a shroud of ambiguity:

> We are gradually starting to realize that the fundamental fact of the Internet is that, with the Internet, we have canceled out the distinction between inside and

[19] Note about format: *Handelingen* are the transcripts and voting records of the Second and First Chamber, "TK" or "EK" indicates *Tweede Kamer* (Second Chamber) or *Eerste Kamer* (First Chamber) respectively, followed by the meeting number, parliamentary year, and page number.

> outside. Because of that, the private space and the public space are permeating into each other. (ibid.: 6357)

This is a discursive practice that is markedly different from earlier ones, and enables (and makes legitimate) new policy options. The "fact" that the Internet negates inside/outside boundaries is presented as indisputable. Additionally, it is used in the context of terrorism: potential terrorists roam between the private and public sphere in both the physical world and the virtual world. "There is a continuing discussion about the use of the Internet for terrorist attacks and in the area of radicalization," Donner remarks (ibid.). It is presupposed that this poses a threat to the open, Dutch, liberal society. Moreover, as the minister and, also, a number of MSCs are eager to point out on multiple occasions, law enforcement agencies are nearly always one step behind, due to the nature of cyberspace. In order to protect this redefined public order in cyberspace, data retention becomes appropriate and legitimate. Ultimately, this argument and arguments derived from it were enough to convince the Second Chamber (with the exception of, as mentioned, the GreenLeft party), which passed the Law Computer crime II with a vast majority on September 27, 2005 (*Handelingen* TK 4, 2005-06: 191).

Finally, the First Chamber simultaneously treated the ratification bill for the Convention on Cybercrime and the Law Computer crime II on May 30, 2006. The plenary debate shows many similarities with the debate in the Second Chamber, again emphasizing feelings of being unsafe. As one member of the First Chamber (MFC) put it, "Fortunately I never feel unsafe in the streets. There is only one street where I do regularly feel unsafe, and that is the electronic highway" (*Handelingen* EK 30, 2005-06: 1349). In the same vein, concerns were raised against the data retention clauses in both bills. Even though, or perhaps thanks to, the First Chamber does not have the power to amend bills, MFC Franken of the

Christian Democrats urged minister Donner—who, notably, was a member of the same party and very proficient in Latin—to not implement those clauses: "*ceterum censeo obligationem preservationis datorum informationis esse delendam*" (ibid.: 1348), which translates as "Furthermore, I am of the opinion that the obligation to preserve database information must be destroyed," a clear reference to the lamentation of Cato the Elder about the "necessary" destruction of Carthage. Here, the MFC makes an intertextual link with an historical phrase to add strength to his argument. We must reject these clauses in favor of our own liberal values. Still, the minister replied, in Latin, "*Ceterum censeo obligationes Unitatis Europeae esse implementanda* [sic]. *Pacta sunt servanda*!" (ibid.: 1352), meaning "Furthermore, I am of the opinion that the obligation of the European Union have to be implemented. Agreements must be kept!" This, in turn, fits with the part of Dutch identity that gives precedence to international law over national law. Despite the objections raised during the debate, the First Chamber passed both bills without a formal vote. Crucially, the adoption of both bills by the Second and First Chamber meant the extension of security to the information layer of cyberspace, which earlier appeared to have failed.

2006-2011: from repression to prevention

Around the passing of the Law Computer crime II, we are gradually seeing politicians and policymakers move away from the technical computer security discourse. Throughout the next years, we will observe discursive practices that are much different from the ones of previous period. Still, while it is reasonable to argue that politicians and policymakers alike consciously think about the language they use to emphasize the severity of their arguments, it is not very likely that they contemplate by themselves or sit down in a circle with others to discuss which *discourse* to employ. As noted in the previous chapter, politicians or

policymakers do not pick discourses from an “archive”—a database, if you will—when it is opportune for them to do so.

Instead, we may argue that their belief systems are expanding. To clarify this, it is helpful to return to Foucault’s concept of discursive formations. In the previous chapter, we used the bookshelf analogy to illustrate this concept: a group of books was placed on a shelf according to a particular subject following certain specified criteria, with the main texts at the core and the more “peripheral” texts toward the fringes. Continuing this analogy, what happens is that new books are added to the core, while even more are added to the margins. In terms of ICT/computer security discourse, the core mainly consisted of texts that emphasized the government’s role of maintaining the public order in cyberspace, and texts that stipulated the appropriate and proportionate policies that were derived from that responsibility. Now, new texts are being added to that core, usually underlining the government’s responsibility to secure Dutch society. This opens up a whole new range of policy options that may be added to the technical computer security discourse. The boundaries of the discourse are expanding, like an ink stain that is slowly expanding on a piece of paper. At a certain point, though, the technical computer security discourse is so qualitatively different from before that we can hardly still call it that way. It is hard to pinpoint exactly when the technical computer security discourse stopped being just that, but by the end of the period under study the cyber security discourse had become completely dominant. In short, as Foucault would put it, the rules of formation changed. Also recall that Foucault was not so much urging us to study the contents of discursive formations (which is not to say that it is irrelevant) as he was arguing that we should examine the grounds of their legitimacy. Why was it legitimate that the technical computer security discourse was expanded? How did authoritative persons or entities transgress the rules?

Late June 2006, a cabinet crisis erupted over news of identity fraud committed by MSC Ayaan Hirsi Ali of the Dutch liberal party at the time of her naturalization (1997), and the subsequent reaction to that news by the responsible minister (and fellow party member) Rita Verdonk. Ultimately, the second Balkenende cabinet fell when one of the coalition parties lost confidence and withdrew its support. This led to the creation of the third Balkenende cabinet, a rump cabinet whose main task was to prepare the early parliamentary elections in November later that year. Demissionary prime minister Balkenende and his Christian Democratic party again won the elections, resulting in the fourth Balkenende cabinet which was installed on February 22, 2007. It was primarily under the auspices of this cabinet that the technical computer security discourse decisively shifted to a cyber security discourse.

The change in the tone of the debate took place in the context of the fourth Balkenende cabinet's new security priorities. Under the fifth pillar (labeled "Security, stability and respect") of the coalition agreement, the cabinet outlined its vision with regards to security:

> Security is a basic condition for a happy life and a core task of the state. Security, certainty, and reliability are ever more important in an open society. At the same time they are still under pressure, among others by the threat of international terrorism.
>
> Guarantees for absolute security are not possible. One of the biggest challenges of the coming period is safeguarding a climate of security, legal certainty and legal protection that gives people confidence. This does not only

> concern combating crime and violence, but also prevention of those things. (*Balkenende-IV*, 2007: 10)

Although this passage does not treat cyber security directly, it is worth to briefly consider some of the discursive practices in it, and how they again constitute identity along spatial, temporal, and ethical dimensions. In this instance, they are easily recognizable: security is constituted as a subject that is necessary for a happy life, and as one the government's ultimate responsibilities. Importantly, it is described as constantly being threatened by external forces. This gives the government the prerogative to take far-reaching actions: absolute security may not be possible but they can sure try. The government is sending out a clear message that they are willing to go great lengths to protect Dutch identity and society (the Self) from (potential) dangerous Others.

As part of this pillar, the government launched the project "Security starts with Prevention," in which the intensification of fighting cyber crime took up an important place. This is a meaningful change, because it put cyber crime in the realm of collective, national security. In the letter of November 6, 2007, signed by several ministers and state secretaries, the government opens with: "Security, stability and respect characterize the society that this cabinet envisions" (*Kamerstuk* 26 684, nr. 119, 2007: 1). Apart from being an almost verbatim quote from the coalition agreement (intertextuality), it is also telling of the cabinet's order of priorities. What matters more is that they identify cyber crime as simultaneously a "less visible type of crime" (ibid.: 3) and a "severe type of crime" (ibid.: 16). Obviously, this is a dangerous mix. As the letter notes, "The by now almost unlimited possibilities of ICT, and especially the Internet, have a flipside," namely that it is a potent source of crime (ibid.: 19).

Similar and even stronger language is used in the letter of December 17 of that same year. In it, the Dutch government outlines the policy agenda *vis-à-vis* ICT security for the following years, basing their proposals on the Report "Recalibration ICT Security Policy." This report identified three possible arenas where action needed to be taken: "Preventing society-disrupting events," "Limiting non-disruptive events to society," and "Tracing and prosecuting cyber criminals." In particular the first arena calls for far-reaching measures, because "it concerns events that have to be prevented at almost any cost. There, the government takes up a guiding role" (*Kamerstuk* 26 643, nr. 103, 2007: 2). These measures are appropriate and legitimate, because "Looking toward the future, the cabinet is of the opinion that our society has to be resilient against threats: against physical but also digital threats, like ICT disruptions or cyber crime" (ibid.: 3). Again, the cabinet is opposing the Dutch Self with an unnamed but threatening Other. It also implies that they believe Dutch society was currently not resilient, or at least not resilient enough. Such a presupposition gives legitimate grounds for the government to step in.

Securitization scholars have shown time and again that national security is a powerful argument carrying a lot of moral force. It is perhaps not very surprising then that, in the wider (foreign) policy debate, there was a large consensus as to the necessity of these measures, with some critical notes about their consequences for, particularly, privacy in the domestic sphere. From left to right, politicians use the same language, portraying remarkable coherence with discourse used in earlier documents. Nevertheless, it was established that computer security discourse was in transition. We find evidence of this in the debate of May 19, 2008, that took place during the General Meeting of the PCCs on Justice and Interior and Kingdom Relations regarding the policy framework for law enforcement against cyber crime and Internet abuse. As MSC Gerkens of the Socialist Party contemplates,

> In 1996 I went online and arrived in a world that back then was veritably anarchist. . . . Although some parts of the Internet still belong to the individual, there are more and more areas that call for regulation. This hurts some people.

Yet due to widespread crime, "the virtual world may have become a matured place that asks for law and order" (*Kamerstuk* 28 684, nr. 149, 2008: 3). MSC Anker of the ChristianUnion party concurs: "The Internet should not be a refuge for criminal offenses. As Chamber, we are noticing a certain awareness about this" (ibid.: 11). The fact that members of both the coalition parties (Anker) and the opposition (Gerkens) use this language is arguably a discursive practice in itself. Not only is there an intertextual link between them, but they also provide each other legitimacy. These phrases still exhibit the technical computer security discourse: both members subscribe to the presupposition that crime is widespread in cyberspace and that actions must follow, i.e. the public order has to be maintained. Yet another member, MSC Teeven (who would later become state secretary of Security and Justice), appears to have already moved to the cyber security discourse:

> The VVD party [Dutch liberal party] judges that for some types of crime – we are not only thinking of terrorism and organized crime, but also child abuse – it is necessary to be able to regularly carry out hacks in order to investigate criminals or terrorist activities, without the persons in question to be informed upfront. (ibid.: 9)

On a side-note, there is a certain irony in Teeven's position. He claims to be a liberal, yet "counterhacking" without notification, even if applied to (potential) criminals, runs extremely

counter to liberal values respecting the individual's private sphere. In any event, MSC Joldersma (Christian Democratic party) provides another instance of cyber security discourse. In a motion urging the government to review its legal instruments against cyber attacks through *inter alia* internationally organized simulations, she puts forward:

> establishing that still very few government institutions and enterprises are prepared for a cyber attack and have no emergency plans at the ready in case critical company processes fail or no longer function well; . . .
>
> considering that a digital attack with a terrorist character is not imaginary and that the proposed law enforcement measures and legal instruments are still insufficiently thought through from the perspective of the virtual world of cyber crime . . .
>
> urges the government, through practical simulations, to test whether our systems and the proposed enforcement measures and updated legal instruments can avert the increasing threat of cyber attacks . . . (ibid.: 29)

Interestingly, both members categorize cyber terrorism as another type of cyber crime rather than a separate category as regularly done by security studies scholars. Still, using (cyber) terrorism invokes a wide variety of dangerous Others. We can only assume that the two MSCs adhere to the presupposition that a terrorist attack in or through cyberspace *will* happen eventually. It is perhaps even more noteworthy that, apparently, after more than ten years, the government is *still* behind with policies against possible evildoers. Law enforcement measures and legal instruments are still insufficient, much like they were in the documents

from the late 1990s. Again, this is another discursive practice by itself: politicians and policymakers keep claiming that the government is always one step behind in cyberspace, and it has been for a long time. If the national security argument was not already enough, constituting the government's position as such adds legitimacy to the argument that ever more far-reaching policy is necessary for controlling cyberspace.

These two arguments are crucial observations for answering the question why the cyber security discourse started to become dominant. In order to clarify this, we must first return to the conceptualization of cyberspace as consisting of four layers. We had already seen that security was extended to three of the four layers, namely the physical, logical, and information layers. What appears to be happening, in these years, is an attempt to further extend security to the fourth layer—the people layer—as well. If members of the Second Chamber assume that cyber terrorism *will* happen, then that must also mean that those members assume that "the people" are under direct threat of getting (physically) harmed. If that is the case, it makes sense that a change in discourse will occur to accommodate for these assumptions.

Second, we must keep in mind that discursive practices are situated within the context of particular discursive *formations* that make them possible to arise. The (transition to) cyber security discourse appeared to have been heavily influenced by traditional security discourse, especially in the wake of the September 11 terrorist attacks—we saw a similar trend in academic circles as evidenced by Chapters 2 and 3. To put it in more theoretical terms, there appeared to have been structural pressures coming from discourses in more "traditional" security circles on the way identity needed to be constructed in the computer security discourse. More specifically, Dutch identity along the spatial axis seemed to have been under pressure: it began to be necessary to protect identity from "dangerous Others" in cyberspace, e.g. cyber terrorists. Although cyber security is inherently transnational, cyber security *policy*

was prior to this point still primarily situated in the realm of domestic policy. With Dutch identity more clearly revolving around a Self/Other dichotomy, cyber security policy now *turns* "Otherness" into something *foreign*. That is to say, cyber security policy is now moving into the realm of foreign policy as well. Recall that Hansen (2006) argued that pressure on one of the dimensions of identity construction also puts pressure on the others. In this case, the temporal and ethical dimensions have to be readjusted to the changed spatial dimension, which indeed appears to happen in the following years.

With the computer security discourse moving from a technical computer security discourse to a cyber security discourse, the construction of (national) security interests will also change. To reiterate, discursive practices construct a particular kind of reality. Several representations are presented as unquestionable "truths," for instance the earlier mentioned claim that policy is always a step behind in cyberspace. Here, though, it has constructed a reality in which Dutch identity is under constant threat in cyberspace. Policy being behind may, incidentally, be represented as part of this constant threat. This legitimates an increased yet appropriate (within this particular discursive formation) amount of spending on cyber security. Indeed, traces of that transition can be observed in the explanatory memorandums to the annual budget proposals of the several ministries that are tasked with cyber security. Before 2008, cyber crime is hardly mentioned at all, usually relegated to one or two lines under police spending. The 2007 budget proposal of the ministry of Justice, for instance, notes that cyber crime is on its radar and that it will be a priority for the next couple of years (Ministerie van Justitie, 2006: 59-60). It should be noted that this budget proposal was still written under the second Balkenende cabinet. Yet with the new security priorities of third Balkenende cabinet, we increasingly find more expressions of the cyber security discourse in the later budget proposals. Spending on combating cyber crime increases, in line with the coalition agreement (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2007: 101).

The Defense ministry budget proposals deserve special attention, in that not a single budget before 2009 mentions the words “cyber” or “electronic.” The 2009 budget, for the first time, mentions that €25 to 50 million will be spent on a “Capability Upgrade Program Electronic Warfare,” spread out over the years 2011-2016 (Ministerie van Defensie, 2008: 70). In light of the transitioning discourse, some people might find the very limited attention to cyber security surprising and even worrisome. After all, if computer (network) security is now part of national security, then one may expect the armed forces stepping up to the plate.

It was precisely this discrepancy that one member of the Second Chamber addressed. In the plenary debate of December 3, 2009 regarding the 2010 Defense ministry budget, MSC Knops (Christian Democrat) dryly asserted with one line:

> And then the threat that the Netherlands is facing the coming years. The CDA party has seen in the responses of both members of government [minister and state secretary of Defense] that they are dealing with cyber threats. Regarding this, I am introducing a motion to further urge the cabinet to take up an additional number of issues. (*Handelingen* TK 33, 2009-10: 3186)

The threat he is referring to is cyber warfare, which he presents as a completely irrefutable fact. If we apply predicate analysis, we see that it is not *a* threat but *the* threat. In his view, the government is doing far too little to prepare for this inevitability, presupposing once again that the government is behind (cf. earlier discussion on cyber crime). The motion, the full text of which can be found in Appendix C, urges the government to create a cyber security strategy:

> considering that several NATO countries have created special divisions for digital warfare, like the United States, the United Kingdom, and Germany, in which they are also developing offensive capabilities; . . .
>
> considering that with cyber warfare, it is insufficient to only have defensive capabilities; . . .
>
> urges the government to develop interdepartmentally a cyber security strategy . . . (*Kamerstuk* 32 123 X, nr. 66, 2009)

After introducing the motion, Knops dropped the topic altogether, with cyber security not to be mentioned a single other time in the remainder of the debate. Nevertheless, the motion, which was adopted with a large majority, started a number of crucial developments that led to the dominance of the cyber security discourse. Indeed, it may rightly be referred to what Hansen (2006) called a "nodal text." Later policy documents would continually refer back to this motion or proceed from the language used in it, underlining its importance. If we consider the discursive practices in it, this is not that surprising. First, it invokes the authority argument by mentioning likeminded countries (in terms of identity) that are already developing a cyber security strategy; second, it uses the comparison with physical warfare, emphasizing that a country also needs offensive capabilities; and, lastly, it echoes the idea of being behind. In the same vein as the two MSCs mentioned earlier, the combined force of these arguments leads MSC Knops to question whether the Dutch Self can protect itself from the dangerous Others in cyberspace.

Following this motion, the transition from the technical computer security discourse to the cyber security discourse sped up dramatically. In a letter from March 2010, minister of

Defense Van Middelkoop provided the Second Chamber with a progress report on the cyber security strategy. In another first, the minister clearly distinguishes the three types of cyber threats that were discussed in Chapter 2: the ministry of Justice is responsible for "digital crime," the National Coordinator for Counterterrorism for "digital terrorism," and the ministry of Defense for "digital warfare." The minister concludes that these types of "activities" may cause "societal disruption" (*Kamerstuk* 26 643 and 32 123 X, nr. 149, 2010: 1). The obvious intertextual links with the documents treated earlier need little further explanation. Crucially, in the second progress report, specifically treating cyber defenses within the armed forces, Van Middelkoop writes that national and international cooperation are necessary, to make sure that "the Netherlands stays in possession of a reliable, secure, and accessible digital *domain*" (*Kamerstuk* 26 643, nr. 164, 2010: 1, emphasis added). Here, cyberspace is referred to as a domain, a new discursive practice that constitutes cyberspace as a space similar to e.g. air or water. This suggests that all laws, norms, regulation and so on also apply to cyberspace. To put it differently, the pressures of the international system of nation-states are now present in cyberspace.

Two letters from the (renamed) ministry of Security and Justice, both dated February 22, 2011, reinforce this picture.[20] In the letter outlining the security priorities of the newly installed Rutte cabinet, minister Opstelten notes that

> preventing society from disrupting, is viewed by the cabinet as one of its most important tasks . . . Digital systems (ICT) are fundamental to our society and economy, and are a catalyst for (further) sustainable economic growth. . . . The National Risk Assessment 2010 asserted that a large cyber conflict will lead to heavy societal disruption. (*Kamerstuk* 30 821, nr. 12, 2011: 1, 3)

[20] With the installation of first Rutte cabinet in October 2010, the ministry of Justice took over the public safety tasks from the ministry of the Interior and Kingdom Relations.

On the same day, the government presented the National Cyber Security Strategy (NCSS) to the Second Chamber. In the accompanying letter, Opstelten uses the almost exact same language: "ICT is of fundamental importance to our society and economy, and is a catalyst for (further) sustainable economic growth" (*Kamerstuk* 26 643, nr. 174, 2011: 1). If we turn the NCSS itself, we find still even more of the same language. Under the heading "Developments that demand action," the NCSS prominently places the subheadings "ICT is of fundamental importance to our society and economy" and "Society is vulnerable," with the latter citing, for instance, the Stuxnet cyber attack against Iran (Ministerie van Veiligheid en Justitie, 2011: 3). Many themes discussed earlier also return, for instance that bad intentions thrive in the anonymity of cyberspace, that the government is behind with legislation, and so on. In sum, the outright survival of the Dutch state and identity is now at the heart of discourse, which by that time can rightly be called a cyber security discourse in the sense that Nissenbaum (2005) had already described it.

The NCSS became even more salient in the subsequent months. On September 5, 2011, the government informed the Second Chamber of the digital "burglary" at DigiNotar. DigiNotar, a company that issued electronic certificates that ensure websites can be trusted and that digital communication is secured, was hacked (allegedly) by an individual from Iran. What made this event extra painful was the fact that many government websites used DigiNotar certificates, which potentially had put those sites at risk for quite some time. In their letter, the minister of the Interior and Kingdom Relations and the minister of Security and Justice almost apologetically conclude: "The Cabinet considers reliable digital communication of essential importance and will do everything to guarantee this. . . . For the Cabinet, threats against the confidence in and integrity of Internet traffic are unacceptable" (*Kamerstuk* 26 643, nr. 188, 2011: 7).

2011-present: securing the cybered nation

Following the event, the hack at DigiNotar was simply referred to as "DigiNotar," constituting a new discursive practice by itself. Underscoring Hansen's (2006) processes of linking and differentiation through language practices, the term "DigiNotar" almost exclusively became associated with the event. To be sure, the Dutch government considered DigiNotar a national crisis (*Kamerstuk* 26 643, nr. 188, 2011: 3; *Kamerstuk* 26 643, nr. 214, 2011: 1). Given that by then the cyber security discourse was completely dominant, this is not surprising. As the government notes,

> Digital information exchange has become an essential part for the functioning of Dutch society. This concerns both economic traffic as it does the functioning of the government. The burglary at DigiNotar has clearly revealed the vulnerability of reliable digital information services . . . (*Kamerstuk* 26 643, nr. 189, 2011: 1)

In short, DigiNotar had to be considered a direct threat against society, but also as a failure on the part of the Dutch government to protect it. We can thus clearly see how cyber security discourse now extended to all four layers of cyberspace. In the plenary debate on DigiNotar this sentiment was shared by members of the Second Chamber regardless of political convictions. MSC Gesthuizen (Socialist Party) exclaimed, "We are facing a serious disaster, a digital doom scenario" (*Handelingen* TK 12, 2011-12: 99). MSC Hachchi (D66, social liberals) pondered, "After all the recent ICT problems, I am doubting whether the government is 'in control'" (ibid.: 101). Using even stronger words, MSC Elissen of the Freedom Party (PVV) stated, "the PVV has argued for quite some time to approach data security in the same way as disaster planning" (ibid.: 106). Moreover, DigiNotar was

considered a “wake-up call” by at least three separate members (ibid.: 100, 102, 104). In response to the event, the ministers of Security and Justice, and Interior and Kingdom Relations announced several measures, the most important of which was the “security breach notification” (using the non-translated English terminology), which was already in the works prior to the event. The measure obligates companies to notify the government, specifically the National Cyber Security Center (NCSC, operational since January 1, 2012), in case of a digital security breach like the hack at DigiNotar.

At this point, two important remarks are necessary. First, with the heavy emphasis on discourse and discursive practices, one might get the impression that it suggests that discourse “caused” the DigiNotar event (or any other cyber event). This is certainly not the case. As a matter of fact, it should be recalled that poststructuralism rejects the notion of causality, at least in the positivist sense of the word. Rather, what discourse and discursive practices do is creating a particular reality that provides the background knowledge that enables agents to give meaning to a (material) subject or object. It also does this in response to “external” events like DigiNotar. The cyber security discourse highlights the government’s responsibility for the collective security of Dutch society in cyberspace. Its starting point is that the Dutch government must do everything within its power to deter or prevent altogether threats against the Dutch “corner” in cyberspace. From this point of view, DigiNotar was a double failure on the part of the government. DigiNotar was constructed as an outright attack on Dutch society. Not only could the government not prevent the event from occurring, it also failed its collective security task because of it. Consequently, the event legitimized new collective security measures, of course in line with the cyber security discourse.

Second, even though discourse does not directly cause a cyber event like DigiNotar, it does give rise to the reorganization of the identity-policy constellation with regards to cyber security. Chapter 3 theorized that the link between identity and policy should be characterized

as an equilibrium. Furthermore, it argued that, if this equilibrium went out of balance, the discourse that was more compatible with state sovereignty will be chosen. State sovereignty, as Walker (1990, 1993) noted, ontologically requires security in order to protect national identity in an otherwise threatening international system composed of many different other identities. In the first section, we observed that cyberspace was primarily considered as an "electronic highway" in which the Dutch government had to maintain public order. Threats came from (small-time) criminals against which the government has to act, like it does in the physical world. As time went on, though, Dutch society became more and more digitalized, an undeniable material reality which poststructuralism would not deny. The point is, however, that the threats against cyberspace were increasingly conceived as threats against Dutch society, and thereby identity, as a whole. First came cyber crime, then came cyber terrorism, and finally cyber warfare. Cyber criminals are an undesirable side-effect of the open nature of cyberspace, but not a threat against Dutch identity *per se*. Cyber terrorists, on the other hand, are an entirely different case. They are described as purposely desiring to undermine the Dutch way of life, i.e. a direct threat against Dutch identity. What makes it even more threatening is the idea that terrorists may strike indiscriminately, anonymously, and at any time in and through cyberspace. There are simply too many "unknowns," making them a particularly dangerous Other. To use Weimann's quote again, the fear of terrorism "segues well" with cyberspace (2005: 131). Cyber warfare, lastly, suffers from many of the same unknowns, but has the "advantage" that "we" as a society can more easily conceptualize cyber warriors. These warriors directly serve an enemy nation. The link with conventional warfare is thus easily made, and we all "know" that warfare threatens our identity. All in all, the technical computer security discourse, with its emphasis on public order and individual responsibilities, was insufficient, and gradually moved to the cyber security discourse, which is far more compatible with the idea of state sovereignty given its

emphasis on collective security. The shift to cyber security discourse has created a discursive space in which far-reaching security measures have become possible, and, more important, legitimate.

The last development, which is the focus of the remainder of this section, evidences the previous idea. Since 2011, the cyber security debate has gradually been militarizing. In January 2012, the *Adviesraad Internationale Vraagstukken* (AIV, Advisory Council on International Affairs) presented the report "Digital Warfare," in which it concluded, among others, that the laws of war also apply to cyberspace. In its mandatory response,[21] the government largely agreed with their findings:

> The findings of the committee with regards to the use of force and the right to self-defense largely match the cabinet's point of view (*jus ad bellum*). The commission's assertion that with regards to digital attacks no other regime should apply than the one that applies to the use of force in the physical domain, the cabinet believes to be important. (Attachment to *Kamerstuk* 33 000 X, nr. 79, 2012: 5)

A more concrete policy agenda executing this point of view followed on June 27, 2012, when minister of Defense Hillen presented the Defense Cyber Strategy (DCS). In the accompanying letter, Hillen writes that "The digital domain, next to land, air, sea, and space, is by now the fifth domain for military actions. . . . The Dutch armed forces draw necessary conclusions from this, and wants to play the prominent role fitting to our country in the digital domain" (*Kamerstuk* 33 321, nr. 1, 2012: 1). Similar language is used in the DCS itself, in which it notes that the Defense ministry's three main tasks that apply to the physical

[21] The AIV is a government-run but otherwise independent think tank. The government is obligated by law to respond to every report (both wanted and unwanted) it releases, see *Kaderwet Adviescolleges* [Framework Law Advisory Committees], article 24.

world also apply to cyberspace. These are, respectively, "protecting of our own and alliance territory, including the Caribbean parts of the Kingdom; promoting international rule of law and stability; [and] supporting civil authorities with law enforcement, disaster planning, and humanitarian aid, both nationally and internationally" (Ministerie van Defensie, 2012: 4). Defense minister Hillen's successor, Hennis-Plasschaert, notified the Second Chamber in August 2013 about the creation of the *Defensie Cyber Commando* (DCC, Defense Cyber Command), to be operational by the end of 2015 (*Kamerstuk* 33 321, nr. 2, 2013: 3). The use of this kind of language, terminology, and names is no coincidence: it is borrowed almost verbatim from US policy documents and in particular from former Undersecretary of Defense Lynn's article in *Foreign Affairs* (Lynn, 2010). In this article, which also rightly may be called a "nodal text," Lynn explained that the US Department of Defense considers "cyberspace as fifth domain" to be official military doctrine. One may logically conclude that the Dutch armed forces now view cyberspace the same way. In the same vein, the name "*Defensie Cyber Commando*" is a clear nod to its American counterpart, US Cyber Command. Again, in terms of discursive practices, using such language presupposes many of the assumptions that can be found in the cyber security discourse that have been discussed at length throughout this chapter. What is more relevant, though, is that these particular discursive practices also employ an intertextual link with US texts on the topic. The US is an important, powerful and likeminded ally of the Netherlands: through intertextuality, the Dutch policy documents also (attempt to) invoke the authority and moral force of the US in the area of cyber security.

Finally, two events bring the argument in favor of identity politics in cyber security policy home, both taking place in the early summer of 2013. First, on June 21, the minister of Foreign Affairs, Timmermans, released the Dutch government's International Security Strategy (IVS, *Internationale Veiligheidsstrategie*). Although cyber threats were already

mentioned in the explanatory memorandum to the 2012 Foreign Affairs budget (Ministerie van Buitenlandse Zaken, 2011: 15), and the 2013 budget even gave a prominent place to "cyber diplomacy" (Ministerie van Buitenlandse Zaken, 2012: 10), the IVS officially made cyber security part of Dutch foreign policy. In the letter to the Second Chamber, Timmermans asserts,

> Modern threats are not very concerned about borders or dikes. Internal and external security are becoming less and less separable from each other. What happens in the world around us directly touches on our own security and prosperity. With its open economy and international orientation, the Netherlands is of course very dependent on foreign countries. (*Kamerstuk* 33 694, nr. 1, 2013: 2)

On cyber security, the IVS notes,

> But there is a flipside [to digitalization]. What if all screens turn black? Our society would be disrupted with one swift strike. The digital infrastructure is becoming more vulnerable. . . . The Netherlands is also pushing for the further ratification and globalization of the Convention on Cybercrime (Treaty of Budapest). (ibid.: 7, 19)

Thus, the securing of Dutch society starts outside of its borders. If the world is secure, then the Netherlands is secure. This also applies to cyberspace, which is now considered part of the world, even if digital. Indeed, security has now definitively extended to all four layers of cyberspace. As Campbell (1992) had already concluded, foreign policy is boundary-

producing. It turns “Otherness” into something foreign, thereby simultaneously revealing that which is domestic, i.e. part of the Self. By incorporating cyber security into foreign policy, the Netherlands—and obviously many other countries in the world as well—is putting up fences around “its corner” in cyberspace.

The second event that abundantly exposed identity politics in cyber security policy is the revelations about global mass surveillance, and the fallout of those disclosures. Early June 2013, whistleblower and former National Security Agency (NSA) employee Edward Snowden leaked thousands of documents to several international newspapers, revealing mass surveillance of and spying on non-American citizens in and through cyberspace by American intelligence agencies. This led to a scandal of huge proportions, severely straining relations between the US and its allies for a short amount of time.

Of course, the outrage in the Netherlands was just as big. Initially, the government remained cautious in passing judgment regarding the case:

> The cabinet is following the reaction of the United States to Mr. Snowden’s disclosures with interest. As noted previously, the cabinet greatly values careful and thorough protection of personal data. Therefore, it is necessary when national security and protection of privacy meet, to be as transparent as possible about procedures, powers, safeguards, and oversight measures. The cabinet deems it encouraging that, in this context, American members of Congress are debating about precisely those topics and make proposals to change legislation . . . (*Kamerstuk* 30 977, nr. 61, 2013: 2)

During the General Meeting of the PCC on the Interior and Kingdom Relations with the responsible minister, Plasterk, on October 16, we observe a different tone. What is surprising,

though, is that the outrage is not so much aimed at the fact that the US is conducting mass surveillance itself, but rather at the possibility that Dutch citizens may have been targeted by US intelligence agencies. We have to remember that cyber security discourse is now fully dominant. It was exactly this discourse (and the transition to that discourse) that created the discursive space that made such policies possible. In that respect, the words of MSC Vos (GreenLeft party) back in 2005 were prophetic: intelligence agencies were given a blank check to search data files with quite limited (public) oversight (see section 1). But, as said, we are in the time of cyber security discourse. National security may also necessitate mass surveillance by Dutch intelligence agencies in order to protect Dutch society and identity from external threats.

What really mattered during the General Meeting was that the US was spying on its friends. To most present members of the Second Chamber, it was perfectly acceptable, and understandable, to conduct mass surveillance in the fight against international terrorism. Moreover, they largely agreed that there simply had to be a balance between privacy and security. But, as MSC Van Raak (Socialist Party) remarked in a demand to the minister, "for once, publicly state that allies do not treat each other this way, that in this way we cannot win the international fight against terrorism, and that we cannot accept this" (*Kamerstuk* 30 977, nr. 71, 2013: 3). MSC Dijkhoff (VVD, Dutch liberal party) then contemplated which other countries would spy in the Netherlands. "With the Russians and the Chinese we pretty much can assume that they are doing it. If that were to come to the surface, we would not be very surprised." But, he adds, "Obviously it is extra painful if an ally turns out to be doing it, if a country that you cooperate with does it. One would expect restraint" (ibid.: 14). Even minister Plasterk chimed in at the end of the meeting,

> The problem is that, now, we have established that American law treats non-Americans completely different than [Dutch law] would do [with regards to surveillance and/or spying]. It is one thing for us if they aim that at a region in the world where there is great political instability, a region that can truly be deemed hostile. If, however, we work together as allies in the fight against terrorism, then we do not appreciate it if we end up in the same category. (ibid.: 19)

Identity politics in all of these statements is easily discernible. MSC Dijkhoff taps into the presupposition that, since Russia and China do not have a very reputable track record concerning surveillance, they must be spying on the Netherlands as well. It also implies that he believes Russia and China are no real friends of the Netherlands, otherwise they would not be spying on us. What he is saying is, then, is that the US thus should not be spying on the Netherlands. After all, we are not the "dangerous Other" to the US. At the core of Plasterk's message is that "we" as a Dutch society do not want to be in the same positions as "the terrorists." Like Dijkhoff, Plasterk is saying that the US should not be conducting mass surveillance in the Netherlands because clearly we are not the dangerous Other. If anything, what this debate made clear is that identity politics in foreign policy is a two-way street. The Netherlands may be creating borders in cyberspace to keep out the dangerous Other, but foreign countries are simultaneously creating borders to contain *their* respective dangerous Others. Obviously, this does not only apply to Western countries, but also to non-Western countries. These countries have their own, yet different, identity-policy constructions—or at least, *we assume they do*, as implied by the Western/non-Western dichotomy (see e.g. the remarks by MSC Dijkhoff above). Slowly but surely, the reorganization of the Westphalian system in cyberspace appears to be becoming a self-fulfilling prophecy.

Summary

This chapter presented the empirical analysis of policy documents that are part of the wider Dutch cyber security debate. Using predicate analysis, it showed how language created a discursive space that gave rise to both the technical computer security discourse and the cyber security discourse, and the transition between them.

In the early period from 1998 to 2006, we observed that the cyber security debate (which was not referred to as such in that time) was primarily dominated by a technical computer security discourse. This discourse tended to characterize cyberspace as a "digital highway" or a "virtual environment" in which the government's task was to maintain public order. Most cyber security policies had the goal of fighting cyber crime, also placing many responsibilities with Dutch citizens. This was in line with idea of Dutch identity as being open and liberal.

Second, we witnessed a transition period from roughly late 2006 to September 2011. Dutch society was increasingly becoming digitalized, bringing with it potential new threats. Concomitantly, politicians and policymakers were slowly beginning to speak in terms of national, collective security. This was also prompted by the installation of the fourth Balkenende cabinet in 2007, whose priority was the prevention of cyber crime. In addition, the cabinet and several other members of the Second Chamber put cyber terrorism in the same category as cyber crime. In 2009, the motion by MSC Knops et al. then spurred the creation of the National Cyber Security Strategy. The strategy would become extremely relevant following the hack at DigiNotar, a crucial event that indelibly changed the cyber security debate in the Netherlands.

Finally, the third section dealing the period from September 2011 roughly to the present paid attention the militarization of cyber security discourse and the politics of identity in Dutch (and foreign) cyber security policy. The section also considered some questions

about causality. Recalling that poststructuralism rejects that notion, it argued that discourse did not so much “cause” cyber events like DigiNotar or the Snowden leaks as it asserted that discourse gives meaning to such events. What discursive practices do, then, is producing the discursive space in which certain responses and solutions become possible. Dutch identity was endangered in the borderless world of cyberspace: even there it has to be protected by a government. As a result, it was concluded that with cyber security discourse being completely dominant, the international system of nation-states appears to be replicated in cyberspace.

CHAPTER 6

CONCLUSION: CYBER SECURITY IS WHAT WE MAKE OF IT

Cyber security discourse has gone down a path from which it is unlikely to return, and continues to give meaning to cyber security events. In August 2013, the German news magazine *Der Spiegel* published an article, based on Edward Snowden's leaks, revealing that the NSA had (allegedly) collected 1.8 million sets of metadata on Dutch telecommunications traffic in one month. The responsible minister, Plasterk of the Interior and Kingdom Relations, then appeared on a news program on Dutch national television the following October, where he was interviewed about the case. During the interview, Plasterk infamously took out a piece of paper from his inside pocket which, he claimed, contained confirmation by the NSA itself that it was indeed conducting surveillance on Dutch citizens. He emphasized that the Dutch intelligence agency AIVD (*Algemene Inlichtingen- en Veiligheidsdienst*, General Intelligence and Security Service) was thus not responsible for collecting the data, and certainly would not share such information with the NSA (Nieuwsuur, 2013).

As it turned out, Plasterk could not have been more wrong, something which the AIVD and even his colleague, Defense minister Hennis-Plasschaert (responsible for the AIVD's military counterpart MIVD), had allegedly warned him against prior to the interview (Klompenhouwer, 2014). Contrary to his claims, the AIVD was really quite responsible for collecting data on Dutch citizens, and also *did* share that information with the NSA. In short, Plasterk had misinformed the Second Chamber, a deadly sin in Dutch politics. During the

plenary debate of February 11, 2014, in which he had to explain his actions to the Chamber, Plasterk barely survived a motion of no confidence. Most notably, however, the debate hardly gave any substantive attention to the news that the AIVD was massively collecting data. Although many MSCs were critical, they still agreed that the collecting of metadata "fits within legal frameworks and serve a legitimate purpose," as one member put it (*Handelingen* TK 52, 2013-14: 4). The outrage was primarily aimed at Plasterk's actions. After surviving the motion of no confidence, he promised to be more careful with public appearances, especially when it came to sensitive information that concerned intelligence agencies.

Dutch cyber security in the future: what is next?

The introduction of several new cyber security policies has already been set in motion. A piece of legislation which was not discussed in the previous chapter is the Law Computer crime III, the successor to the previous two computer crime laws. The first law proposal was presented by minister of Security and Justice Opstelten in May 2013, and is currently in the advisory phase. Like its predecessor, it will again expand the responsibilities and powers of law enforcement agencies. One of the measures that the law intends to introduce is the so-called "counterhacking," a wish already expressed in 2008 by the current state secretary of Security and Justice Teeven when he was still a member of the Second Chamber (see Chapter 5, section 2). Counterhacking gives law enforcement agencies possibilities to hack computers and computer systems of potential suspects to search for information, and even to plant spyware that can keep computers under close watch, such as "keyloggers" (software that registers every keystroke a user makes) (Ministerie van Veiligheid en Justitie, 2013: 15-16). Naturally, this led to much criticism from privacy watchdogs. Note that the proposal was presented before the Snowden leaks; it therefore remains to be seen whether the final law will look the same.

Still, the proposed Law Computer crime III fits in with the dominant cyber security discourse. The government is on the offense, so as to defend the Netherlands in cyberspace. Similar expansions of offensive capabilities can be found elsewhere. The Defense Cyber Strategy discussed in the previous chapter already explicitly mentioned creating offensive capabilities. Later, in May 2014, minister of Defense Hennis-Plasschaert repeated her earlier announcement that the Defense ministry would speed up the operationalization of the Defense Cyber Command (*Kamerstuk* 33 321, nr. 3, 2014: 3). Moreover, despite the uproar caused by Edward Snowden, the Dessens Committee, tasked with investigating the functioning of Dutch intelligence agencies, concluded that the AIVD's and MIVD's possibilities to indiscriminately collect data and conduct surveillance should be expanded. In the current situation, the intelligence agencies are only allowed to intercept wireless communication; the Committee recommended that this power should be expanded to wired communication as well, of course under strict oversight from the government (Rijksoverheid, 2013). Again, all of these proposals logically follow from the collective security task that is embedded in the cyber security discourse.

Reflections and recommendations

This thesis has traced the genealogy of cyber security in the Netherlands. It revealed the discursive practices that are at the foundations of the early technical computer security discourse, the current cyber security discourse, and the transition from one to the other. The role of the government changed along with it: it went from maintaining the public order in cyberspace to preserving the collective security of the "cybered" Dutch nation-state. Around 2009, politicians and policymakers began using language that implicitly and at times explicitly identified (potential) dangerous Others. These dangerous Others are conceived as a direct threat to Dutch identity, and must be contained. Paradoxically, the open nature of

cyberspace has thus led to the creation of boundaries in cyberspace, and it is unlikely that this trend will be halted (or reversed). What is surprising as well is the observation that while Dutch identity emphasizes liberal, individualized values, the solutions to (cyber) security threats are collectivized.

Next, this thesis has made a contribution to IR debates on cyber security and on the role of identity in foreign policy. With regards to the latter, it has shown that "choices" between discourse tend to fall out in favor of discourses that are compatible with the idea of identity that is embodied in state sovereignty. Once cyberspace was conceived of as a "domain" similar to physical domains, the rules of the game of the international system of nation-states also applied as a result. Since a state's survival is always on the line, to put it in realist terms, governments best insure themselves against threats. In the Dutch case, Dutch identity also came to be constituted in collective terms, fitting with the changed conception of cyberspace. As seen, a new discourse gradually followed, a discourse that reinforced the adapted Dutch identity. This identity had to be protected against the dangerous Others. Yet in order to maintain the equilibrium between identity and policy, new policy necessarily had to be introduced so as to balance things out. Far-reaching measures were introduced, measures that could only have become possible under a cyber security discourse rather than a technical computer security discourse.

Furthermore, although this thesis did not employ securitization theory, there are some overlaps with poststructuralism, particularly about threat perceptions. "Securitizers" have to convince a relevant audience that a certain (perceived) threat is a threat against the survival of the state. One possible angle that scholars of securitization theory may investigate in the future, though, is the question *who* this relevant audience should be. In the documents studied in this thesis, there tends to be a dialog between the government on one side and politicians and policymakers on the other side. That is to say, they only speak to each other. What is the

role of the "general" public, in this case Dutch citizens, in this process? Here, there appears to be a considerable gap between politics and citizenry. It is reasonable to argue that the Dutch citizenry wants the government to give them some measures of safety (such as maintaining the public order in cyberspace), but at no point did the government (in policy documents) really consider whether Dutch citizens even want far-reaching policies with regards to cyber security. Do Dutch citizens really want the government to do everything in its power to mitigate risks, if that means giving up important aspects of the right to personal privacy? The public outrage among Dutch citizens in response to the Snowden leaks suggests no. One thus gets the feeling that the government has very little faith in the capacity of its citizens to secure themselves in cyberspace. Cyber security policies, not only Dutch ones, have qualitatively the open yet anonymous nature of cyberspace. Surveillance and other measures of control are becoming more prevalent by the day.

Lastly, some concerns might be raised against this study. First, given the large role that agency has played in this thesis, one may legitimately ask the question if structure has no place in it. Unsatisfyingly, we may argue both yes and no. A poststructuralist analysis would certainly not deny that structural pressures exert influence on actors. In the second section of the previous chapter we saw, for instance, that the National Cyber Security Strategy was partially instigated by the fact that other countries already had one (see also Appendix C). Here, a realist scholar like Waltz would immediately point to the forces of competition and socialization. Yet what matters is that a poststructuralist would approach such structural pressures from a different angle. Yes, structural pressures are there, but only because actors interpret them as *being* there. As has been noted on many occasions, poststructuralism believes that there is no such thing as an extra-discursive reality. Additionally, we should not forget the productive power that is inherent to discourse, an aspect that may be read between the lines but perhaps had deserved more explicit attention in this thesis. In the end, it is

discourse that produces structures which include a range of legitimate and appropriate behaviors and policy responses, but excludes others. These structures then influence actors in return, because, as was the case with intertextuality, such exchanges are a two-way street. In the example above, structural pressures enable and constrain policy actions, because those are only appropriate within the cyber security discourse. What is more, Dutch politicians attached great value to the fact that it was countries like the US, the UK, and Germany that had already created a NCSS. These are likeminded countries with largely similar Western identities, putting them in a position of authority. Dutch policy gains legitimacy by referring to those countries—and *vice versa*—but is always viewed through the productive power of cyber security discourse.

Second, can a discourse analysis like the one applied in this thesis reveal some "hidden meaning" or the "true intentions" of policymakers or other actors? The answer simply is no, but a poststructuralist would also argue that it is not a relevant question. Asking a question like that implies that this study is (and should be) looking for an ultimate "truth," a stance that is congruent with a positivist approach to science. And this is exactly what poststructuralism argues against: there are no absolute truths in the positivist sense, only socially constructed truths. In addition, the point of discourse analysis is *inter alia* to reveal power relations embedded in discourse. Politicians and policymakers have to legitimize policy, which they do through language. Even if they have ulterior motives, they still need to use discourse that is acceptable enough to a (relevant) audience to push through policies.

Lastly, can we draw large, sweeping conclusions from only one case? Moreover, does the choice for the Netherlands not also come with an inherent Western liberal bias? Like above, this depends on the stance one takes with regards to scientific research. Arguing that large generalizations should be drawn from this study again seems to imply a positivist idea: the idea to isolate particular "independent variables" that always determine a certain

outcome. But as before, this is not something that poststructuralism is trying to do, given that it rejects causality in the first place. What we *can* say, based on this study, is that identity and discourse on state sovereignty are intricately linked. Here, possibilities for future research may be found. Identity is something every country and individual has. Therefore, it is also not really an issue that this study focused on the Western, Dutch identity. Identity will always lead to the production of policies, whereby these policies simultaneously reproduce that identity. Note here that there is no "one way" of causality: they are mutually constitutive. Obviously, the same applies to non-Western countries. Future studies may research how identity and cyber security policy are interlinked in countries like Russia and China. It is likely that the same processes found in this study will be found there as well, with the likely difference that those countries have different conceptions of "dangerous Others." A final possibility for future research lies in international regimes. This study necessarily only looked at Dutch policy. However, how do different identities clash in the setting of international organizations? Such studies may provide important insights into processes of intertextuality between different countries, and why certain discourses become dominant within international organizations rather than others.

REFERENCES

Abbate, J. (1999). *Inventing the Internet*. Cambridge, MA: MIT Press.

Arquilla, J. (2009, July 26). Click, Click... Counting Down to Cyber 9/11. *San Francisco Chronicle*. Retrieved 6 August 2013, from http://www.sfgate.com/opinion/article/Click-click-hellip-counting-down-to-Cyber-9-11-3291819.php

Arquilla, J. (2012). Cyberwar Is Already upon Us. *Foreign Policy*. Retrieved 9 May 2013, from http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us

Arquilla, J., and Ronfeldt, D. (1993). Cyberwar Is Coming! *Comparative Strategy 12*(2), 141-165.

Arquilla, J., and Ronfeldt, D. (1997). A New Epoch—And Spectrum—of Conflict. In J. Arquilla and D. Ronfeldt (Eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (pp. 1-20). Santa Monica, CA: RAND.

Arquilla, J., and Ronfeldt, D. (Eds.). (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND.

Ashley, R.K. (1987). The Geopolitics of Geopolitical Space: Toward a Critical Social Theory of International Politics. *Alternatives 12*(4), 403-434.

Ashley, R.K. (1989). Living on Border Lines: Man, Poststructuralism, and War. In J. Der Derian and M.J. Shapiro (Eds.), *International/Intertextual Relations: Postmodern Readings of World Politics* (pp. 259-321). New York, NY: Lexington Books.

Barnard-Wills, D., and Ashenden, D. (2012). Securing Virtual Space: Cyber War, Cyber Terror, and Risk. *Space and Culture 15*(2), 110-123.

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

Berkowitz, B.D. (1997). Warfare in the Information Age. In J. Arquilla and D. Ronfeldt (Eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (pp. 175-189). Santa Monica, CA: RAND.

Berners-Lee, T. (1989). *Information Management: A Proposal*. Geneva: CERN. Retrieved 1 August 2013, from http://cds.cern.ch/record/1405411/files/ARCH-WWW-4-010.pdf

Berners-Lee, T., and Cailliau, R. (1990). *WorldWideWeb: Proposal for a HyperText Project*. Geneva: CERN. Retrieved 1 August 2013, from http://www.w3.org/Proposal.html

Bhalla, N. (2003). Is the Mouse Click Mighty Enough to Bring Society to Its Knees? *Computers & Security 22*(4), 322-336.

Butler, J. (2006). *Gender Trouble: Feminism and the Subversion of Identity*. London: Routledge Classics. (Original work published 1990)

Buzan, B., Wæver, O., and de Wilde, J. (1998). *Security: A New Framework for Analysis*. Boulder, CO: Lynne Riener.

Campbell, D. (1992). *Writing Security: United States Foreign Policy and the Politics of Identity*. Minneapolis, MN: University of Minnesota Press.

Campbell, D. (2010). Poststructuralism. In T. Dunne, M. Kurki and S. Smith (Eds.), *International Relations Theories: Discipline and Diversity* (2nd ed., pp. 213-237). Oxford: Oxford University Press.

Carr, J. (2012). *Inside Cyber Warfare: Mapping the Cyber Underworld* (2nd ed.). Sebastopol, CA: O'Reilly.

Choucri, N. (2012). *Cyberpolitics in International Relations*. Cambridge, MA: MIT Press.

Clark, D.D. (2010). Characterizing Cyberspace: Past, Present, and Future. MIT Working Paper Series, Version 1.2, March 12.

Clarke, R.A., and Knake, R.K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. New York, NY: HarperCollins.

Council of Europe. (2001). Convention on Cybercrime. Retrieved 23 June 2014, from http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

Cox, R. (1981). Social Forces, States and World Orders: Beyond International Relations Theory. *Millennium: Journal of International Studies 10*(2), 126-155.

Davis, N.C. (1997). An Information-Based Revolution in Military Affairs. In J. Arquilla and D. Ronfeldt (Eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (pp. 79-98). Santa Monica, CA: RAND.

De Lange, R. (2014, April 14). Opmars Cybersecurity. *Het Financieele Dagblad*. Retrieved 21 May 2014, from http://fd.nl/fd-outlook/259339-1404/opmars-cybersecurity/

De Lange, R., and Jonker, S. (2014, March 22). Cyberdienst Navo naar Den Haag. *Het Financieele Dagblad*. Retrieved 26 May 2014, from http://fd.nl/economie-politiek/620578-1403/cyberdienst-navo-naar-den-haag/

Deibert, R.J. (2013). *Black Code: Inside the Battle for Cyberspace*. Toronto, ON: Signal/McClelland & Stewart.

Denning, D.E. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet As a Tool for Influencing Foreign Policy. In J. Arquilla and D. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 239-288). Santa Monica, CA: RAND.

Doty, R.L. (1993). Foreign Policy as Social Construction: A Post-Positivist Analysis of U.S. Counterinsurgency Policy in the Philippines. *International Studies Quarterly 37*(3), 297-320.

Doty, R.L. (1996). *Imperial Encounters: The Politics of Representation in North-South Relations*. Minneapolis, MN: University of Minnesota Press.

Dunn Cavelty, M. (2007). Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology & Politics 4*(1), 19-36.

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

Dunn Cavelty, M. (2012a). Cyber-Security. In A. Collins (Ed.), *Contemporary Security Studies* (pp. 362-378). New York: Oxford University Press.

Dunn Cavelty, M. (2012b). The Militarisation of Cyber Security As a Source of Global Tension. In D. Möckli (Ed.), *Strategic Trends 2012 – Key Developments in Global Affairs* (pp. 103-124). Zürich: ETH Center for Security Studies.

Dunn Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact on the Cyber-Security Discourse. *International Studies Review 15*(1), 105-122.

Eriksson, J. (2001). Cyberplagues, IT, and Security: Threat Politics in the Information Age. *Journal of Contingencies and Crisis Management 9*(4), 211-222.

Eriksson, J., and Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International Political Science Review 27*(3), 221-244.

Eriksson, J., and Giacomello, G. (Eds.). (2007). *International Relations and Security in the Digital Age*. London: Routledge.

Flichy, P. (2007). *The Internet Imaginaire* (L. Carey-Libbrecht, Trans.). Cambridge, MA: MIT Press.

Forsyth, J.W., Jr. (2013). What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace. *Strategic Studies Quarterly 7*(1), 93-113.

Foucault, M. (1977). Nietzsche, Genealogy, History. In D.F. Bouchard (Ed.), *Language, Counter-Memory, Practice: Selected Essays and Interviews* (pp. 139-164). Oxford: Basil Blackwell.

Foucault, M. (1991). *Discipline and Punish: The Birth of the Prison* (A.M. Sheridan Smith, Trans.). London: Penguin Books. (Original work published 1977)

Foucault, M. (2002). *The Archaeology of Knowledge* (A.M. Sheridan Smith, Trans.). London: Routledge Classics. (Original work published 1969)

Fritsch, S. (2011). Technology and Global Affairs. *International Studies Perspectives 12*(1), 27-45.

Gibson, W. (1984). *Neuromancer*. New York: Berkeley Publishing Group.

Hansen, L. (2006). *Security as Practice: Discourse Analysis and the Bosnian War*. London: Routledge.

Hansen, L. (2012). Discourse Analysis, Post-Structuralism, and Foreign Policy. In S. Smith, A. Hadfield and T. Dunne (Eds.), *Foreign Policy: Theories, Actors, Cases* (2nd ed., pp. 94-109). Oxford: Oxford University Press.

Hansen, L., and Nissenbaum, H. (2009). Digital Disaster, Cyber Security and the Copenhagen School. *International Studies Quarterly 53*(4), 1155-1175.

Helms, R., Costanza, S.E., and Johnson, N. (2012). Crouching Tiger or Phantom Dragon? Examining Discourse on Global Cyber Terror. *Security Journal 25*(1), 57-75.

Junio, T.J. (2013). How Probable Is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate. *Journal of Strategic Studies*, 1-9.

Keohane, R.O., and Nye, J.S., Jr. (1998). Power and Interdependence in the Information Age. *Foreign Affairs 77*(5), 81-94.

Kiss, J. (2014, March 12). An Online Magna Carta: Berners-Lee Calls for Bill of Rights for Web. *The Guardian*. Retrieved 20 March 2014, from

http://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web

Klimburg, A. (2011). Mobilising Cyber Power. *Survival: Global Politics and Strategy 53*(1), 41-60.

Klompenhouwer, L. (2014, February 6). "AIVD en Hennis Waarschuwden Plasterk" – Debat is Dinsdag, Hennis Uitgenodigd. *NRC Handelsblad*. Retrieved 29 June 2014, from http://www.nrc.nl/nieuws/2014/02/06/aivd-waarschuwde-plasterk-over-onvolledige-informatie/

Kramer, F.D., Starr, S.H., and Wentz, L.K. (Eds.). (2009). *Cyberpower and National Security*. Washington, DC: National Defense University Press.

Kristeva, J. (1980). *Desire in Language: A Semiotic Approach to Literature and Art* (T. Gora, A. Jardine and L.S. Roudiez, Trans.). Oxford: Basil Blackwell.

Laclau, E., and Mouffe, C. (1985). *Hegemony & Socialist Strategy: Towards a Radical Democratic Politics*. London: Verso.

Landler, M., and Markoff, J. (2007, May 29). Digital Fears Emerge after Data Siege in Estonia. *New York Times*. Retrieved 9 May 2013, from http://www.nytimes.com/2007/05/29/technology/29estonia.html

Langner, R. (2011). Cracking Stuxnet, a 21st-Century Cyber Weapon. *TED Talk*. Retrieved 9 May 2013, from http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html

Lawson, S. (2013). Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *Journal of Information Technology & Politics 10*(1), 86-103.

Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., et al. (2009). A Brief History of the Internet. *Computer Communication Review 39*(5), 22-31.

Lewis, J.A. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington, DC: Center for Strategic and International Studies. Retrieved 6 August 2013, from http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

Libicki, M.C. (2009). *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND.

Liff, A.P. (2012). Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies 35*(3), 401-428.

Lizza, R. (2011, May 2). The Consequentialist: How the Arab Spring Remade Obama's Foreign Policy. *The New Yorker*. Retrieved 23 April 2014, from http://www.newyorker.com/reporting/2011/05/02/110502fa_fact_lizza

Lynn, W.J., III. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs 89*(5), 97-108.

Maass, P., and Rajagopalan, M. (2012, August 1). Does Cybercrime Really Cost $1 Trillion? *Wired*. Retrieved 5 August 2013, from http://www.wired.com/threatlevel/2012/08/cybercrime-trillion/

Manjikian, M.M. (2010). From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly 54*(2), 381-401.

Markoff, J. (2008, August 12). Before the Gunfires, Cyberattacks. *New York Times*. Retrieved from http://www.nytimes.com/2008/08/13/technology/13cyber.html

McGraw, G. (2013). Cyber War is Inevitable (Unless We Build Security In). *Journal of Strategic Studies*, 1-11.

Milliken, J. (1999). The Study of Discourse in International Relations: A Critique of Research and Methods. *European Journal of International Relations 5*(2), 225-254.

National Research Council. (1991). *Computers at Risk: Safe Computing in the Information Age*. Washington, DC: National Academy Press.

National Research Council. (1994). *Realizing the Information Future: The Internet and Beyond*. Washington, DC: National Academy Press.

National Security Council. (2010). The Comprehensive National Cybersecurity Initiative. Retrieved 30 June 2014, from http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

Newmyer, J. (2010). The Revolution in Military Affairs with Chinese Characteristics. *Journal of Strategic Studies 33*(4), 483-504.

Nicolescu, B. (2002). *Manifesto of Transdisciplinarity* (K.-C. Voss, Trans.). Albany, NY: SUNY Press.

Nieuwsuur. (2013, October 30). Plasterk over de NSA en Afluisteren. Retrieved 29 June 2014, from http://nieuwsuur.nl/video/569130-plasterk-over-de-nsa-en-afluisteren.html

Nissenbaum, H. (2005). Where Computer Security Meets National Security. *Ethics and Information Technology 7*(2), 61-73.

Nye, J.S., Jr. (2004a). The Information Revolution and American Soft Power. In J.S. Nye, Jr. (Ed.), *Power in the Global Information Age: From Realism to Globalization* (pp. 81-96). London: Routledge.

Nye, J.S., Jr. (2011). *The Future of Power*. New York, NY: PublicAffairs.

Nye, J.S., Jr. (Ed.). (2004b). *Power in the Global Information Age: From Realism to Globalization*. London: Routledge.

Nye, J.S., Jr., and Owens, W.A. (1996). America's Information Edge. *Foreign Affairs 75*(2), 20-36.

Radford, G.P. (2003). Trapped in Our Own Discursive Formations: Toward an Archeology of Library and Information Science. *The Library Quarterly 73*(1), 1-18.

Rattray, G.J. (2001). *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press.

Reardon, R., and Choucri, N. (2012). *The Role of Cyberspace in International Relations: A View of the Literature*. Paper presented at the 2012 ISA Annual Convention, San Diego, CA.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies 35*(1), 5-32.

Rid, T. (2013). Cyberwar and Peace: Hacking Can Reduce Real-World Violence. *Foreign Affairs 92*(6), 77-87.

Rijksoverheid. (2013). Commissie-Dessens: Wet op de Inlichtingen- en Veiligheidsdiensten Moet Worden Aangepast. Retrieved 29 June 2014, from http://www.rijksoverheid.nl/nieuws/2013/12/02/commissie-dessens-wet-op-de-inlichtingen-en-veiligheidsdiensten-moet-worden-aangepast.html/

Rothkopf, D.J. (1998). Cyberpolitik: The Changing Nature of Power in the Information Age. *Journal of International Affairs 51*(2), 325-359.

Sanger, D.E. (2012, June 1). Obama Ordered Sped Up Wave of Cyberattacks against Iran. *New York Times*. Retrieved 2 July 2013, from http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Sanger, D.E. (2013, July 10). Differences on Cybertheft Complicate China Talks. *New York Times*. Retrieved 5 August 2013, from http://www.nytimes.com/2013/07/11/world/asia/differences-on-cybertheft-complicate-china-talks.html

Schimmelfennig, F. (2001). The Community Trap: Liberal Norms, Rhetorical Action, and the Eastern Enlargement of the European Union. *International Organization 55*(1), 47-80.

Schmid, A.P., and Jongman, A.J. (1988). *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature* (2nd ed.). New Brunswick, NJ: Transaction Books.

Shapiro, M.J. (1989). Textualizing Global Politics. In J. Der Derian and M.J. Shapiro (Eds.), *International/Intertextual Relations: Postmodern Readings in World Politics* (pp. 11-22). New York, NY: Lexington Books.

Singel, R. (2008, January 23). War Breaks Out Between Hackers and Scientology — There Can Be Only One. *Wired*. Retrieved 5 August 2013, from http://www.wired.com/threatlevel/2008/01/anonymous-attac/

Stohl, M. (2006). Cyber Terrorism: A Clear and Present Danger, The Sum of All Fears, Breaking Point or Patriot Games? *Crime, Law and Social Change 46*(4-5), 223-238.

US Strategic Command. (2011). U.S. Cyber Command. Retrieved 9 May 2013, from http://www.stratcom.mil/factsheets/Cyber_Command/

Walker, R.B.J. (1990). Security, Sovereignty, and the Challenge of World Politics. *Alternatives 15*(1), 3-27.

Walker, R.B.J. (1993). *Inside/Outside: International Relations as Political Theory*. Cambridge: Cambridge University Press.

Waltz, K.N. (1979). *Theory of International Politics*. Reading, MA: Addison-Wesley.

Weimann, G. (2005). Cyberterrorism: The Sum of All Fears? *Studies in Conflict & Terrorism 28*(2), 129-149.

Weinberg, L., Pedahzur, A., and Hirsch-Hoefler, S. (2004). The Challenges of Conceptualizing Terrorism. *Terrorism and Political Violence 16*(4), 777-794.

Wendt, A. (1999). *Social Theory of International Politics*. Cambridge: Cambridge University Press.

Wiener, N. (1948). *Cybernetics: Or Control and Communication in the Animal and the Machine*. Cambridge, MA: MIT Press.

APPENDIX A

List of consulted parliamentary documents

Handelingen [EK (First Chamber)/TK (Second Chamber)] [meeting number], [parliamentary year], [page number(s)]. ([Year]). [Description]. [Exact date].

Kamerstuk [dossier number(s)], [order number]. ([Year]). [Description]. [Exact date].

Handelingen EK 30, 2005-06, 1346-1353. (2006). Plenary debate re. Law Computer crime II and bill ratifying Convention on Cybercrime. 30 May 2006.

Handelingen TK 105, 2004-05, 6348-6367. (2005). Plenary debate re. Law Computer crime II. 13 September 2005.

Handelingen TK 107, 2004-05, 6417. (2005). Voting record re. bill ratifying Convention on Cybercrime. 15 September 2005.

Handelingen TK 4, 2005-06, 191. (2005). Voting record re. Law Computer crime II. 27 September 2005.

Handelingen TK 33, 2009-10, 3155-3197. (2009). Plenary debate re. 2010 ministry of Defense budget. 3 December 2009.

Handelingen TK 12, 2011-12, 99-127. (2011). Plenary debate re. hack at DigiNotar. 13 October 2011.

Handelingen TK 52, 2013-14, 1-64. (2014). Plenary debate re. the misinforming of the Second Chamber by minister of the Interior and Kingdom Relations Plasterk about collection of metadata. 11 February 2014.

Kamerstuk 23 530, nr. 40. (1999). Letter of the minister of Justice re. negotiations on Convention on Cybercrime. 23 December 1999.

Kamerstuk 23 530, nr. 45. (2000). List of questions and answers re. Convention on Cybercrime. 27 November 2000.

Kamerstuk 25 880, nr. 1-2. (1998). Letter of the minister of Justice re. memo "Legislation for the electronic highway." 12 February 1998.

Kamerstuk 26 643, nr. 103. (2007). Letter of the minister of Justice and others re. policy agenda "Recalibration ICT Security Policy." 17 December 2007.

Kamerstuk 26 643 and 32 123 X, nr. 149. (2010) Letter of the minister of Defense re. progress building up of digital defenses. 11 March 2010.

Kamerstuk 26 643, nr. 164. (2010). Letter of the minister of Defense re. progress of setting up digital defenses within ministry of Defense. 12 July 2010.

Kamerstuk 26 643, nr. 174. (2010). Letter of the minister of Security and Justice presenting National Cyber Security Strategy. 22 February 2011.

Kamerstuk 26 643, nr. 188. (2011). Letter of ministers of the Interior and Kingdom Relations, and Security and Justice re. hack at DigiNotar. 5 September 2011.

Kamerstuk 26 643, nr. 189. (2011). Letter of ministers of the Interior and Kingdom Relations, and Security and Justice re. measures taken in response to hack at DigiNotar. 16 September 2011.

Kamerstuk 26 643, nr. 214. (2011). Letter of the minister of the Interior and Kingdom Relations replying to motions adopted during plenary debate on DigiNotar. 9 November 2011.

Kamerstuk 26 671, nr. 3. (1999). Explanatory memorandum to the proposed Law Computer crime II. 8 July 1999.

Kamerstuk 26 671, nr. 22. (2005). Report of a General Meeting of the PCCs on the Interior and Kingdom Relations, Economic Affairs, and Justice re. the National High Tech Crime Centre (NHTCC). 20 December 2005.

Kamerstuk 26 671, nr. 24. (2006). Letter of the state secretary of Economic Affairs re. final advice on Project NHTCC. 18 May 2006.

Kamerstuk 27 460, nr. 1. (2000). Letter of the minister of the Interior and Kingdom Relations re. cabinet position on the advisory report by the Committee "Constitutional rights in the digital age." 16 October 2000.

Kamerstuk 27 834, nr. 3. (2001). Letter of the minister of Justice re. law enforcement in the electronic environment. 15 August 2001.

Kamerstuk 28 684, nr. 119. (2007). Letter of the ministers of Justice, Interior and Kingdom Relations, and others re. security program "Security starts with Prevention." 6 November 2007.

Kamerstuk 28 684, nr. 149. (2008). Stenographic report of a General Meeting of the PCCs on Justice and Interior and Kingdom Relations re. law enforcement *vis-à-vis* cyber crime and internet abuse. 19 May 2008.

Kamerstuk 29 800 X, nr. 55. (2004). Report of a General Meeting of the PCC on Defense re. letters of the minister of Justice on the MIVD 2003 annual report. 4 November 2004.

Kamerstuk 30 036 (R 1784), nr. 6. (2005). Report by the PCC on Justice re. preparatory research for the ratification bill of the Convention on Cybercrime. 31 May 2005.

Kamerstuk 30 821, nr. 12. (2011). Letter of the minister of Security and Justice re. National Risk Assessment 2010 and new priorities of first Rutte cabinet. 22 February 2011.

Kamerstuk 30 977, nr. 61. (2013). Letter of the minister of the Interior and Kingdom Relations offering cabinet reaction to Snowden leaks. 13 September 2013.

Kamerstuk 30 977, nr. 71. (2013). Report of a General Meeting of the PCC on the Interior and Kingdom Affairs re. cabinet reaction to Snowden leaks. 14 November 2013.

Kamerstuk 32 123 X, nr. 66. (2009). Motion by MSC Knops et al. urging the government to develop a cyber security strategy. 3 December 2009.

Kamerstuk 33 000 X, nr. 79, attachment. (2012). Cabinet reaction to AIV advice "Digital Warfare." 6 April 2012.

Kamerstuk 33 321, nr. 1. (2012). Letter of the minister of Defense presenting Defense Cyber Strategy. 27 June 2012.

Kamerstuk 33 321, nr. 2. (2012). Letter of the minister of Defense re. progress made with Defense Cyber Strategy. 26 August 2013.

Kamerstuk 33 321, nr. 3. (2014). Letter of the minister of Defense re. development of offensive cyber capabilities. 17 March 2014.

Kamerstuk 33 694, nr. 1. (2013). Letter of the minister of Foreign Affairs presenting the International Security Strategy. 21 June 2013.

List of consulted explanatory memorandums to annual ministerial budget proposals

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties [Ministry of the Interior and Kingdom Relations]. (2007). *Kamerstuk* 31 200 VII, nr. 2. Explanatory memorandum to 2008 budget. 18 September 2007.

Ministerie van Buitenlandse Zaken [Ministry of Foreign Affairs]. (2011). *Kamerstuk* 33 000 V, nr. 2. Explanatory memorandum to 2012 budget. 20 September 2011.

Ministerie van Buitenlandse Zaken. (2012). *Kamerstuk* 33 400 V, nr. 2. Explanatory memorandum to 2013 budget. 18 September 2012.

Ministerie van Defensie [Ministry of Defense]. (2008). *Kamerstuk* 31 700 X, nr. 2. 16 September 2008. Explanatory memorandum to 2009 budget.

Ministerie van Justitie [Ministry of Justice]. (2006). *Kamerstuk* 30 800 VI, nr. 2. 19 September 2006. Explanatory memorandum to 2007 budget.

List of other consulted reports/strategies

Balkenende-IV. (2007). Coalitieakkoord tussen de Tweede Kamerfracties van CDA, PvdA en ChristenUnie. 7 February 2007. Retrieved 23 June 2014, from http://www.rijksbegroting.nl/rijksbegrotingsarchief/regeerakkoorden/regeerakkoord_2007.pdf

Ministerie van Defensie. (2012). Defensie Cyber Strategie. Retrieved 9 May 2013, from http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/brochures/2012/06/27/brochure-defensie-cyber-strategie/brochure-defensie-cyber-strategie.pdf

Ministerie van Veiligheid en Justitie [Ministry of Security and Justice]. (2011). De Nationale Cyber Security Strategie (NCSS): Slagkracht door Samenwerking. Retrieved 9 May 2013, from http://www.nctv.nl/Images/cyber-security-strategie_tcm126-444043.pdf

Ministerie van Veiligheid en Justitie. (2013). Explanatory memorandum to first proposal Law Computer crime III. Retrieved 29 June 2014, from http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/05/02/memorie-van-toelichting-wetsvoorstel-versterking-aanpak-computercriminaliteit.html

MIVD. (2005). Annual Report 2004. Retrieved 23 June 2014, from http://www.rijksoverheid.nl/documenten-en-publicaties/jaarverslagen/2005/03/01/mivd-2004.html

APPENDIX B

Table B.1 Predicate analyses of parliamentary documents, 1998-2013.

Document	Predicate(s)	Presupposition(s)	Subject-position(s)
[1] *Kamerstuk* 25 880, nr. 1: Letter of the minister of Justice re. memo "Legislation for the electronic highway," 12 February 1998	"De nota komt tot de conclusie dat de overgang naar de informatiesamenleving vergaande veranderingen brengt, maar niet leidt tot een radicale breuk met het verleden." "Het kabinet kiest als uitgangspunt dat – bij het huidige niveau van ontwikkeling van de elektronische snelweg – de juridische normen uit de fysieke wereld tevens toepasbaar moeten zijn in de elektronische omgeving: wat 'off line' geldt moet ook 'on line' gelden." "De open, techniekonafhankelijke formulering van belangrijke delen van het Nederlandse recht, maakt dit recht geschikt voor toepassing in de elektronische omgeving." "De nota constateert 1 fundamenteel probleem voor de wetgever dat niet goed oplosbaar is: het internationale karakter van de elektronische snelweg verhoudt zich niet goed met territoriaal georganiseerde overheden."	Dutch society is changing into an information society. This is not a break with the past. On the contrary, it is continuity. The physical and electronic are similar. Therefore, same norms apply. Dutch law is formulated in an open, technology independent fashion. Therefore, legal scope can and should be widely applied. Problems with jurisdiction in cyberspace, no boundaries like in the physical world.	*Identity*: Dutch society is open, liberal. These norms must be preserved in electronic environment. *Oppositional*: physical vs. virtual, national vs. international *Similarity*: online and offline
[2] *Kamerstuk* 26 671, nr. 3: Explanatory memorandum re. Law Computer crime II, 8 July 1999	"In de afgelopen jaren heeft de informatietechnologie zich op stormachtige wijze verder ontwikkeld." "De informatisering van de maatschappij laat de	The government has a legitimate claim to control and guidance within national boundaries. Society is "informationalizing." This affects the government's	*Oppositional*: government vs. citizens, nation-state vs. international community, order vs. disorder

	rol van de overheid niet onberoerd. Enerzijds worden de mogelijkheden van de overheid tot controle en sturing, zeker in nationaal verband, kleiner" "anderzijds brengt de verantwoordelijkheid van de overheid voor een ordelijk verloop van het verkeer tussen burgers" "elektronische snelweg"	possibilities for control and guidance. It has a responsibility to ensure that traffic between citizens goes in an orderly fashion. Information in and through cyberspace is *like* an electronic highway.	*Similarity*: traffic in cyberspace comparable with traffic in the real world
[3] *Kamerstuk* 23 530, nr. 40: Letter of the minister of Justice re. negotiations on Convention on Cybercrime, 23 December 1999	"Daar computernetwerken zich niet aan landsgrenzen storen, is het mogelijk dat daarbij buitenlandse computers op hun inhoud worden onderzocht." "Het materiële strafrecht omschrijft een aantal gedragingen dat de landen in hun nationale wetgeving strafbaar dienen te stellen. Enerzijds gaat het om gedragingen die zich richten tegen de vertrouwelijkheid, de integriteit, en de beschikbaarheid van computersystemen en de daarin opgeslagen en overgedragen gegevens. . . . Anderzijds betreft het inhoudgerelateerde gedragingen. Het fundamentele recht op vrijheid van meningsuiting speelt daarbij een rol." "consensus"/ "compromis" (4x)	The government has the authority to search computer networks. Computer networks are transnational. Dutch jurisdiction ends at the national border. Countries have a responsibility to preserve the confidentiality, integrity, and access to computer systems and their respective data. Countries have a responsibility to deter or mitigate certain content-related behavior. Countries (ought to) have legitimate means to enforce criminal law within national boundaries.	*Oppositional*: national vs. trans/international, acceptable behavior vs. deviant behavior *Complementarity*: information and information systems, criminal law and criminal procedures *Identity*: Dutch government in four cases intends to follow consensus, avoiding conflict
[4] *Kamerstuk* 27 460, nr. 1: Letter of the minister of the Interior and Kingdom Relations re. cabinet position on the advisory report by the Committee "Constitutional	"Voor overheid, burger en bedrijfsleven biedt de informatiemaatschappij veel nieuwe kansen." "elektronische snelweg" "deze voorstellen techniekonafhankelijk van opzet	We live in an information society. There are opportunities inherent to information society. Everyone has constitutional rights. These apply equally to all, independent of technology.	*Oppositional*: offline vs. online, international vs. national, multicultural vs. monocultural, LCD vs. high standards *Identity*: the Netherlands is

rights in the digital age," 16 October 2000	zijn" "Het voorgaande is in de lijn van het uitgangspunt dat 'on-line' en 'off-line' in beginsel dezelfde normen moeten gelden." "Los hiervan kan geconstateerd worden dat de toegang tot informatie en informatiekanalen steeds belangrijker wordt. Dit betreft een terrein dat vooral beheerst wordt door particuliere bedrijven die hier een zekere macht kunnen uitoefenen die te vergelijken is met overheidsmacht." "Niettegenstaande de toenemende internationalisering en europeanisering, blijft Nederland een aparte natie vormen, waarin aan eigen normen en waarden een grote waarde wordt gehecht. Juist in de huidige multiculturele samenleving waarin van een gezamenlijke achtergrond en geschiedenis geen sprake is, zijn in een nationale grondwet gewaarborgde grondrechten van groot belang." "het niveau van grondrechtenbescherming in internationale regelingen zijn niet meer dan de grootste gemene deler" "Onze nationale grondrechten geven het peil aan dat onze eigen samenleving heeft bereikt in termen van onder meer cultuur en rechtvaardigheid."	There exists an "offline" and an "online" world. Norms are valid in both. Information and ICT is controlled by private companies. Their power is comparable to governmental power. The world and the Netherlands is internationalizing and Europeanizing. But Netherlands remains a separate nation. There is an international system of nation-states. A multicultural society does not have a shared background and history, as opposed to a monocultural society. Therefore, we need constitutional rights. It is desirable to preserve these. Internationally, always the lowest common denominator. National norms are superior.	multicultural, lacks a shared history/background. Dutch norms and values are superior to international norms. *Similarity*: offline technology is in principle similar comparable to online technology, thus constitutional rights apply. Digital environment is a medium like the printing press, speech, etc. *Complementarity*: information and information systems
[5] *Kamerstuk* 23 530, nr. 45: List of questions and answers re. Convention on Cybercrime, 27 November 2000	"Ik meen dat gegevens die zijn opgeslagen op een gegevensdrager die fysiek zich bevindt op het territoir van een land, onder de rechtsmacht van dat land vallen en buiten de rechtsmacht van enig	Each country has a legitimate claim over certain territory. Judiciaries have no power outside their own borders. Cyberspace contains a physical	*Oppositional*: inside vs. outside, international vs. national norms, governments vs. citizens, collective vs. individual security.

	ander land." "In Nederland en een aantal andere Europese landen is het aanzetten tot rassenhaat strafbaar. Dat blijft. . . . Ten aanzien van racisme en pornografie aanvaarden de betrokken landen niet dat zij door een dergelijke internationale norm impliciet moreel in gebreke worden gesteld." "Het lijkt onjuist dat van overheidswege de standaarden voor beveiliging worden voorgeschreven. Zoals ieder zelf moet weten welk slot hij op zijn achterdeur wil zetten en zelf het risico draagt wanneer hij daarin nalatig is, zo moet ook de wetgever terughoudend zijn de eigen verantwoordelijkheid van bedrijven en burgers voor de beveiliging van hun gegevens (bijvoorbeeld bedrijfsgeheimen) af te nemen."	component. Incitement to racial hatred is an exception to freedom of expression (in the Netherlands). Other countries disagree. The government should not prescribe security standards for ICT. This is an individual responsibility, because we live in a liberal society.	*Identity*: the Netherlands believes incitement to racial hatred is wrong. The Netherlands is a liberal country: citizens have individual responsibilities. *Complementarity*: physical and digital components of information (systems) *Similarity*: securing computers is like securing one's home.
[6] *Kamerstuk* 27 834, nr. 3: Letter of the minister of Justice re. law enforcement in the electronic environment, 15 August 2001	"wordt geconcludeerd dat de kwaliteit van de opsporing krachtig versterking behoeft in het licht van de ontwikkelingen op het gebied van de informatie- en communicatietechniek." "dat de rechtsbescherming van de burger in een 'on line' situatie gelijkwaardig dient te zijn aan een 'off line' situatie" "Criminaliteitsbeheersing begint bij preventie" "biedt de elektronische omgeving gelegenheids-structuren om criminaliteit te plegen" "heeft de gebruiker onvoldoende kennis over de veiligheidsrisico's die in de elektronische	It is possible to investigate crime in the electronic environment. Citizens enjoy same legal protection online as they do offline. Online law enforcement is currently behind. It is the government's task to protect society from crime. Controlling crime starts with prevention. Users of the electronic environment currently lack sufficient knowledge about the risks, and measures they can take. The government has the task to inform/educate citizens	*Oppositional*: government vs. citizens, prevention vs. reaction, collective vs. individual *Complementarity*: risks in the electronic environment and measures to take *Similarity*: offline and online legal protection should be equal

	omgeving spelen en over de maatregelen die genomen kunnen worden om die risico's te beheersen" "dient er in de elektronische omgeving een geloofwaardige strafrechtelijke handhaving te zijn" "er wordt momenteel . . . hard gewerkt om het handhavingstekort in de elektronische omgeving weg te nemen"	about this. There exists a law enforcement deficit in the electronic environment. This is undesirable. Needs to believable: in order to deter or punish crime. Because protecting society.	
[7] *Kamerstuk* 30 036 (R 1784), nr. 6: Report by the Permanent Chamber Committee (PCC) on Justice re. preparatory research for the ratification bill Convention on Cybercrime, 31 May 2005	"ook een internationale aanpak vergt" "in principe moet in de virtuele wereld strafbaar zijn wat ook in de 'normale' wereld strafbaar is" "Ziet de regering eveneens dat deze methode meer proportioneel is voor wat betreft de inbreuk op de persoonlijke levenssfeer dan de vergaarplicht?"	Cybercrime is a transnational problem. This requires an international approach. Criminal proceedings are bound by territory. Computer networks are also part of the domestic sphere.	*Oppositional*: national vs. international, criminals vs. law-abiding citizens, domestic vs. public sphere *Complentarity*: national and transnational *Similarity*: online and offline
[8] *Handelingen* Second Chamber, 105-6348 to 6367: Plenary debate re. Computer crime II bill, 13 September 2005	MSC Gerkens, SP: "Het zou naïef zijn om te denken dat criminelen niet digitaliseren en de rest van de wereld wel." "Als gevolg daarvan lopen wij dan ook achter de feiten aan." "Aan de ene kant promoten wij breedband en on line zijn van jong tot oud, maar aan andere kant geven wij ruim baan aan de criminele randver-schijnselen van dit instrument." "Ik vind dat dit kabinet veel te weinig verantwoordelijkheid neemt voor het informeren	Criminals are inventive and will use new ways to commit crime. ICT develops at an incredibly rapid pace. Yet Dutch policy is lagging behind, which is undesirable. Dutch politicians and the government agree that every Dutch citizen should go and have equal access to being online. Criminals can and will exploit weaknesses of internet/digital environment. Like offline, such activities	*Oppositional*: naiveté vs. rationality, government vs. citizens, public vs. private space (on the internet) *Similarity*: digitalization of society comparable to the introduction of the printing press (technological determinism), crime in cyberspace is "old" crime in a "new outfit" *Identity*: everyone should have access to internet, fits with an

	van gewone gebruikers van internet over de gevaren die er zijn.” “Wij staan nu al op achterstand” MSC Van der Staaij, SGP: “wat off line geldt, moet ook on line gelden” “‘Een stap ter hemel en een stap ter hel’ werd gezegd na de uitvinding van de boekdrukkunst.” “Ik beklemtoon dat ICT niet alleen een probleem is, maar ook kan helpen bij de oplossing. Bijvoorbeeld bij de bestrijding van terrorisme” MSC Van Fessem, CDA: “Wij vinden ook internet niet meer of minder dan een communicatiemiddel.” “De ontwikkelingen gaan immers razendsnel.” MSC Weekers, VVD: “Het probleem dat wij bespreken, houdt zich immers niet aan landsgrenzen.” MSC Van Dam, PvdA: “het klinkt allemaal heel spannend, maar eigenlijk gaat het om heel oude criminaliteit” “Criminaliteit op internet is . . . weliswaar heel gewone criminaliteit, maar verpakt in een nieuw jasje.” MSC Vos, GL:	should be punishable by law. Government has a task to enforce laws.	open/liberal society

	"Het is belangrijk om een zekere mate van veiligheid op de digitale snelweg te bieden, en daarbij passen strafbepalingen. . . . Het blijft alleen de vraag of wetswijzigingen gezonde technologische ontwikkelingen niet in de weg staan." "Mijn fractie vindt dit een tamelijk eng voorstel" Minister of Justice Donner, CDA: "het fundamentele gegeven van internet is dat wij met internet het onderscheid tussen binnen en buiten opgeheven hebben. De private ruimte en de openbare ruimte lopen daardoor in elkaar over." "De overheid heeft in beginsel een verantwoordelijkheid bij de voorlichting van gebruikers."		
[9] *Kamerstuk* 26 671, nr. 22: Report of a General Meeting of the PCCs on the Interior and Kingdom Relations, Economic Affairs, and Justice re. the National High Tech Crime Centre (NHTCC), 20 December 2005	"De kwaliteit van opsporing en vervolging van high tech crime kan nog niet worden gegarandeerd, omdat deze nog te afhankelijk is van de kennis van individuen." "Dat kan wellicht ooit worden geïntegreerd in de opsporing en vervolging van criminaliteit in et algemeen, maar vooralsnog is de tijd daar nog niet rijp voor."	Criminal procedures are still behind. Cybercrime is "high tech" crime (as opposed to "low tech"). Law enforcement agencies/officials should all have knowledge about cybercrime. This fits with the offline = online approach.	*Similarity*: offline and online *Identity*: government has to maintain public order, also in cyberspace
[10] *Kamerstuk* 26 671, nr. 24: Letter of the State Secretary of Economic Affairs re. final advice on Project NHTCC, 18 May 2006	"Dit project concentreert zich primair op het vormgeven van de proactieve taak van de overheid en meer specifiek van de politie, op het gebied van de bestrijding van ICT-criminaliteit." "Ontwikkel een Nationale Infrastructuur voor de	The government has a "proactive" task to combat cybercrime. This seems to aim at prevention. The government has to keep up the pace in order to respond to rapid developments in	*Oppositional*: proactive vs. reactive, international vs. national, virtual vs. physical, public vs. private *Identity*: emphasis on *National* Infrastructure and *National*

	bestrijding van cybercrime." "Deze Nationale Infrastructuur laat zich het best omschrijven als een virtuele ringleiding tussen publieke en private organisaties die betrokken zijn bij de aanpak van cybercrime." "Het Nationaal Meldpunt Cybercrime is per 1 maart operationeel voor meldingen betreffende haatzaaiende en terroristische uitingen op het internet." "Cybercrime is een fenomeen dat zich kenmerkt door snelle technologische veranderingen en een sterke internationale dimensie."	ICT. Cybercrime is strongly international. "Virtual ringleader": implies a space that is circumscribed by a ring. Within this ring, law enforcement agencies have jurisdiction.	Registration Point Cybercrime, meant for all Dutch citizens.
[11] *Handelingen* First Chamber, 30-1346 to 1353: Plenary debate re. ratification bill for the Convention on Cybercrime, and Law Computer crime II, 30 May 2006	MFC Franken, CDA: "Nu is het natuurlijk bijzonder kwalijk wanneer een burgemeester publiekelijk een strafbare en bovendien zeer schadelijke handeling als een soort heldendaad ophemelt, maar het getuigt ook van een grenzeloze naïviteit wanneer iemand nog denkt, dat het verspreiden van een virus of the inbreken in computersystemen een onschuldige bezigheid is van een enkele 'nerd' of een soort Robin Hood, die alleen rijken besteelt ten bate van de armen." "Aftappen is een principiële inbreuk op een grondrecht en bovendien zeer kostbaar voor de providers." "Natuurlijk kunnen wij alleen maar denken in de reële wereld en is het voor een mens noodzakelijk	- Mayors should not praise criminal behavior. What the hacker did was an act of crime. Hackers or persons who spread computer viruses are far from innocent, thinking they are is a sign of naiveté. This mayor is both unintelligent and wrong. By extension, anyone who agrees with this position must be unintelligent and wrong as well. - Wiretapping is an infringement of the constitutional right to privacy. Citizens have a right to privacy. The government should stay outside citizens' homes. - It is impossible for persons to	*Oppositional*: unintelligent vs. smart persons, feeling safe vs. unsafe, privacy vs. intrusion *Identity*: wiretapping against liberal values (individualism) *Similarity*: privacy of the home in the real world applies to the virtual world as well, offline = online

	om te denken in modellen om de gedachten te bepalen. . . . Hoe staat dat echter bij computervredebreuk? Het woord is modelmatig geënt op de realiteit." MFC De Wolff, GL: "Ik voel mij gelukkig nooit onveilig op straat. Er is slechts één weg waar ik mij wel regelmatig onveilig voel, en dat is de elektronische snelweg." Minister of Justice Donner, CDA: "Ceterum censeo obligationes Unitatis Europeae esse implementanda. Pacta sunt servanda!"	think outside the real world. Ideas and principles that should apply to the virtual world are necessarily grounded in the real world. - Cyberspace is unsafe. - Agreements have to be followed! Especially the ones by the EU.	
[12] Coalition Agreement fourth Balkenende cabinet, 7 February 2007	"Veiligheid is een basisvoorwaarde voor een gelukkig bestaan en een kerntaak van de staat. Veiligheid, zekerheid en betrouwbaarheid zijn van steeds grotere betekenis in een open maatschappij. Tegelijkertijd staan ze onder steeds grotere druk, onder meer door de dreiging van internationaal terrorisme." "Garanties voor absolute veiligheid zijn niet mogelijk. Een van de grootste uitdagingen van de komende tijd is om een klimaat van veiligheid, rechtszekerheid en rechtsbescherming te waarborgen dat mensen vertrouwen geeft. Daarbij gaat het niet alleen om bestrijding van criminaliteit en geweld, maar ook om de preventie daarvan."	Without security, you cannot live a happy life. We live in an open society. Government has the task to make sure society is secure, its most important task. There are dangerous Others out there threatening the open society. Government is currently not doing enough to safeguard security, legal certainty and legal protection. These things are necessity for confidence. Government must stop threats from even occurring.	*Oppositional*: Self vs. dangerous Other, open vs. closed society *Identity*: Netherlands is an open society *Complementarity*: prevention and repression of crime
[13] *Kamerstuk* 28 684, nr. 119:	"Veiligheid, stabiliteit en respect kenmerken de	There are threats to the security,	*Oppositional*: threats vs.

Letter of the ministers of Justice, Interior and Kingdom Relations, and others re. security program "Security starts with Prevention," 6 November 2007	samenleving die dit kabinet voor ogen staat. Een samenleving waarin mensen zich veilig, vertrouwd, en onderling verbonden weten." "project *Veiligheid begint bij Voorkomen*" "de bestrijding van 'minder zichtbare vormen van criminaliteit', zoals cybercrime" "Met 'ernstige vormen van criminaliteit' wordt . . . in het bijzonder gedoeld op *financieel-economische criminaliteit, cybercriminaliteit en georganiseerde misdaad*." "De langzamerhand onbegrensde mogelijkheden van ICT, en internet in het bijzonder, hebben een keerzijde" On prevention: "Van belang is dat burgers en bedrijven zelf de nodige maatregelen nemen voor een veilige elektronische communicatie." "Bevorderen van het bewustzijn . . . door de overheid . . . is daarvoor een voorwaarde."	stability, and respect in Dutch society. Apparently, society is currently characterized by those traits. It is preferable to prevent crime than to combat crime. Cyber crime is both a "severe" type of crime and a "less visible" type of crime. ICT/internet's unlimited possibilities are a liability. Threaten society. The government has to secure society.	security, unlimited possibilities of the virtual vs. the limited possibilities of the physical *Identity*: Dutch society should be secure, stable, respectful
[14] *Kamerstuk* 26 643, nr. 103: Letter of the minister of Justice and others re. policy agenda "Recalibration ICT Security Policy," 17 December 2007	"Voorkomen van maatschappij ontwrichtende gebeurtenissen" "Het betreft gebeurtenissen die ten koste van bijna alles moeten worden voorkomen. Daarbij treedt de overheid sturend op. . ." "Kijkend naar de toekomst is het kabinet dan ook van mening dat onze samenleving weerbaar dient te zijn tegen dreigingen: tegen fysieke maar ook tegen digitale dreigingen, zoals ICT-verstoring of	The government has a responsibility to secure citizens from society-disrupting events. These kind of events legitimize an almost unlimited use of governmental powers. Society is currently not resilient (enough) against threats. Threats have to be prevented from	*Oppositional*: government vs. citizens, peacefulness vs. external threats *Complementarity*: prevention and repression

	cybercrime." "Evenals bij andere vormen van criminaliteit begint een effectieve aanpak van cybercrime bij preventie."	coming into existence.	
[15] *Kamerstuk* 28 684, nr. 149: Stenographic report of a General Meeting of the PCCs on Justice and Interior and Kingdom Relations re. law enforcement *vis-à-vis* cyber crime and internet abuse, 19 May 2008	MSC Gerkens, SP: "In 1996 ging ik online en belandde in een wereld die toen nog waarlijk anarchistisch was. . . . Hoewel sommige stukjes internet nog steeds van het individu zijn, zijn er steeds meer gebieden die roepen om regulering. Voor sommigen doet dat pijn. . . . Omdat deze wereld alle door mensen geschapen grenzen overschrijdt, is het de vraag welke autoriteit die taak moet oppakken. In dat hiaat hebben de criminelen hun slag geslagen. De leemte maakte internet tot een paradijs. Het is tijd dat wij die ruimte terugpakken." MSC Teeven, VVD: "Naar het oordeel van de VVD-fractie kan het bij bepaalde vormen van criminaliteit – wij denken niet alleen aan terrorisme en georganiseerde misdaad, maar ook kindermisbruik – nodig zijn om regelmatig te kunnen hacken om criminelen en terroristische activiteiten te onderzoeken, zonder dat de betrokkenen daarvan al direct op de hoogte worden gesteld." MSC Heerts, PvdA: "Uit de woorden van de minister over een hernieuwde doordenking van de betekenis van	Many if not most parts of the Internet have been claimed by various parties. Internet no longer "anarchical." This mandates regulation. But we are behind: criminals have jumped into this vacuum. This is a battle we have already lost, but we may still win the "war" against criminals. Terrorism is part of cyber crime. Terrorists act relatively anonymous, and strike indiscriminately. We have to answer such tactics in kind. Security appears to go at the cost of privacy. Quotes a professor,	*Oppositional*: anarchy vs. rule of law, criminals vs. law enforcers, privacy vs. security *Identity*: terrorism against the open society must be stopped *Similarity*: virtual world and physical world are, in principle, equal, but its distinct nature requires new ways of thinking about policies (this implies that the two are, in fact, separate) *Complementarity*: not only public order must be maintained, but entire society must protected/secured

privacy leidt deze hoogleraar zelfs af dat dit alleen maar kan betekenen dat de minister het privacybegrip wil inperken.”	derives authority. How does minister respond?
MSC Anker, CU:	
“Internet moet dus geen vrijplaats zijn voor strafbare feiten. Als Kamer merken wij dat er een zekere bewustwording over is.”	Internet is now a refuge for punishable offenses. Earlier, we did not realize this.
MSC Joldersma, CDA:	
“Ik heb de indruk dat wij nog te weinig vat hebben op die ingewikkelde wereld van cybercrime. Het gaat ons voorstellingsvermogen te boven en de brief van het kabinet lijkt nog heel erg uit te gaan van dingen die wij in de gewone wereld gebruiken.”	The world of cybercrime is complicated. We still know too little about it. This implies being behind. We need new approaches: policy based on ideas from the ‘normal’ world is insufficient. (Then virtual world is not normal.)
“Ik ben ervan overtuigd dat er ongelooflijk veel ‘nerds’ zijn, die nu niet de maatschappelijke verantwoordelijkheid voelen om te melden”	“Nerds” are lone individuals, feel no societal responsibility.
Minister of Justice Hirsch Ballin, CDA:	
“Wat weten wij, ook internationaal bezien, over aard en omvang van internetcriminaliteit? Internationaal staat het onderzoek nog in de kinderschoenen. Ik denk dat wij op dit terrein vooroplopen”	Research into internet crime is still fledgling (it has been from the start…), but the Netherlands is doing better.
“In het kader van de terminologie wordt wel eens gezegd dat je of meer voor de veiligheid bent of meer voor de persoonlijke levenssfeer, maar ik ben voor de veiligheid, ook in de persoonlijke	Choosing either safety or privacy is a false dichotomy.

	levenssfeer.”		
	“Het is mijn taak en verantwoordelijkheid om op te treden tegen de misstanden en tegen alles wat daar [op internet] crimineel of anderszins onrechtmatig wordt gedaan. De preventie hoort daar uiteraard ook bij.”	Authority argument: I have a legitimate task to combat cyber crime/terrorism. This is fact.	
	Motie-Teeven/Heerts: “overwegende dat de opsporing van terroristische misdrijven en misdrijven in relatie tot georganiseerde criminaliteit via het internet buitengewoon ingewikkeld is; constaterende dat het rechtmatig virtueel kunnen doorzoeken om terroristische en criminele activiteiten te kunnen opsporen, zonder dat betrokkenen daarvan al direct bij aanvang op de hoogte worden gesteld; verzoekt de regering, te bewerkstelligen dat dit virtueel doorzoeken, als hierover omschreven, op internet mogelijk wordt”	Internet complicates criminal investigations into terrorism; this necessitates extraordinary measures. In order to break their anonymity, we must also remain anonymous. (Virtual warrants)	
	Motie-Joldersma c.s.: “overwegende dat een digitale aanslag met een terroristisch karakter niet denkbeeldig is en dat de voorgestelde handhavingsmaatregelen en juridische instrumenten nog onvoldoende vanuit de virtuele wereld van cybercrime zijn doordacht” (Reactie Hirsch Ballin: “Wij zullen deze motie daarom graag uitvoeren.”)	A digital terrorist attack is a very real possibility. We have to adapt counterterrorism measures to meet this threat; these measures are currently insufficient.	
[16] *Handelingen* Second Chamber, 33-3155 to 3197:	MSC Knops, CDA: “Dan de dreiging die Nederland de komende jaren	Threat of cyber attacks is indisputable. Therefore, have to	*Oppositional*: cyber war vs. cyber peace

Continuation of plenary debate re. Defense ministry annual budget 2010, 3 December 2009	te wachten staat. . . . Op dat punt [cyberdreiging] dien ik een motie in om het kabinet nog verder aan te sporen om daarbij een aantal zaken op te pakken." Motie-Knops c.s.: "overwegende dat cyberaanvallen op computersystemen en netwerken een nieuw type bedreiging vormen; . . . overwegende dat in cyberwarfare met defensieve capaciteiten alleen niet volstaan kan worden; . . ."	prepare our defenses. But also requires an offense (comparison with physical warfare). We are currently in "cyber peacetime," but we may be attacked at any time.	*Similarity*: physical and cyber warfare *Complementarity*: defensive and offensive cyber capabilities
[17] *Kamerstuk* 26 643 and 32 123 X, nr. 149: Letter of the minister of Defense re. progress digital defenses, 11 March 2010	"In onze technologisch hoogontwikkelde, open samenleving is sprake van toenemende afhankelijkheid van ICT. Ook in de toekomst blijft ICT zich snel ontwikkelen en tot nieuwe toepassingen en afhankelijkheden leiden. Dit brengt ook dreigingen met zich mee." "Maatschappelijke ontwrichting kan ontstaan wanneer kwaadwillenden vitale ICT-systemen ontregelen . . ."	The Netherlands is dependent on ICT. This offers both threats and opportunities. Attacks may lead to societal disruptions. Government no longer only maintaining public order but securing society.	*Identity*: Netherlands as an open society *Oppositional*: citizens vs. dangerous Others
[18] *Kamerstuk* 26 643, nr. 164: Letter of the minister of Defense re. progress of setting up digital defenses within ministry, 12 July 2010	"Defensie is in toenemende mate afhankelijk van betrouwbare, veilige, en beschikbare netwerken en andere ICT-applicaties. Om de inzetbaarheid van de krijgsmacht te blijven waarborgen, zal Defensie haar digitale weerbaarheid de komende jaren belangrijk moeten versterken." "Deze groeiende afhankelijkheid en kwetsbaarheid van netwerken en software noodzaken tot een gezamenlijke aanpak, zowel nationaal als internationaal, zodat Nederland kan blijven	Defense ministry and armed forces are becoming more and more dependent on ICT. MoD has to increase its digital resilience, or risk attacks. MoD's traditional tasks also extend to the digital domain, i.e. monopoly on violence also applies there. Cyberspace *is* a domain.	*Oppositional*: Self (Netherlands) vs. dangerous Others *Similarity*: monopoly on violence in physical and cyberspace, anarchy of the international system also applies

	beschikken over een betrouwbaar, veilig en toegankelijk digitaal domein."		
[19] *Kamerstuk* 26 643, nr. 174: Letter of minister of Security and Justice presenting National Cyber Security Strategy, 22 February 2011	"Deze aanpak moet ertoe bijdragen dat Nederland tot de toplanden behoort in de wereld op het gebied van cyber security." "ICT is van fundamenteel belang voor onze samenleving en economie en een katalysator voor (verdere) duurzame economische groei. Tegelijkertijd leidt de kwetsbaarheid, afhankelijkheid en complexiteit van ICT tot nieuwe dreigingen waartegen betrokken (inter)nationale organisaties intensief zullen moeten samenwerken en krachtiger moeten optreden."	ICT is fundamental for society, is internationally oriented, as is the Netherlands itself. ICT is constituted as a subject with vulnerability, complexity, and dependency. This is a weakness that dangerous Others while inevitably exploit. This legitimates new measures.	*Oppositional*: Self vs. dangerous Others, ICT as opportunity vs. ICT as weakness *Complementarity*: transnational character of ICT necessitates cooperation at national and international level *Identity*: Netherlands as an internationally oriented country (presence of international organizations), a booming cyber security (which is transnational) would fit in.
[20] *Kamerstuk* 30 821, nr. 12: Letter of the minister of Security and Justice re. National Risk Assessment 2010 and new priorities of Rutte-I cabinet, 22 February 2011	"Zorg voor een vrije en veilige samenleving is de belangrijkste taak van de overheid. Het voorkomen dat de samenleving ontwricht raakt, ziet het kabinet als één van de belangrijkste opgaven om die zorg voor veiligheid waar te maken." "De Nederlandse welvaart is te danken aan onze open en veilige samenleving, internationale oriëntatie en een geografische positie . . . Onze veiligheid hebben wij te danken aan een robuuste rechtsstaat, een lange traditie van samenwerken aan veiligheid en welvaart die zijn wortels heeft in het bedwingen van het water en een actieve internationale samenwerking . . ." "De ontwikkeling ICT biedt ongekende	Government is responsible for collective safety of society. In order to keep society free, government needs to protect it. (Free from outside influence/threats.) The Netherlands is an internationally oriented country, resulting in both prosperity and security. Government has to honor these traditions. ICT is fundamental for society,	*Oppositional*: Self vs. dangerous Others, ICT as opportunity vs. ICT as weakness, individual vs. collective, government vs. citizens. *Complementarity*: transnational character of ICT necessitates cooperation at national and international level; government and citizens must cooperate *Identity*: Netherlands as an internationally oriented country (presence of international organizations), a booming cyber

	mogelijkheden. . . . De maatschappij wordt steeds meer afhankelijk van het gebruik van ICT. Uitval van systemen, misbruik van ICT door kwaadwillenden en het onbetrouwbaar worden van data kunnen ernstige gevolgen hebben." "Dit kabinet staat voor een participerend veiligheidsbeleid. Dat betekent dat het kabinet burgers en bedrijven zelfredzaam en weerbaar wil maken, onder andere op het terrein van mogelijke crises. . . . Er ligt nadrukkelijk een rol voor de overheid om die zelfredzaamheid en weerbaarheid te faciliteren."	is internationally oriented, as is the Netherlands itself. ICT is constituted as a subject with vulnerability, complexity, and dependency. This is a weakness that dangerous Others while inevitably exploit. This legitimates new measures. Citizens and companies have personal responsibilities, but government has to facilitate them collectively.	security (which is transnational) would fit in.
[21] *Kamerstuk* 26 643, nr. 188: Letter of ministers of the Interior and Kingdom Relations, and Security and Justice re. hack at DigiNotar, 5 September 2011	"De inbraak bij DigiNotar en het gebleken aanmaken en gebruik van 'valse' certificaten vormen een ernstige aantasting van het vertrouwen en de integriteit van het digitale communicatie-verkeer met potentieel grote gevolgen voor dit verkeer." "Het Kabinet acht een betrouwbare digitale communicatie van wezenlijk belang en stelt alles in het werk om dit te borgen. . . . Voor het Kabinet is de bedreiging van het vertrouwen in en de integriteit van het internetverkeer onacceptabel."	The government has tasks to prevent theft, and to maintain trust in and integrity of digital communication. This case presents a failure on the part of the government, which apparently has not yet done enough. These events are "unacceptable" which is why the government "will do everything" to maintain the public order.	*Oppositional*: collective security vs. individual responsibilities *Identity*: threats to open society must be stopped.
[22] *Kamerstuk* 26 643, nr. 189: Letter of ministers of the Interior and Kingdom Relations, and Security and Justice re. measures taken in response to hack at	"Digitale informatie-uitwisseling is een essentieel onderdeel geworden voor het functioneren van de Nederlandse samenleving. Het gaat hierbij zowel om het economische verkeer als om het functioneren van de overheid."	Threats against information exchange are threats against Dutch society. The Internet is never completely safe, but government has a legitimate task	*Oppositional*: Dutch Self vs. dangerous Others, government vs. society *Identity*: security is necessary for

DigiNotar, 16 September 2011	"Gegeven het feit dat internet per definitie niet als volledig veilig te beschouwen is alsmede internationaal bepaald wordt, kunnen inbreuken op die veiligheid nooit geheel worden uitgesloten."	to safeguard it.	a happy life
[23] *Handelingen* Second Chamber, 12-99 to 127: Plenary debate re. hack at DigiNotar, 13 October 2011	MSC Gesthuizen, SP: "Wij staan voor een serieus drama, een digitaal doemscenario." MSC Hachchi, D66: "De overheid gaat met haar tijd mee en zet ICT en internet in bij haar communicatie met mensen. D66 is daarvan groot voorstander, maar de overheid moet niet de veiligheid uit het oog verliezen. Na alle ICT-problemen van de laatste tijd twijfel ik of de overheid wel 'in control' is" MSC El Fassed, GL: "We weten hoe het wel moet, maar niet waarom het de overheid nog steeds maar niet lukt om privacy en veiligheid bovenaan te zetten." MSC Hennis-Plasschaert, VVD: "De zaak DigiNotar was en is een enorme wake-upcall. Er lijkt heel lang sprake te zijn geweest van een welhaast ongefundeerd vertrouwen in ICT-infrastructuur, -diensten, en -producten en vooral in de veiligheid daarvan." MSC Gesthuizen, SP: "We weten inderdaad dat internet niet 100% veilig is. Risico's kun je niet uitsluiten. Je kunt wel het	Failure of the government to ensure digital security is a "doom scenario." Its failure is a threat to society. Government is not in control, existing policies are insufficient. We have proper knowledge about ICT, yet we are still behind. DigiNotar case underwrites the necessity of the government's role in cyber security. It has a job to protect society. Guaranteed safety not possible, but government has to do everything within its possibilities. Widespread agreement about this. Accepted as fact.	*Oppositional*: Dutch Self vs. dangerous Others, government vs. society, collective vs. individual security *Similarity*: ICT security and disaster planning

	gevaar beperken door de risico's zo veel mogelijk in kaart te brengen en daar een passend systeem voor te vinden." MSC Hachchi, D66: "Ik denk dat iedereen het met de heer Koopmans eens is dat 100% veiligheid op internet niet mogelijk is." MSC Elissen, PVV: "De PVV-fractie pleit er langer voor om databeveiliging te benaderen op soortgelijke wijze als rampenbestrijding." Minister of Security and Justice Opstelten, VVD: "Inbreuken op de veiligheid van het internet raken ons direct. . . . Een aantal Kamerleden had aarzelingen over de scherpte en noodzaak van die strategie [NCSS]. Ik denk dat de hele DigiNotar-affaire die noodzaak in een ander daglicht heeft geplaatst." MSC Hennis-Plasschaert, VVD: "Als liberaal spreekt die eigen verantwoordelijkheid mij zeer aan." Minister of Security and Justice Opstelten, VVD: about motion Hennis et al. on notification obligation: "Daarin staat ongeveer wat ik zelf in de eerste termijn heb gezegd. Het is een krachtige en brede ondersteuning van ons beleid op een heel	Treating data security the same way as disaster planning. Implying that cases like DigiNotar are as catastrophic as natural/physical disasters.

	belangrijk punt."		
[24] *Kamerstuk* 33 000 X, nr. 79, attachment: Cabinet reaction to AIV advice "Digital Warfare," 6 April 2012	"De toenemende dreiging tegen nationale belangen in het digitale domein en de stijging van het aantal (complexe) digitale aanvallen baren het kabinet zorgen. Spionage, sabotage, misdaad en terrorisme langs digitale weg vormen een directe bedreiging voor de nationale veiligheid." On right to self-defense: "De constatering van de commissie dat ten aanzien van digitale aanvallen geen ander regime geldt dan voor het gebruik van geweld in het fysieke domein, acht het kabinet van belang."	Digital threats are increasing, These are a threat to Dutch society, identity, and security. Since digital warfare is like physical warfare, the principles of "just war" also apply. Digital attacks are attacks against Dutch national security, monopoly on violence lies with Dutch armed forces.	*Oppositional*: Dutch Self vs. dangerous Others, government vs. society, collective vs. individual security *Similarity*: digital and physical warfare are, in principle, the same
[25] *Kamerstuk* 33 321, nr. 1: Letter of the minister of Defense presenting Defense Cyber Strategy, 27 June 2012	"Het digitale domein is, naast het land, de lucht, de zee en de ruimte inmiddels het vijfde domein voor militair optreden." "De Nederlandse krijgsmacht trekt hier de noodzakelijke conclusies uit en wil in het digitale domein de vooraanstaande rol spelen die bij ons land past."	Accepting as fact that cyberspace is a domain like any other physical domain. This means that armed forces also have "jurisdiction" there. Netherlands is a very progressive country, also in cyberspace.	*Oppositional*: inside vs. outside *Similarity*: digital domain compared with physical domains *Identity*: threats to open society must be stopped, Netherlands as an internationally oriented country.
[26] *Kamerstuk* 33 694, nr. 1: Letter of the minister of Foreign Affairs re. international security strategy, 21 June 2013	"Vrede en veiligheid zijn geen vanzelfsprekendheid. Het vergt een continue investering om een veilige wereld en daarmee een veilig Nederland zeker te stellen." "Tegelijkertijd vormen cyberaanvallen een van de grootste veiligheidsdreigingen van deze tijd. Moderne dreigingen laten zich weinig gelegen liggen aan grenzen of dijken. Interne en externe veiligheid zijn steeds minder goed van elkaar te	The world is unsafe. If the world is safer, then the Netherlands is safer. Cyber attacks are one of the biggest security threats. They may disrupt our society with one blow. We have to protect our country from both internal and external threats. In order to secure our borders,	*Oppositional*: Dutch Self vs. dangerous Others, government vs. society, collective vs. individual security *Identity*: threats to open society must be stopped, Netherlands as an internationally oriented country.

	scheiden. Wat er in de wereld om ons heen gebeurt, raakt direct aan onze eigen veiligheid en welvaart. Met zijn open economie en internationale oriëntatie is Nederland immers sterk afhankelijk van het buitenland." On ICT/cyber security: "Maar er is een keerzijde. Wat als alle schermen op zwart springen? Onze samenleving zou in één klap ontwricht raken. De digitale infrastructuur wordt steeds kwetsbaarder.	we have to operate outside those borders.	
[27] *Kamerstuk* 33 321, nr. 2: Letter of the minister of Defense re. progress made with Defense Cyber Strategy, 26 August 2013	"Defensie Cyber Commando (DCC)" "De snelheid waarmee ontwikkelingen in het digitale domein zich voltrekken, stelt hoge eisen aan het adaptieve en innovatieve vermogen van Defensie.	Term "DCC" borrowed from US Cyber Command. Implies that the Netherlands is/must be following example set by them. Rapid developments in digital domain.	*Oppositional*: inside vs. outside *Similarity*: digital domain compared with physical domains *Identity*: threats to open society must be stopped
[28] *Kamerstuk* 30 977, nr. 61: Letter of the minister of the Interior and Kingdom Relations offering cabinet reaction to Snowden leaks, 13 September 2013	"Het kabinet volgt met aandacht de reactie van de Verenigde Staten op de onthullingen van de heer Snowden. Het kabinet hecht, zoals eerder gemeld, zeer aan zorgvuldige en deugdelijke bescherming van persoonsgegevens. Het is daarom noodzaak om waar nationale veiligheid en privacybescherming elkaar raken, zo transparant mogelijk te zijn over procedures, bevoegdheden, waarborgen, en toezichtmaatregelen."	Personal data very important to government, as is right to privacy. But national security sometimes necessitates extreme measures.	*Oppositional*: (national) security vs. privacy *Identity*: the Netherlands is an open liberal country (privacy), but have to protect that open society
[29] *Kamerstuk* 30 977, nr. 71: Report of a General Meeting of the PCC on the Interior and Kingdom Affairs re. cabinet reaction to Snowden leaks, 14	MSC Van Raak, SP: "Maar vooral, Minister, spreek nu eindelijk eens een keer uit dat bondgenoten zo niet met elkaar omgaan, dat we op deze manier de internationale strijd tegen het terrorisme niet kunnen winnen en	There is a fight against international terrorism. We need allies in this battle whom we can trust. "Re-politicizing" cyber security,	*Oppositional*: friends/allies vs. enemies/terrorists, Dutch Self vs. (dangerous) Other, security vs. privacy *Identity*: a Western country like

November 2013	dat we dit niet accepteren. Maak het politiek, zorg voor balances, zorg ervoor dat de Amerikanen niet alles kunnen doen." MSC Bontes, PVV: "Mijn vraag is of met zo'n overeenkomt [no-spy agreement between US and the Netherlands] de strijd tegen het terrorisme gewaarborgd blijft." "Van de strijd tegen terrorisme kun je niet lichtzinnig zeggen dat allemaal wel meevalt en dat we de nadruk moeten leggen op privacybescherming. Nee, die twee moeten in balans zijn. MSC Van Raak, SP: "Het optreden van Amerika belemmert of bedreigt de internationale strijd tegen het terrorisme juist. . . Is hij [MSC Bontes] het met mij eens dat het optreden van de Verenigde Staten er juist toe leidt dat bondgenoten elkaar niet meer kunnen vertrouwen en dat terroristen de lachende derden zijn?" MSC Recourt, PvdA: "De norm die mijn fractie hanteert bij deze balans, is dat je alleen als het noodzakelijk is, gericht en gecontroleerd gegevens van burgers kunt opvragen, bijvoorbeeld bij providers. Daarbij komen proportionaliteit en subsidiariteit om de hoek kijken. Met deze criteria moet je bekijken of het terecht is dat iemands privacy geschonden	which is now depoliticized. The fight against terrorism goes before everything. Should we emphasize privacy too much, we will lose the fight, suffer attacks, etc. Cooperation is based on mutual trust. It's okay to spy on enemies and terrorists, but not okay to spy on your friends. Surveillance is legitimate in fight against terrorism, but the right to privacy might only be suspended only there is a clear and real necessity. This is only allowed if	the US is liberal, should not spy on its friends (the Netherlands). Russia/China on the other hand, we may expect it from them.

	wordt voor dat andere doel, namelijk de nationale veiligheid.”	national security is at stake.
	MSC Dijkhoff, VVD:	
	“In grote lijnen is de VVD van mening dat je mensen die dreigen terroristische activiteiten te ontplooien, gericht in de gaten moet houden als je daar informatie over hebt. . . . Dan kom ik op de vraag wat andere landen in Nederland doen. Hierin wil ik ook enige nuance aanbrengen. Bij de Russen en de Chinezen gaan we er eigenlijk wel van uit dat ze het doen. Als dit zou uitkomen, zouden we daar niet heel verbaasd over zijn. Het doet natuurlijk extra pijn als een bondgenoot het doet, als een land waarmee je samenwerkt, het doet. Daarvan verwacht je terughoudendheid.”	Makes a clear distinction between Western allies and Eastern opponents. We agree Russia/China are obviously spying on us, this is fact. But they are our adversaries. Americans are our friends, you don’t spy on your friends.
	Minister of the Interior Plasterk, PvdA:	
	“Aangezien het terrorisme voor het overgrote deel internationaal van karakter is, is de bestrijding daarvan ook internationaal van karakter. Het is dus buitengewoon waardevol dat we in de Amerikanen – dat geldt ook voor andere diensten, in andere landen – goede bondgenoten hebben. Dat is het uitgangspunt.”	
	On spying on non-Americans: “Dat is wat ons betreft wellicht nog tot daar aan toe als men dat richt op een regio in de wereld waar heel grote politieke instabiliteit is, een regio die echt als vijandig kan worden beschouwd. Als we echter als bondgenoten samenwerken in de strijd tegen het	Fight against terrorism is international, as is terrorism itself. We need good allies, the US is a good ally. This is the starting point. However, they are

	terrorisme, dan stellen we dus niet op prijs dat we in diezelfde categorie terechtkomen." MSC Van Raak, SP: "Dat wil ik niet, omdat ik het onfatsoenlijk vind dat bondgenoten zo met elkaar omgaan. Regering en parlement moeten onze burgers kunnen beschermen. Maar dit geldt juist ook in het kader van de bestrijding van het internationale terrorisme. Als de geheime diensten zo met elkaar omgaan, kunnen ze ook niet voldoende samenwerken. Dát moet je allemaal politiek maken."	spying on non-Americans. We don't care if they spy on politically unstable regions or enemies. Right to privacy does not apply to them. But we are friends. Real outrage is Americans spying on allies. We don't want to be in the same category as the "terrorists."

APPENDIX C

Motion by member of the Second Chamber Knops et al. urging the Dutch government to develop a cyber security strategy. *Kamerstuk* 32 123 X, nr. 66. (2009).

(original)

MOTIE VAN HET LID KNOPS C.S.
Voorgesteld 3 december 2009

De Kamer,

gehoord de beraadslaging,

overwegende, dat cyberaanvallen op computersystemen en netwerken een nieuw type bedreiging vormen;

overwegende, dat deze dreiging niet alleen uitgaat van de georganiseerde criminaliteit of terroristische organisaties, maar potentieel ook van krijgsmachten van andere landen;

overwegende, dat diverse NAVO-landen speciale afdelingen opgericht hebben voor digitale oorlogsvoering, zoals de Verenigde Staten, het Verenigd Koninkrijk en Duitsland, en daarbij ook offensieve capaciteiten ontwikkelen;

overwegende, dat in cyberwarfare met defensieve capaciteiten alleen niet volstaan kan worden;

constaterende, dat cyberwarfare in de Defensiebegroting 2010 ontbreekt;

verzoekt de regering in interdepartementaal verband een cyber security strategie te ontwikkelen, actief bij te dragen aan de gedachtevorming over cyberwarfare binnen de NAVO en de Kamer hierover uiterlijk 1 maart 2010 te informeren,

en gaat over tot de orde van de dag.

Knops
Voordewind
Eijsink

(translation)

MOTION BY MEMBER KNOPS ET AL.
Proposed 3 December 2009

The Chamber,

having heard the debate,

considering that cyber attacks against computer systems and networks form a new type of threat;

considering that this threat does not only come from organized crime or terrorist organizations, but potentially the armed forces of other countries as well;

considering that several NATO countries have created special divisions for digital warfare, like the United States, the United Kingdom, and Germany, in which they are also developing offensive capabilities;

considering that with cyber warfare, it is insufficient to only have defensive capabilities;

establishing that cyber warfare is missing in the 2010 Defense budget;

urges the government to develop interdepartmentally a cyber security strategy, to actively participate in the thought process on cyber warfare within NATO, and to inform the Chamber about this before 1 March 2010 at the latest,

and proceeds to the order of the day.

Knops
Voordewind
Eijsink