The Discourse of Cyberterrorism

'Exceptional measures call for the framing of exceptional times'

Research question

How and why has 'cyberspace' been constituted as a source of danger and a location for legitimate security practices in the Netherlands?

Nouschka Myrthe Auwema
nouschkaauwema@telfort.nl
s1121774

Thesis MSc Political Science
Thesis supervisor: Dr. Francesco Ragazzi
Second Reader: Prof. dr. Petr Kopecký

Word Count: 18.169
13 June 2015

Table of Contents

Abstract **3**

Introduction **4**

Chapter 1: Thesis Proposal **8**

Literature Review 8

Theoretical Framework 13

Hypothesis 16

Object of Study 16

Methods of Data Generation and Analysis 17

Scope and Limitations 19

Chapter 2: Danger in Cyberspace: The Field of Cyberterrorism **20**

History of the field 20

Actors within the field 22

Chapter 3: Framing Cyberterrorism **26**

Cyberterrorism is not a threat 27

Cyberterrorism is a threat right now 28

Cyberterrorism has the potential to become a threat in the future 29

Framing danger in cyberspace as cyberterrorism 34

Chapter 4: Sociology of the Actors of Cybersecurity **36**

Sociological background: technological capital, legitimacy and authority 36

Interests 39

Conclusion and Discussion **44**

Illiberal practices in the Netherlands? 46

The need for cybersecurity norms 46

References **47**

Appendix A: List of questions for interviews 52

Appendix B: Transcripts of interviews 53

Abstract

The configuration of the discourse of cyberterrorism in the Netherlands is a mix of public and private actors that have diverging views about whether cyberterrorism is a genuine security threat. How and why have several of these actors argued that it is a genuine security threat? What was their interest in doing so? Has cyberterrorism possibly been framed or hyped as a genuine security threat? This thesis examines the discourse of cyberterrorism in the Netherlands by examining the field, the position on cyberterrorism of the actors within this field, and finally, their levels of technological capital, legitimacy and authority. Considering the differences in these levels, this thesis contends that public and private actors have different interests in arguing that cyberterrorism is a threat. While public actors are concerned with the protection of Dutch cyberspace and the Dutch society, private actors, with the exception of Fox-IT, have multiple interests. This has led these private actors to frame or hype cyberterrorism as a genuine security threat, without the necessary background to base their statement on. Exceptional measures have led to the framing of exceptional times.

Introduction

Something called 'cyberspace' is a fairly recent phenomenon, in which billions of people nowadays take part and interact with each other. Cyberspace has, according to Frans Osinga, three layers: a physical layer of infrastructure; a neutral or logical layer that contains the internet (and intranets); and a social layer that interacts with the other two (Osinga 2012, 8). The internet, a small part of cyberspace, has had the most profound influence in daily life. In 2012, "more than 2.2 billion people were connected to the internet, 32.7% of the world population" (Ducheine et al. 2012, 1). Especially with the rise of the social media such as Facebook, Twitter, MySpace and many others, it seems like cyberspace is a friendly space. Cyberspace has also had an effect on the military, when cyber was added as a fifth domain, to the four existing ones: land, sea, air and space (Rothman and Brinkel 2012, 51). The military is involved because, according to Ducheine et al., cyberspace has also become a new space for contest – "an arena to be either defended and secured or penetrated and exploited" – by states as well as by non-state actors (2012, 2).

In other words, cyberspace has become securitised. Cybersecurity has been a challenge for government as well as private actors, since the very start of cyberspace and the internet (Rothman and Brinkel 2012, 49). In the Netherlands, cybersecurity is defined by the National Coordinator for Security and Counterterrorism (NCTV) as: "a state of being free of danger or damage caused by disruption or fallout of information and communication technology (ICT) or abuse of ICT. This danger, damage or fallout can be the result of digital warfare, digital espionage, digital terrorism, digital activism, and digital crime" (NCTV 2011).

Ducheine et al. argue that "between 2006 and 2009 there has been a 400% increase in cybersecurity threats and incidents within US civilian organisations" (2012, 2). It has been argued that one of these threats is digital terrorism, or also called cyberterrorism. This form of cybercrime is the focus of this research. With the rise of cyberspace and especially the internet, cyber has been added as a component to terrorism. Terrorism has been, throughout world history, a contentious act. It has been used by states, as well as by non-state actors (Rogers 2012, 224). While the actions of these actors result in the deaths of a few thousand people each year, which makes it only a minor cause of death across the world, by the early 2000s, terrorism was elevated into "the principal challenge to security" (Rogers 2012, 222). That governments have noticed the threat of cyberterrorism is apparent through the fact that they have focused some of their (intelligence) capabilities to monitoring and detecting cyberterrorism (Conway 2007, 73).

In the literature about cyberterrorism there is a lot of disagreement about whether cyberterrorism is a genuine security threat. Authors such as Cronin (2003), Furnell and Warren (1999), and Weimann (2005) have a “concerned view that see cyberterrorism as constitutive of a genuine security threat” (Jarvis, Macdonald and Nouri 2014, 69). Other authors such as Conway (2007, Bendrath (2003), and Giacomello (2004) argue that cyberterrorism “is little more than a hyperbolic media construction” (Jarvis, Macdonald and Nouri 2014, 69). How has this debate about whether cyberterrorism is a genuine security threat taken form in the Netherlands?

In the Netherlands, the earliest form of protecting the population to the 'dangers of cyberspace' was the Computer Crime Law that came into effect on March 1, 1993 (Blane 2003, 17-18). This law was based on a report of the Advisory Committee on Computer Crime, established in the early 1980s. Thus more than 30 years ago, at the very start of cyberspace and the internet, the Dutch government already came to think that 'cyberspace' could inhabit a threat to government and society and it therefore needed protection. But is this worry justified? The Dutch government certainly thinks so: the National Coordinator for Security and Counterterrorism has stated that the increasing dependence on ICT makes society more and more vulnerable to abuse and disturbance (NCTV 2011, 1).

In 2007, the Committee of Experts on Terrorism (CODEXTER) of the Council of Europe conducted a survey among its member states to research the issue of cyberterrorism. For the Netherlands, it became clear that while the National Coordinator for Security and Counterterrorism is mainly responsible for the countering of cyberterrorism, other actors such as the national prosecutor's office, the police and the Intelligence and Security Services were also taking part. The Dutch government found that, if they wanted to be better able to counter cyberterrorism, and cybercrime in general, they had to establish an agency that could oversee this shared approach. This resulted in the implementation of the National Cyber Security Strategy (NCSS) and an accompanying Centre (NCSC) in 2011.

According to the National Coordinator for Security and Counterterrorism the need for this strategy is that safe and reliable ICT is of utmost importance to the prosperity and wellbeing of the Netherlands, the provision of sustainable economic growth as well as the use of social media (NVTC 2011, 2). While ICT thus creates chances, it also enhances the vulnerability of a society that increasingly relies on it. Therefore the strategy (NCSS) argues that cooperation between public and private actors is necessary to deal with cybersecurity and cybercrime, also internationally (NCTV 2011, 3).

In response to questions concerning cyberattacks in the USA asked by Member of Parliament Klaas Dijkhoff, the former Dutch Minister of Security and Justice Ivo Opstelten mentions that counterterrorism and cybersecurity are, alone as well as in combination, a priority to the General Intelligence and Security Service (AIVD) and that further investments are needed to keep up with technological developments (Minister of Security and Justice 2013). Furthermore, the National Cyber Security Centre, the General and Military Intelligence and Security Service (AIVD and MIVD), and the High Tech Crime Unit of the police are aware that state and non-state actors are increasingly involved in cyberspace, and not only for 'good' purposes (Minister of Security and Justice 2013). In order for this cooperation to work properly investments and innovations are also needed.

The previous paragraphs indicate that the Dutch government is convinced, already since the 1980s, that cyberterrorism poses a genuine security threat, as apparent from statements made by Opstelten and the NCTV. Dutch authors that argue otherwise hardly seem to exist or fail to express their opinion in public. In a recent interview by RTL News, scholars Michel van Eeten and Bart Jacobs do argue that cyberterrorism is hardly threatening now and that cyberattacks have become part of secret warfare conducted by Security and Intelligence Services of other countries (RTL News 2014). In their opinion, cyberattacks are thus something that are currently employed solely by governments as part of warfare and/or monitoring. They do not think that terrorists currently have the capabilities to carry out such attacks. However, they do not question that cyberterrorism can become a (greater) threat in the future, if terrorists acquire the necessary capabilities. But how governments have come to see cyberterrorism as a (potential) threat while there has been no cyberterrorist attack to date, is a question that remains unanswered in the Netherlands.

Although there is a large ongoing international debate in the literature about whether cyberterrorism is a genuine security threat, no opponent in this debate has researched why certain actors have ‘framed’ cyberterrorism as a genuine security threat. In order to research how cyberspace is constituted as a source of danger, and thus as a threat to security, the meaning of cyberterrorism needs to be deconstructed by looking at the Dutch actors involved using the term cyberterrorism and what their interests are in framing cyberterrorism as a threat. Bigo argues why researching these questions, through International Political Sociology (IPS) is important: First, “IPS starts its analysis of security by deconstructing the meaning of (in)security in order to trace its origins. Each historical case where the label is used needs to be analysed in order to understand the interests of the actors using it, and the authority that these actors claim they have to draw the limits between security and insecurity.” Second is an

analysis of "what immanent practices are captured under the label of security (or insecurity), by whom and for what reasons" (Bigo 2012, 127).

To assess how the discourse of cyberterrorism is configured in the Netherlands and how the actors involved have argued successfully that cyberterrorism is a genuine security threat, this research will answer the following research question: *How and why has 'cyberspace' been constituted as a source of danger and a location for legitimate security practices in the Netherlands?*

Chapter 1 lays out the research proposal that is the guide for this research. Chapter 2 then goes on by unravelling the field of cyberterrorism in the Netherlands. Chapter 3 gives an overview of the positions that the actors of this field have taken on the (potential) threat of cyberterrorism. Finally, chapter 4 connects these positions with the sociological background of the actors in the field, namely their technological capital, legitimacy and authority. Furthermore, it argues what the interests of the actors are in arguing that cyberterrorism is a threat and how these interests can be connected with their levels of technological capital, legitimacy and authority.

This research will have societal relevance because it attempts to explain how and why cyberterrorism has been framed as something we need to worry about, while there is, arguably, nothing to worry about. Society faces several threats each day in the physical world, which are fairly well known by people. However, because cyberspace is a more fluid concept and difficult to denote, it is sometimes hard to understand what disadvantages it can have. By expressing that some actors in cyberspace pose a threat in such a way that they can disrupt society, these actors may try to create more fear amongst its population than is actually necessary. This research attempts to answer if this (inflicted) fear for cyberterrorism is justified.

Chapter 1: Thesis Proposal

Literature Review

"About 31,300. That is roughly the number of magazine and journal articles written so far that discuss the phenomenon of cyberterrorism. Zero. That is the number of people who been hurt or killed by cyberterrorism at the time this went to press" (Singer 2012). In recent years a lot has been written about cyberterrorism. However, cyberterrorism itself did not kill anyone to date. This quote is an example of the main controversy concerning cyberterrorism. Why is it so high on the political and media agenda, while it is, arguably, not a threat? In other words, have public and private actors framed cyberterrorism, and if so, why?

Wardlaw gives a definition of terrorism: "Political terrorism is the use, or threat of use, of violence by an individual or a group, whether acting for or in opposition to established authority, when such action is designed to create extreme anxiety and/or fear-inducing effects in a target group larger than the immediate victims with the purpose of coercing that group into acceding to the political demands of the perpetrators" (1982, 16). Following this definition, terrorism must impose, or threat to impose, harm on people, with the intention to create fear and/or anxiety. Cyberterrorism, then, must be understood, according to Heickerö, as "the development of 'traditional' terrorism with different means but similar political and ideological agendas. Terrorists on the internet take advantage of modern societies' increasing dependence on computer networks and mobile communications" (2014, 564). Similar to 'regular' terrorism, cyberterrorism must thus at least have the intent to harm or kill people and/or create fear/anxiety within society, but with the use of a different mean, namely cyber.

To research the threat posed by cyberterrorism, Jarvis, Macdonald and Nouri have conducted a survey amongst 118 researchers (2014, 68). It appears that there is no consensus about the essentially contested concept cyberterrorism. There is a lot of disagreement on whether cyberterrorism poses a security threat, what the potential targets are and whether it already has occurred (Jarvis, Macdonald and Nouri 2014, 83). Similarly, Chen, Jarvis and Macdonald state that "there is, at the risk of understatement, something of a disconnect between the amount of attention that cyberterrorism commands and the clarity with which it is understood" (2014, vii). The academic debate about whether cyberterrorism is a genuine security threat can be divided into two sides: those that argue that cyberterrorism is a genuine security threat and those that argue that it is nothing more than a 'hyperbolic media construction'. According to Heickerö, governments and security firms usually are proponents

of the first view, while scientists and analysts at universities and research institutes are more sceptical (2014, 555).

The first group, composed of authors such as Collin (1997) Cronin (2003), Furnell and Warren (1999), and Weimann (2005), argues that cyberterrorism is a genuine security threat. The term was first coined by Barry Collin of the U.S. Institute for Security and Intelligence in the 1980s. In 1997 he was among the first to argue "make no mistake, the threats are real today" (Collin 1997, 17). For Collin, cyberterrorism is a reality because the destructive capacity is similar to physical terrorist attacks, including the ability to cause deaths and wounded (Collin 1997). Another important scholar on this side of the debate is Dorothy Denning. She argues that "the possibility of cyberterrorism remains a concern, as Al-Qaeda and other terrorist groups have become increasingly aware of the value of cyberspace to their objectives" (Denning 2007, 123). Terrorist groups not only use the internet for propaganda uses, communication and data collection, they have also managed to tie hacking groups to them and their cause (Denning 2007, 123).

What these authors have in common is that they see the internet as a positive tool for terrorists to advocate their goals and intentions (Jarvis, Macdonald and Nouri 2014). Similarly, Rogers argues that "the widespread availability of broadband makes it possible to distribute detailed coverage of paramilitary actions within hours of the events. Furthermore, statements by leaders are distributed by all the major means" (Rogers 2012, 231). As a result of globalisation, terrorists and organisations now have more opportunities and access to technologies to not only recruit potential new terrorists, but also to carry out attacks (Cronin 2003, 46). For example, Furnell and Warren argue that with the rise of the internet, "there is now the capability to undermine and disable a society without a single shot being fired or missile being launched" (1999, 28). Another important aspect of their argument is that cyberterrorists are conducting their activities with a specific political or ideological agenda, in contrast to most hackers (Furnell and Warren 1999, 30-31).

The last argument put forward by this group of authors is that the risk that cyberterrorists themselves face has declined because they do not need to detonate bombs, fire shots or launch missiles, and they face a lower financial cost (Cronin 2003; Furnell and Warren 1999; Weimann 2005). Weimann has identified five factors why cyberattacks might appeal to terrorists: "comparatively lower financial costs; the prospect of anonymity; a wider selection of available targets; the ability to conduct attacks remotely; and, the potential for multiple casualties" (Weimann 2005).

More recently, other opinions have been expressed in this debate. This group, composed of authors such as Conway (2007), Singer (2012) Giacomello (2004), and Bendrath (2003), argues that cyberterrorism is "little more than a hyperbolic media construction" (Jarvis, Macdonald and Nouri 2014, 69). The media needed a new 'fantasy' or 'threat' to replace the redundant Cold War threat, while also the political discourse shifted its focus to cyberterrorism (Conway 2007; Jarvis, Macdonald and Nouri 2014, 71). These discourses are not particularly driven by and do not necessarily reflect empirical realities, but they have had significant effects on internet users, because they worry about the possibility of cyberterrorism (Bendrath 2003; Jarvis, Macdonald and Nouri 2014, 71).

What these sceptical authors have in common is that they all suggest that the cost-benefit analysis is not in favour of terrorists, terrorists have too little knowledge to carry out a cyberterrorist attack and the chances of inflicting great damage are little (Giacomello 2004; Conway; 2007; Singer 2012). Mauro Conway argues that although terrorists might want to carry out a cyberterrorist attack, having the ability to do so is something else, also difficult to acquire, and violent jihadis' IT knowledge is not adequate enough to carry out such an attack (2011, 27). This is in contrast with terrorists' knowledge and ability of making bombs and 'real-life' attacks, which are therefore usually less difficult to carry out (Conway 2011, 28). Furthermore, the risk involved in hiring hackers or others, who are capable of carrying out cyberterrorist attacks, is often too high for a terrorist group (Conway 2011, 28).

Peter Singer argues that there are two main parts of the problem of cyberterrorism: first of all, "the way we talk about the issue", and second, "we often mix up our fears with the actual state of affairs" (Singer 2012). There is a lot of disagreement about what a clear definition of cyberterrorism is, whether certain cybercrimes can be seen as cyberterrorism, and whether terrorists are interested in and capable of carrying out a cyberterrorist attack. Singer concludes with stating that terror groups use the internet the same as everyone else does; their main goal, namely, is still to gather and share information with their followers and to recruit potential new terrorists (2012). Heickerö also argues that "the internet is used as a tool for coordination by terrorists who are planning operations. It would thus be unwise and counterproductive to attack a system that benefits them" (Heickerö 2014, 556).

Furthermore, he argues that "it is in the interest of security firms to add to the unease, since there is money to be made from it. Cyberterrorism is not economically rational" (Heickerö 2014, 555). Following this logic, it seems that actors who 'promote' the threat of cyberterrorism have an interest in doing so. Because why is the fear for cyberterrorism so great, while "so far there has not been a single lethal cyberattack, at least not publicly"

(Heickerö 2014, 556)? Heickerö goes on by arguing that cyberattacks to date "do not follow the usual logic of terrorism: spectacular effects and high rates of casualties" (Heickerö 2014, 556). Is cyberterrorism thus a logical choice for terrorists or is the threat of cyberterrorism overstated by public and private actors and is it thus in their own interest to argue that the threat to security is genuine?

The above paragraphs show that both sides of the debate focus on researching whether cyberterrorism is a genuine security threat or not. However, because none of the authors provide evidence that suggests that a cyberterrorist attack has taken place, it may be time to move the debate about cyberterrorism into a different direction. Especially because the two sides of the debate "are unable to conclude whether cyberterror is fact or fiction, or, since they are unwilling to dismiss the threat completely, how long it is likely to remain fiction […] due to too many uncertainties concerning the scope of the threat" (Dunn Cavelty 2008, 20). Instead of researching whether the threat is real or not, the research needs to make a move to how cyberterrorism has been framed as a threat, or as Dunn Cavelty puts is: "why and how is a threat that has little or no relation to real-world occurrences included on the security political agenda?" (2008, 20).

Until now, Dunn Cavelty is one of the rare scholars that has written about the US cyberterror discourse. She argues that "for some years, experts and government officials have warned of cyberterrorism as a looming threat to national security. However, if we define cyberterror as an attack or series of attacks that is carried out by terrorists, that instills fear by effects that are destructive or disruptive, and that has a political, religious, or ideological motivation, then none of the disruptive cyber-incidents of the last years qualify as examples of cyberterrorism. So why has this fear been so persistent?" (Dunn Cavelty 2008, 19). Dunn Cavelty looks at how cyberterror threats are framed in the US and the characteristics of the rapid conceptualisation of cyberspace as a source of danger in the 1990s (2008, 19).

Dunn Cavelty's research "introduces a framework for the analysis of threat frames, partly based on the Copenhagen school's securitization approach" (2008, 21). Securitization theory solely focuses on the speech act of threat framing. Dunn Cavelty defines threat framing as "the process whereby particular agents develop specific interpretive schemas about what should be considered a threat or risk, how to respond to this threat, and who is responsible for it" (2008, 21). Her research only brings her to answering the question of how cyberterrorism is perceived as a threat, namely by threat framing. However, she does not provide an explanation for what the interests of the actors are in framing cyberterrorism as a threat.

In fact, no opponent in the debate has researched why actors argue that cyberterrorism is a threat. They have not gone past the question if cyberterrorism is a threat at all. The debate about the discourse of cyberterrorism can be pushed in a new direction by adopting an International Political Sociology (IPS) approach. IPS deconstructs the meaning of (in)security, through which it can understand the interests of the actors using it and their authority to claim what a security threat is. Furthermore, it does an analysis of the practices that are implemented to counter the specific security threat, by whom and for what reasons (Bigo 2012, 127).

This type of research about the discourse of cyberterrorism, using an International Political Sociology approach, has not taken place in and about the Netherlands. Therefore, this research will be the first to look at the interests of the actors that are involved in the framing of cyberterror threats, thus the discourse of cyberterrorism, in the Netherlands, and the security practices of these actors. To address this gap in the literature, this research will attempt to answer the following research question: *How and why has 'cyberspace' been constituted as a source of danger and a location for legitimate security practices in the Netherlands?*

This research is necessary to conduct because to date no research has been done on why certain actors argue that cyberterrorism is a threat, when it is arguably not a threat at all. This research will attempt to answer which interests public and private actors in the Netherlands have in arguing that cyberterrorism is a (potential) threat. One reason for conducting this research is assessing whether the (potential) threat of cyberterrorism justifies the current measures to counter cyberterrorism in the Netherlands. A concern is namely that by naming certain acts cyberterrorism, these acts become securitized, while there might not be a valid reason to do this. Peoples and Vaughan-Williams argue that "when an issue comes to be treated as a security issue, it is justifiable to use exceptional political measures to deal with it. In other words it is securitized: we treat it with the same degree of urgency as we would a military threat" (2010, 77). Furthermore, this research can lead to additional research on whether liberal regimes, such as the Netherlands, engage in illiberal practices by framing cyberterrorism as a threat.

Theoretical Framework

The focus of this research is the discourse of cyberterrorism. According to Peoples and Vaughan-Williams, discourse can be understood, in Foucauldian terms, as "a series of practices, representations, and interpretations through which different regimes of truth … are (re)produced" (2010, 65). The discourse of cyberterrorism, in the USA, has been researched by Dunn Cavelty with the use of Securitization Theory by Ole Wæver. Wæver argues that "in place of accepting implicitly the meaning of security as a given and then attempting to broaden its coverage, why not try instead to put a mark on the concept itself, by entering into and through its core?" (1995, 47). This thus entails taking the concept of cyberterrorism and deconstruct it by looking at it "as a concept and a word" (Wæver 1995, 47). However, Securitization Theory can only answer the question of how cyberterrorism became securitized and not by whom and what the interest(s) of actors are in doing so.

Therefore, this research will make use of International Political Sociology as developed by Bigo. According to Bigo, "from an International Political Sociology point of view, concepts are significant only in relation to certain localised contexts (spatially and temporally) and if they are understood as emerging in relation to specific practices, which themselves are moulded by power and politics" (2012, 122). Bigo therefore starts his research of (in)security by looking at the practices of actors and how they perceive their actions. Bigo goes beyond researching what security means as a concept, as Securitization Theory does, to researching what security does (2012, 124). The main question underlying Bigo's research is thus: "who is performing an (in)securitization move or countermove, under what conditions, towards whom, and with what consequences?" (Bigo and Tsoukala 2008, 5).

For Bigo, naming what security is, is not determined by a dominant actor, but rather the result of bureaucratic competition within the field of the management of 'unease' (Bigo and Tsoukala 2008, 5). These actors have different forms of capital and legitimacy as well as different interests in defining what security is (Bigo and Tsoukala 2008, 4-5). International Political Sociology goes beyond the use of speech acts to determine what security is, as Securitization Theory does, to research routines, everyday politics of bureaucratic officials, and the accepting audience. Bigo argues that "security should therefore be analysed as a process of (in)securitization by which some practices are subsumed by actors under a claim that they provide security in order to generate acceptance for their activities; even if it implies use of (physical and symbolic) violence. The process is driven by the permanent struggles among the actors concerning these claims, the refusal to accept them, and the competitions

they engage in to determine in their own social universes what is security, what is insecurity and what is fate" (Bigo 2012, 124).

The bureaucratic competition between actors involved in the discourse of cyberterrorism takes place within the field of the management of 'unease'. For the concepts of 'habitus' and 'field' Bigo draws upon Pierre Bourdieu. Habitus refers to "the framework of orientation, provided for both by formal and informal social structures, within which actors are emplaced in society" (Peoples and Vaughan-Williams 2010, 69). The field is then "the social universe within which actors relate to each other and those structures: a complex web of relations between different positions determined by inequalities such as power and wealth" (Peoples and Vaughan-Williams 2010, 69). Thus the habitus of those actors that are involved in the discourse of cyberterrorism determines their framework of orientation, while in the field they compete with other actors over the definition of cyberterrorism. There are certain concepts which differ among others in the discourse of cyberterrorism, which might be decisive in their ability to convince in the discourse. These concepts are (technological) capital, legitimacy, and authority.

The notion of capital is derived from Pierre Bourdieu. According to Bourdieu, capital is "accumulated labour (in its materialised form or its 'incorporated', embodied form) which, when appropriated on a private, i.e. exclusive, basis by agents or groups of agents, enables them to appropriate social energy in the form of reified or living labour" (2011, 81). Because cyberterrorism and cybersecurity has the addition of a cyber-component, this research will look at the concept technological capital as a specific form of capital that public and private actors possess. Technological capital is defined as "the portfolio of scientific resources (research potential) or technical resources (procedures, aptitudes, routines and unique and coherent know-how, capable of reducing expenditure in labour or capital or increasing its yield) that can be deployed in the design and manufacture of products" (Bourdieu 2005, 194). Bonelli has added to this definition of (technological) capital a set of beliefs that an actor possesses about the subject of the discourse, in this case cyberterrorism (Bonelli 2008, 107).

Legitimacy is understood as the acceptance by a population of an authority, for example, the government or private actors. The actors that are involved in the discourse of cyberterrorism struggle for legitimacy for their countermeasure practices by naming cyberterrorism a security threat (Bigo 2012, 126). The academic debate laid out in the literature review exemplifies this ambiguity by disagreeing about whether cyberterrorism is a genuine security threat. This ambiguity is created by the disagreement on which practices fall

under the concept of cyberterrorism and counter cyberterrorism. These practices then are determined by "the identity of the actors practising them" (Bigo 2012, 126).

Besides legitimacy, actors involved in the discourse of cyberterrorism also need the authority to determine the discourse. Authority is the power that an actor has to implement laws and measures or to perform certain practices. The professionals of the management of 'unease' argue that they have the authority to determine the discourse of cyberterrorism "through the authority of the statistics" (Bigo 2008, 12). This authority of statistics is based on the technological capital they possess and their access to relevant databases. According to Bigo, this has allowed these professionals "to establish a field of security in which they recognize themselves as mutually competent, while finding themselves in competition with each other for the monopoly of the legitimate knowledge on what constitutes a legitimate unease, a 'real' risk" (Bigo 2008, 12).

All the above concepts come together in the dispositif of the field of the management of 'unease'. This dispositif consists of "a) discourses; b) specific architectural facilities; c) regulatory decisions; d) administrative measures; and e) scientific discourses" (Bigo 2008, 37). The discourse is determined by public as well as private actors that deal with cyberterrorism, while the scientific discourse is determined by those scholars who research cyberterrorism. The specific architectural facilities are composed of the systems and technological capital public and private actors possess and/or have access to. The regulatory decisions and administrative measures are the practices that these actors have implemented as a result of framing cyberterrorism as a genuine security threat.

As mentioned earlier, one of the reasons for conducting this research is assessing whether the possible threat of cyberterrorism justifies the current measures to counter cyberterrorism in the Netherlands. Peoples and Vaughan-Williams have argued that the practices of the actors involved in the field of the management of 'unease' or the field of cyberterrorism "have led to liberal regimes creating an atmosphere that both justifies and necessitates further illiberal practices" (Peoples and Vaughan-Williams 2010, 69). Do exceptional times call for exceptional measures? Or do exceptional measures call for the framing of exceptional times?

Hypothesis

The hypothesis that follows from the research question and the theoretical framework is:
The own interests of actors with technological capital, legitimacy and authority have resulted in the framing of cyberterrorism as a genuine security threat.

Object of Study

The field of the management of 'unease' in the Netherlands is composed of several government agencies, such as the NCTV, the General and Military Intelligence and Security Agencies, the High Tech Crime Unit of the police, multiple private companies, such as Fox IT, and several scholars that study cyberterrorism.

According to the National Cyber Security Strategy (NCSS) increased cooperation between actors involved with cybersecurity is necessary. Government agencies, private companies and research institutes, need to work together to fully understand cyberattacks (NCTV 2011, 3). Public-private partnerships are equal partners in the cooperation to ensure the continuity and security of supply of safe IT infrastructure and services (NCTV 2011, 4). When these actors work together in countering cyberterrorism, they are also the ones with the possible legitimacy and authority to determine the discourse of cyberterrorism, and thus possibly also the ones who frame cyberterrorism as a genuine security threat. According to the survey done by the Committee of Experts on Terrorism (CODEXTER), "the National Coordinator for Counterterrorism coordinates the approach to combating the use of the Internet for terrorist purposes, together with the national prosecutor's office, the police and intelligence agencies" (CODEXTER 2007, 1).

This research will look at the bureaucratic competition within the field of management of 'unease' and argue which actor(s) was/were able to be the most convincing in the discourse of cyberterrorism and which measures were implemented as a consequence, thus studying the dispositif of cyberterrorism. This research will also look at whether scholars have had any influence on the discourse of cyberterrorism.

Methods of Data Generation and Analysis

Data generation

The main method of data generation was conducting semi-structured elite interviews and gathering primary government documents. According to Manheim et al. "people are referred to as elite if they have knowledge that, for the purpose of a given research project, require that they be given individualised treatment in an interview" (2012, 301). The advantage of elite interviewing is that it can tell "how certain individuals or types of individuals think and act" (Manheim et al. 2012, 301). Because this research revolves around the discourse of cyberterrorism, elite interviewing is a good fit for data generation. The interviews were mainly guided by questions, but the interviewee also had the ability to speak freely if they had relevant information for my research, which might not have been received if the interview was strictly guided by questions alone. The primary documents were needed because, unfortunately, I was not able to talk to some important public actors, such as the NCSC, the NCTV, the High Tech Crime Unit, and the AIVD.

Sources

Interviews were conducted with people from the public actors that deal with cyberterrorism and are engaged in the discourse of cyberterrorism, specifically someone from the Ministry of Defence, and Wouter Jurgens from the organisation of the Global Conference on CyberSpace 2015 from the Ministry of Foreign Affairs. Interviews with private security companies that take part in the discourse of cyberterrorism and in providing cybersecurity systems and advice, such as Eric Luiijf from TNO, Ronald Prins from Fox-IT, and Liesbeth Holterman from Nederland ICT were also conducted. Furthermore, to provide a more critical view on the subject, interviews were conducted with private companies that deal with security and civil liberties on the internet, such as Ton Siedsma from Bits of Freedom. Lastly, interviews were conducted with academic personnel. Specifically, Paul Ducheine from the University of Amsterdam and the Dutch Defence Academy, and Constant Hijzen, PHD student at the Centre for Terrorism and Counterterrorism at Leiden University.

All requests for interviews were done at the end of April and the beginning of May. The interviews were conducted from the end of April to the beginning of June. The planning of the interviews is summarised in the table below.

List of interviews

The list of questions that was used for the interviews is added in Appendix A. Almost all interviews were recorded in Dutch and the translated transcripts are added in appendix B. The interview with the Ministry of Defence was not recorded and the person wishes to remain anonymous.

Table 1: List of interviews

Name & organisation	**Time and date**
Paul Ducheine, professor Cyber Warfare	Tuesday 21 April 15.00 in Amsterdam
Liesbeth Holterman, Nederland ICT	Wednesday 22 April 15.45 in the Hague
Ton Siedsma, Bits of Freedom	Tuesday 28 April 11.00 in Amsterdam
Ronald Prins, Fox-IT	Friday 8 May 11.30 in Delft
Eric Luiijf, TNO	Wednesday 13 May 11.00 in The Hague
Ministry of Defense	Friday 29 May 9.30 in The Hague
Constant Hijzen, PhD student	Monday 1 June 10.00 in The Hague
Wouter Jurgens, Ministry of Foreign Affairs	Tuesday 2 June 15.00 in The Hague

Data analysis

The analysis of the received data was done through sociological discourse analysis. International Political Sociology focuses on the field that defines a particular issue, in this research cyberterrorism. Sociological discourse analysis has helped to lay out the field that makes up the discourse of cyberterrorism and define the actors in it and what their interests are in framing cyberterrorism as a threat to the Netherlands. Furthermore, this field can influence the actors because of their position in it or their position in their respective organisation/institution. As also Ruiz argues about discourse analysis, "meaning [attached by actors to their actions] is not only a product of individual constraints and beliefs. Instead, the meanings that guide individual actions are, to a large degree, socially produced and shared patterns" (2009, 2). Thus the field in which actors are emplaced in society largely determines their action(s) and the meaning(s) they attached to these action(s).

Regular discourse analysis consists of two levels of analysis; textual and contextual. Textual analysis focuses on the discourse as an object of study, contextual analysis focuses on understanding the discourse by researching the enunciation, thus seeing the discourse as an event (Ruiz 2009, 3). Sociological discourse analysis adds a third level of analysis; the interpretive level. Interpretive analysis "provides an explanation of the discourse as it addresses sociological aspects and considers discourse as information, ideology or a social product" (Ruiz 2009, 3).

This interpretive level allows researchers to analyse the discourse and make connections between the discourse and the social order in which the discourse is uttered (Ruiz 2009, 10). Thus, for the purpose of this research, I will analyse the discourse of cyberterrorism while also researching the social order in which the actors involved in the discourse are members of, namely the field of cyberterrorism, as well as researching their practices.

To be able to research the discourse of cyberterrorism, first a clear definition of discourse must be provided. Ruiz has done so and argues that "discourse is defined as any practice by which individuals imbue reality with meaning" (2009, 2). Sociologists specifically focus on the verbal form, expressed in writing or speech, mainly because it is fairly easy to access and examine, and often a certain authority is exercised by the person expressing the discourse (Ruiz 2009, 2). The discourse of cyberterrorism, for the purpose of this research, was thus examined through the statements and practices of those actors that possibly have the legitimacy and authority to determine that cyberterrorism is a genuine security threat.

Scope & Limitations

The results of this research might be applicable to other cases in which the country concerned is also a liberal regime, like the Netherlands. In many other countries, such as the US and UK, cyberterrorism has been claimed as a genuine security threat by the actors involved in the discourse. Similar research can thus be done in these countries to determine whether the interest of the same type of actors have resulted in the framing of cyberterrorism as a genuine security threat.

However, limitations also exist in this research because it is only composed of one case and the results may depend on the people I was able to interview. Therefore, generalizability and reproduction may not be possible.

This research focuses on the discourse and scientific discourse of cyberterrorism and in a limited way on the specific architectural facilities actors in these discourses possess. Further research needs to be done on more architectural facilities, regulatory decisions and administrative measures in order to determine the dispositif of cyberterrorism in the Netherlands.

Chapter 2: Danger in Cyberspace: The Field of Cyberterrorism

Cyberspace in the Netherlands has been securitised as a location of danger and a location for legitimate security practices, by naming cyberterrorism as a genuine security threat. However, until now cyberterrorism has not taken place in the Netherlands. In order to find an answer to the question of by whom has "a threat that has little or no relation to real-world occurrences been included on the security political agenda?" (Dunn Cavelty 2008, 20), this chapter goes in depth into the field of cyberterrorism in the Netherlands. This field consists of several public as well as private actors. These government and private actors deal with and counter (the threat of) cyberterrorism in the Netherlands, whether that is on a technological level or on a policy level. This chapter provides the contextual analysis of the discourse of cyberterrorism in the Netherlands, i.e. detailing by which actors the field of cyberterrorism in the Netherlands is composed.

Field of Cyberterrorism in the Netherlands

The field is "the social universe within which actors relate to each other and the formal and informal social structures: a complex web of relations between different positions determined by inequalities such as power and wealth" (Peoples and Vaughan-Williams 2010, 69). How did the field of cyberterrorism originate in the Netherlands and how is it composed nowadays?

History of the field

The field of cyberterrorism in the Netherlands came into existence in the 1990s/2000s. According to Eric Luiijf, the first time the media spoke about cyberterrorism was, approximately, in 1995. However, the media usually do not know what they are actually talking about. Using the right definitions is a big challenge for them. Cyberterrorism is a popular term to use because it is a catchy title, and it has a 'special' annotation for people.[1] Both because of the word 'terrorism' that usually already frightens people, as well as of the addition of the word 'cyber'. Cyber is for many people a difficult concept to understand. They usually do not know what it exactly encompasses, and they underestimate the scale of cyberspace.

[1] Eric Luiijf, interview, 13 May 2015, The Hague.

The moment cyber and cybersecurity gained a lot of attention within the government was after the DigiNotar hack in 2011, according to Wouter Jurgens.[2] This was the moment that they began taking cybersecurity threats more seriously than they did before this hack, because it had never happened on such a scale in the Netherlands. Although it was not a cyberterrorist attack, it did show how vulnerable Dutch cyberspace was. It brought about a discussion in the Netherlands concerning the protection of cyberspace and the defence against cybersecurity threats. As a result, "a lot of measures were implemented, capabilities were increased, and the National Cyber Security Centre (NCSC) was established".[3] From this moment on, the realisation came that our vulnerability in cyberspace is growing "because we are increasingly digitalising and because more and more of our daily life is going online, for example our identity, our health care etcetera".[4]

The private sector has been concerned about cybersecurity and cybersecurity threats much earlier than the government.[5] Since the turn of the century they have been thinking about what it means to be secure in cyberspace. However, vulnerability is still high within a lot of companies, especially the smaller ones who have little budget for cybersecurity.[6]

Currently, one of the most pressing concerns within the discourse of cyberterrorism is the 'Internet of Things'. This term was first coined by Kevin Ashton in 1999 (Ashton 2009). The 'Internet of Things' is the situation in which devices are run by computers and/or cyberspace rather than by human control. It allows for devices to communicate with each other, without human interfering, through embedded systems. Examples of these devices include heart monitoring implants, automobiles that will be able to drive themselves, and smart meters that can read the use of gas and current automatically through Wi-Fi. All of these devices have the promise of making daily life easier. However, if terrorists or others with malicious intentions are able to disturb or shut down these systems, it can have severe and possible deathly consequences. This makes the need for more cybersecurity vital within the discourse of cyberterrorism. However, as Ronald Prins argues, the wish of the Dutch government to be the most digital country in the world in 2018, contradicts with the wish to

[2] Wouter Jurgens, interview, 2 June 2015, The Hague
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Liesbeth Holterman, interview, 22 April 2015, The Hague.
Ronald Prins, interview, 8 May 2015, Delft.
Constant Hijzen, interview, 1 June 2015, The Hague.
Wouter Jurgens, interview, 2 June 2015, The Hague.

be the most cyber securitised country in the world in 2017.[7] To have both is essentially not possible: "the safest cybersecurity country is not digitalised".[8]

Actors

The field of cyberterrorism in the Netherlands consists of public as well as private actors. The following section outlines the public and private actors who have said something about cyberterrorism and/or deal with (the threat of) cyberterrorism and counter cyberterrorism. Public actors are several ministries and associated organisations. Private actors are private security companies, civil rights foundations, companies in the vital infrastructure, think tanks, academia, and Nederland ICT. There is a realisation that the private and public sector should work together in order to make the Netherlands secure in cyberspace.[9][10] Most of the public and private actors are represented in a public-private partnership that frequently consults with each other; the Cyber Security Council.

There is a wide variety of actors who have said something about cyberterrorism. These actors can be divided along the line of public or private actors. Especially the variety of actors within the private sector is widespread. There are actors who deal with the technological aspect of cyberterrorism, meaning the development of systems that can detect, monitor, fight off, and possibly prevent a cyberterrorist attack. The private security company that is the strongest advocate of securing ourselves against cybercrime in general, and cyberterrorism specifically, is Fox-IT. Fox-It has as a goal to develop technical and innovative solutions that make society safer and focuses on cybersecurity (Fox-IT 2015).

More than 550 ICT companies are united in the trade organisation Nederland ICT. They have one specific advisory group about cybersecurity, in which some of the biggest companies in the Netherlands are represented. This advisory group signals developments within the field of cybersecurity and advises the board of Nederland ICT about points of view and activities, and also gives advice on the representation within the Cyber Security Council.[11] Some of the companies in this advisory group are Google Netherlands, CGI Netherlands, KPN IT Solutions, Microsoft, and UPC (Nederland ICT 2015).

Vital (ICT) infrastructure companies are slowly realising that they also need to think about cybercrime in general, and cyberterrorism specifically, as several of my interviewees

[7] Ronald Prins, interview, 8 May 2015, Delft.
[8] Ibid.
[9] Liesbeth Holterman, interview, 22 April 2015, The Hague.
[10] Wouter Jurgens, interview, 2 June 2015, The Hague.
[11] Liesbeth Holterman, interview, 22 April 2015, The Hague.

have argued.[12] However, there is not a lot of information to be found publicly in which these companies themselves state that cybercrime is one of their priorities. That the vital infrastructure sector is thinking about these kind of threats is mainly evident from my interviews. For example, Paul Ducheine argued that "a company such as Tennet, who suffered from a power-out recently, no doubt thinks about the digital disturbance of their systems or supply of power".[13] Liesbeth Holterman also argued that "a lot of members of Nederland ICT see cyberterrorism as a threat and they are working on protecting and further securing their systems that have been attacked by cybercriminals/cyberterrorists. That are banks, vital infrastructure etcetera".[14]

Eric Luiijf argued that because we in the Netherlands are very dependent on a very large I(C)T infrastructure, we are a very interesting target for terrorists. There is a risk of solely focusing on the internet as a possible target. It is important, however, to take into account that the internet is only a small part of cyberspace, "about 95% of ICT in the Netherlands is not connected to the internet".[15] It is very important for companies in the vital infrastructure sector, such as Tennet and the Nederlandse Aardolie Maatschappij BV (NAM), to realise that although they might not have connected their (transport) systems to the internet, they can still be a target for cyberterrorists. For example, if the power supply, delivered by Tennet, is shut down by a cyberterrorist attack it can have the effect of creating fear or anxiety within the population. According to Constant Hijzen it might even go further, "maybe it is creating deaths/wounded by shutting down vital infrastructure in traffic or public transport".[16] Lastly, Wouter Jurgens argued that "the technical community, the people who control the infrastructure of the internet itself, are closely involved [in the discourse]. Not only nationally, but also with their international network".[17]

There are also non-profit private actors that are in the discourse of cyberterrorism. For example, think tanks are non-profit organisations that do research and are involved in advocating a certain subject. Think tanks that have written about cybersecurity, and cyberterrorism in particular, are the Hague Security Delta, the International Centre for Counter-Terrorism (ICCT), Clingendael, and TNO. Eric Luiijf from TNO, for example, wrote

[12] Paul Ducheine, interview, 21 April 2015, Amsterdam.
Liesbeth Holterman, interview, 22 April, The Hague.
Eric Luiijf, interview, 13 May 2015, The Hague.
Constant Hijzen, interview, 1 June 2015, The Hague.
[13] Paul Ducheine, interview, 21 April 2015, Amsterdam.
[14] Liesbeth Holterman, interview, 22 April 2015, The Hague.
[15] Eric Luiijf, interview, 13 May 2015, The Hague.
[16] Constant Hijzen, interview, 1 June 2015, The Hague.
[17] Wouter Jurgens, interview, 2 June 2015, The Hague.

the chapter "Definitions of Cyber Terrorism" in the book *Cyber Crime and Cyber Terrorism Investigator's Handbook* (Luiijf 2014). This article describes various definitions of cyberterrorism and what is missing in these definitions. At the end, he develops his own definition of cyberterrorism, based on the definition of terrorism the AIVD uses. The research done by the Hague Security Delta on the field of cybersecurity is very significant, because they are the think tank that is mostly involved in this field. In January 2015, they even started a master's programme about cybersecurity in order to enhance the research and thought about the subject.

Next to think tanks there are also a few academics that research the subject of cyberterrorism, or cyberspace, cybercrime, and intelligence agencies in general. Paul Ducheine is a professor Cyber Warfare at the Netherlands Defence Academy and Supernumerary professor Military Law of Cyber Operations & Cyber Security at the University of Amsterdam. Furthermore, some researchers at the Faculty Campus the Hague, such as Sergei Boeke and Constant Hijzen are interested in the subject of cybersecurity/cyberterrorism.

Lastly, civil rights foundations such as Bits of Freedom and Buro Jansen & Janssen focus on the implemented measures and activities that public actors undertake to counter the (potential) threat of cyberterrorism specifically, and cybercrime in general. Usually they are critical in their evaluation of these measures and activities. They are very much needed in civil society, because they are "an addition to the more formal supervisory structure".[18] Furthermore, these foundations can have a broader reach into society than public actors have. This can create the situation in which these foundations are better able to convince in a discourse than public actors. Whether this is the case in the discourse of cyberterrorism will be laid out in the following chapters.

The public actors that deal with cyberterrorism, and cybercrime in general, are four ministries, and affiliated organisations. These ministries are the Ministry of Defence, Security and Justice, Foreign Affairs, Economic Affairs.[19] Organisations that are run from within these ministries that deal with cyberterrorism are the High Tech Crime Unit of the police, the AIVD, the NCSC and NCTV, the Defence Cyber Command, and possibly the MIVD.[20]

[18] Constant Hijzen, interview, 1 June 2015, The Hague.
[19] Wouter Jurgens, interview, 2 June 2015, The Hague.
[20] Paul Ducheine, interview, 21 April 2015, Amsterdam.
Liesbeth Holterman, interview, 22 April 2015, The Hague.
Ton Siedsma, interview, 28 April 2015, Amsterdam.
Eric Luiijf, interview, 13 May 2015, The Hague.
Ministry of Defence, interview, 29 May 2015, The Hague.

The final actor that deals with cyberterrorism specifically, and cybercrime/cybersecurity in general, is the Cyber Security Council.[21] The Cyber Security Council is a national and strategic advisory organ, and a public-private partnership in which "strategic problems in the cyber domain are approached from a multidisciplinary angle" (Cyber Security Council 2015a). The Cyber Security Council is, arguably, one of the most important actors in the field of cybersecurity because it is the only organ that brings together public as well as private actors that face cybersecurity threats such as cyberterrorism. It not only advises the government, but also private actors on cybersecurity. It also advises on the National Cyber Security Strategy, does research on cybersecurity, and is able to deploy members during cybersecurity crises or incidents (Cyber Security Council 2015a). An overview of the actors in the field of cyberterrorism in the Netherlands is displayed in table 2.

Table 2: Field of cyberterrorism in the Netherlands

Public actors	**Private actors**	**Public-private partnership**
Ministry of Security and Justice	Fox-IT	Cyber Security Council
Ministry of Foreign Affairs	Bits of Freedom	
Ministry of Defence	Buro Jansen & Janssen	
Ministry of Economic Affairs	Vital infrastructure	
Police: High Tech Crime Unit	Nederland ICT	
AIVD	Academia	
MIVD	Think tanks	
NCSC		
NCTV		
Defence Cyber Command		

Constant Hijzen, interview, 1 June 2015, The Hague.
Wouter Jurgens, interview, 2 June 2015, The Hague.
[21] Liesbeth Holterman, interview, 22 April 2015, The Hague.

Chapter 3: Framing Cyberterrorism

This chapter provides the textual analysis of the discourse of cyberterrorism in the Netherlands, i.e. researching what the actors involved in this discourse have said about cyberterrorism and determining their positions on the topic. The analysis is done on two different types of discourse: a textual discourse derived from mainly primary documents; and a verbal discourse transcribed into a textual discourse, i.e. the interviews (Ruiz 2009, 4). The actors in the field of cyberterrorism in the Netherlands can be distinguished into three positions. This chapter lays out these three positions on the basis of whether they argue that cyberterrorism is a threat or not; now or in the future. Furthermore, there are slight differences in the definitions of cyberterrorism they use.

These positions can be distinguished on the basis of whether they are a public or private actor, or a public-private partnership, and whether they argue that cyberterrorism is a genuine security threat now or in the future or not at all. First, there is one private actor that argues that cyberterrorism is a threat right now, namely Fox-It. Second, there are many actors that argue that there is potential for cyberterrorism to become a threat in the future. These are mainly the public actors, most private actors, and the public-private partnership: the Cyber Security Council. Third and lastly, there is one public actor that argues that cyberterrorism is not a threat, namely the Ministry of Defence and MIVD. This mapping has been done through discourse analysis of the discursive structure of the field of cyberterrorism in the Netherlands.

Positions in the Field of Cyberterrorism in the Netherlands

There are three types of positions in the field to be distinguished. These types can be distinguished on the basis of whether they are a public or private actor and whether they argue that cyberterrorism is a genuine security threat now, or in the future. First, there are two public actors that argues that cyberterrorism is not a genuine security threat, namely the Ministry of Defence and the MIVD. Second, one private actor, namely Fox-IT, argues that cyberterrorism is a genuine security threat now. Third and lastly, there are public as well as private actors that argue that there is potential for cyberterrorism in the future. Essentially there are thus two different types of actors that argue that cyberterrorism is a genuine security threat now or in the future.

Cyberterrorism is not a threat

This first position is characterised by two actors, namely the Ministry of Defence and the MIVD. They view cyberterrorism as "the terrorist use of cyberspace as an extension for actions with a terrorist aim or goal. With terrorists we mean groups and affiliated individuals who act with terrorist means"[22]. These two actors do not think that cyberterrorism is a threat at the moment: "the Dutch Ministry of Defence usually does not mention the term cyberterrorism, and thus does not think that cyberterrorism is an existential threat at the moment"[23]. The main reason that is given for not naming the term cyberterrorism is because "naming cyberterrorism as a threat would mean giving exposure to […] terrorist organisations"[24]. So, it seems that although they do not use the term cyberterrorism per se, they have put thought into what it would mean or entail if they did use the term. For them, the advantages (possible increase of capabilities, money, research, more clarity about the different forms of cybercrime) of using the term do not outweigh the disadvantages (extra exposure for terrorists, enlarging the Netherlands as a target for terrorists, further radicalisation of people).

The website of the Ministry of Defence only mentions the relation between cyber and terrorism in the following manner: "threats from cyberspace can come from other states, but also from so-called non-state actors such as terrorist and religious groups and commercial parties. Threats may entail: attacks on systems; and espionage" (Ministry of Defence 2015a). However, the term cyberterrorism as a threat is not mentioned.

The capabilities of the Defence Intelligence and Security Service (MIVD) will be increased in the coming years for covertly gathering information from the cyber domain (Ministry of Defence 2015b). Threats in the cyber domain can come from "both within the organisation's own systems (weak spots and 'back doors') and from external parties" (Ministry of Defence 2015c). However, it is not entirely clear which threats in the cyber domain the Ministry of Defence and the Defence industry are facing, are a priority within the whole Ministry of Defence.

What defines this position is thus a tendency to not overstate cyberterrorism as a problem/threat while it has not even happened yet[25]. The Ministry of Defence and the MIVD, at the moment, do not see the urgency to name cyberterrorism as a threat to the Netherlands, now or in the future. Although there have been signals that people are specialising in

[22] Ministry of Defence, interview, 29 May 2015, The Hague.
[23] Ibid.
[24] Ibid.
[25] Ibid.

cyberspace, which terrorist aim/goals can be reached through cyberspace, and that terrorists are taking lessons in hacking.

Cyberterrorism is a threat right now

The second position in the field of cyberterrorism is characterised by one private actor. Ronald Prins from Fox-IT views cyberterrorism as "when terrorists meet their goal of bloodshed and the creation of fear through the manipulation of digital systems. The effect must be that a lot of people notice it, for example when people cannot access their money at banks, or it must have an effect in the physical world, such as disrupting the train systems. Cyberterrorism is not when terrorists use the internet for their media campaign".[26] Although we have not seen anything that resembles cyberterrorism, he has been saying for over five years that "there is a lot of potential for terrorists to use the internet to reach their goals/aims", and we should worry about cyberterrorism right now.[27]

The main problem in cyberspace is that there are too many vulnerabilities. Terrorists can take advantage of that, because they are able to gain the knowledge very soon or even already have the knowledge that is necessary to carry out a cyberterrorist attack.[28] The digitalisation of our society, mainly through the 'Internet of Things', is increasing continuously. For example, "where there used to be physical cables tied to each other, there is now a Windows computer that controls everything".[29] Innovation can be very useful in daily life. However, most people do not realise what kind of effects and consequences their digital products have on them, and how these products can be manipulated by terrorists when they want to reach their aims/goals.

Ronald Prins argues: no one else is saying that cyberterrorism is a threat right now: "the tendency is: as long as it has not happened, it is not really there".[30] The focus, especially within the government, is on other cyber related crime, such as cyber espionage, and possibly cyberwar. From this point of view, it is understandable that there is not many attention given to cyberterrorism, especially because it has not happened yet. Furthermore, if the government, and private actors as well, take defensive measures it does not really have to matter at which cyber threat specifically they are aimed at, because cybersecurity needs to be taken care of anyway.

[26] Ronald Prins, interview, 8 May 2015, Delft.
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] Ibid.

It is not a matter of 'if' they will do it, but rather 'when' they will do it: "I believe that something serious is going to happen in the future. The hacking of TV5 Monde in France was a small example of terrorists that hack".[31] The main reason why this attack cannot be qualified as a cyberterrorist attack is that the effect on society was not tremendous. Instead of creating fear amongst the population, which is arguably the greatest when there is ignorance about what is going on, it soon became clear who the perpetrators were. Although the problem was not solved within minutes, the population early on realised what the problem entailed, and was therefore less worried and afraid of what was going on and might happen in the following hours.

This hack does show that terrorists are able to hack into television stations. It is now, arguably, only a matter of time until they attack another target that could have much more devastating effects when it is shut down. For example a power plant, the Amsterdam Internet Exchange or banks. Cyberterrorism has a lot of advantages for terrorists because they already have the knowledge, it is a lot safer for their own lives than attacks in the physical world, it is a lot less expensive, and there are favourable scale advantages.[32]

What defines this position is the urgency to think about cyberterrorism being an immediate threat. It might not have happened yet, but terrorists have the necessary skills and capabilities to carry out a cyberterrorist attack. We should not underestimate what they are capable of, and we should not wait patiently until something cyberterror related does happen.

Ronald Prins has stated that he does hear many actors saying that although cyberterrorism has not happened, they do realise that terrorists will resort to cyberterrorism in the future.[33] Exactly these actors make up the last position in the field of cyberterrorism.

Cyberterrorism has the potential to become a threat in the future

This third position encompasses the largest group of actors and is composed of several public actors, most private actors, as well as the public-private partnership from within the discourse of cyberterrorism. This section makes a distinction between these three groups.

Public actors

First of all, there are the public actors. These public actors are the four ministries, the NCSC, the NCTV, the High Tech Crime Unit of the police, and the AIVD. The AIVD has defined

[31] Ibid.
[32] Ibid.
[33] Ibid.

cyberterrorism as "the digitally sabotaging of vital components in the Dutch society, such as water installations, money flows (banks), and the railways" (AIVD 2015a). According to their yearly report the AIVD has detected the intention for cyberterrorist attacks, and the potential for cyberterrorism is growing, however at the moment there is no concrete cyberterrorist threat against the Netherlands (AIVD 2015b). But since organisations in the West have regularly been the victim of digital attacks, that could be linked to terrorist(s) organisations, the likelihood that cyberterrorism will take place in the future is growing significantly (AIVD 2015b). The AIVD thus acknowledges that there is potential for cyberterrorism. However, they think that terrorists have not yet acquired the knowledge and capabilities to carry out cyberterrorist attacks. At the moment the focus of the AIVD in the cyber domain is therefore centred on other forms of cybercrime, such as espionage and sabotage.

The Ministry of Security and Justice, the NCSC, and the NCTV do not use the term cyberterrorism itself, because the term often denotes exaggeration (NCTV 2010). They prefer to use the term cyberattack in general, even if there is a terrorist attack against the internet itself, or a terrorist attack against vital infrastructure or critical online-services and the internet is used as a mean (NCTV 2010). They thus think that cyberterrorism can take place, even if they are not using the term, because of abuse of the term in the past. In a study from 2010 cyberterrorism, or a cyberattack with or through terrorist means, is not seen as a threat (NCTV 2010). However, a lot has happened since then. According to the National Cyber Security Centre, the greatest threat in the cyber domain now comes from state actors in the form of digital espionage, and criminals, because of cybercrime (NCSC 2014). Currently, they still do not use the term cyberterrorism at the Ministry of Security and Justice. However, in some documents they do identify some possible attacks that can be qualified as cyberterrorism. For example, in the Magazine 'Nationale Veiligheid en Crisisbeheersing (2015) an article about cyberattacks argues that the greatest worry is about the military use of digital means, such as cyberwar or cyberterrorism (NCTV 2015).

For the prosecution of perpetrators are criminalisation of cyber(terrorist)attacks and authorisations for surveillance and detection necessary. According to Paul Ducheine this is "a task for the police, the public prosecutor's office and the High Tech Crime Unit of the police".[34] Currently cyberterrorism is not criminalised, and there is thus a task for the legislators to define cyberterrorism as a criminal act in criminal law. Until then, acts of cyberterrorism are harder to prosecute. Furthermore, "a new law must have detection

[34] Paul Ducheine, interview, 21 April 2015, Amsterdam.

possibilities for the police [..] and the Intelligence and Security Services".[35] Unfortunately there are no documents to be found in which the High Tech Crime Unit of the policy directly states that they view cyberterrorism as a threat. However, their focus is exclusively on the cyber domain, and thus on the threats in this domain. When legislation makes it possible for them do detect, monitor and prepare cases for prosecution, it can be imagined that cyberterrorism is added to their list of threats in the cyber domain. Especially because an actor such as the High Tech Crime Unit has "specific knowledge about perpetrator profiles, attack profiles etcetera. They know what to pay attention to and they also have international networks".[36]

The last two ministries, Economic Affairs and Foreign Affairs, are involved in a slightly different manner than the Ministry of Security and Justice. This is because they are not directly involved in the detection and monitoring of cyberterrorism, and cybercrime in general. However, these two ministries are interested in the subject from different points of view. The Ministry of Foreign Affairs defines cyberterrorism as "the achievement of kinetic effects through cyber. An attack with ICT means. In that way it is similar to 'regular' terrorism. In methodology because the effect of an attack is the same: creating damage or deaths/wounded, as well as because they have the same aim of creating fear/anxiety in society.[37] Although there have been no examples of cyberterrorism yet, "the element 'creating fear' or 'disrupting society' has a lot of potential [to be achieved with cyber as the mean]".[38] Wouter Jurgens makes one very important remark: "the achievement of kinetic effects with the aim of creating fear or disrupting society we have not seen in the way of classical terrorism. What we do see is that state actors undertake actions that have these kinetic effects, but because they are state actors we do not call it terrorism".[39] This remark is highly relevant for this research because it is about the very definition of which actors can carry out terrorist attacks and thus also cyberterrorist attacks. Apparently the Ministry of Foreign Affairs does not think that (cyber)terrorism can be carried out by state actors or state sponsored actors. However, this research uses the following definition of actors that can resort to terrorism: “Political terrorism is the use, or threat of use, of violence by an individual or a group, whether acting for or in opposition to established authority” (Wardlaw 1982, 16). This entails that state actors could carry out cyberterrorist attacks. However, the actions within the cyber

[35] Ibid.
[36] Wouter Jurgens, interview, 2 June 2015, The Hague.
[37] Ibid.
[38] Ibid.
[39] Ibid.

domain of such actors are usually slightly different from terrorist actions: political pressure, intimidation, and destabilisation, for example, are used.[40] Therefore the Ministry of Foreign Affairs does not see cyberterrorism as a current threat, but it does think that the terrorist (organisations) use of cyber could have kinetic effects as a result: "we do take into account that it could happen, and […] we should not exclude the possibility in the future".[41]

The Ministry of Economic Affairs became involved in this area only very recently and their main point of view is from an economic perspective. For example, when banks are affected by a cyberattack it could have economically destabilising effects in society. Therefore they were present at the Global Conference on Cyberspace.[42]

Public-private partnership

The Cyber Security Council is the public-private partnership in which many public and private actors come together to discuss cybersecurity and threats in the cyber domain. There is a lot of thought put into who must take place within the Cyber Security Council.[43] According to several interviewees, public-private cooperation is very important in the Netherlands in general[44], but especially in this field: "in the basis, especially in the Netherlands, but also in Europe, we realise that this is a domain in which cooperation is necessary"[45] and, "it is a totally shared responsibility".[46]

Wouter Jurgens furthermore argues, "from within the private sector it is about their primary work being dependent on ICT and cyber, or if they have obligations to supply products and/or services to consumers, governments or companies that can be disrupted by society. […] The government needs to worry about and has the responsibility to think of what is important to keep going in times of crisis, considering vital infrastructure".[47]

In a magazine published by the Cyber Security Council (2015b), Rob Bertholee (head of the AIVD) argues that they know that terrorist organisations have the capacity to employ the internet. They do not know whether terrorist organisations can carry out a terrorist attack via the internet, but they do not exclude the possibility that it might be possible or can happen (Cyber Security Council 2015b). He furthermore argues that in the Netherlands we generally

[40] Ibid.
[41] Ibid.
[42] Ibid.
[43] Liesbeth Holterman, interview, 22 April 2015, The Hague.
[44] Ministry of Defence, interview, 29 May 2015, The Hague.
[45] Ibid.
[46] Liesbeth Holterman, interview, 22 April 2015, The Hague.
[47] Wouter Jurgens, interview, 2 June 2015, The Hague.

underestimate the risks in the cyber domain; we are too naïve; and we should thus worry about threats in this domain (Cyber Security Council 2015b).

The Cyber Security Council does not have their own statement about cyberterrorism, but it is essentially composed of the actors that take part in the Council. Most of these actors, with the exception of the Ministry of Defence and the MIVD, all think that cyberterrorism is a (possible) threat in the future and that we should start worrying now about how vulnerable we are and secure ourselves against any type of cybercrime, including cyberterrorism.

Private actors

The private actors that argue that cyberterrorism is a (possible) threat in the future are the civil rights foundations (Bits of Freedom and Buro Jansen & Janssen), the vital infrastructure and Nederland ICT.

Members of Nederland ICT, approximately 550 ICT companies, see cyberterrorism as a (potential) threat and "they are working on protecting and further securing their systems that have been attacked by cybercriminals. They are banks, companies from the vital infrastructure sector etcetera".[48] Companies in the vital infrastructure sector should pay attention to cyberterrorism because "if a product or service is being used in vital infrastructure it needs a better protection" than other products.[49] Especially because sometimes it can be a matter of life and death, such as in hospitals or power plants. Ronald Prins therefore argues that there needs to be an analogue back-up or an analogue system in the first place.[50] We should worry about vital infrastructure being attacked because it is a very large sector in the Netherlands and many systems and people depend on it. Vulnerabilities in their systems can therefore have larger effects than in other countries that are less digitalised.

Liesbeth Holterman from Nederland ICT views cyberterrorism essentially the same as terrorism: "many deaths is not necessary per se, but a group needs to have an aim of disrupting the society. The way in which this happens can differ, for example a hack or a DDoS-attack. A state or non-state actor that wishes to disrupt society. […] The main goal needs to be to create fear".[51] She makes an important remark that terrorism can come from state as well as non-state actors, which some other interviewees have not or failed to make. She does believe that cyberterrorism is a threat, but that "terrorists are naïve in thinking that

[48] Liesbeth Holterman, interview, 22 April 2015, The Hague.
[49] Paul Ducheine, interview, 21 April 2015, Amsterdam.
[50] Ronald Prins, interview, 8 May 2015, Delft.
[51] Liesbeth Holterman, interview, 22 April 2015, The Hague.

societal disruption can only be caused by a physical attack or presence".[52] Not enough attention is given to the subject of cyberterrorism, otherwise it would have been seen as a current threat by more people. However, she does argue that "everyone with some sense of the cyber domain sees that there are threats in it. There are, however, differences in how they view these threats as big or not".[53] This is a bold statement, especially because all of my other interviewees, with the exception of Ronald Prins, have argued that cyberterrorism is not a threat, or only one for the future. But even she indicates that terrorists have not come to the realisation that cyberterrorism is possible. So can it then really be a threat right now?

Bits of Freedom argues that they see cyberterrorism "as a digital exponent of 'regular' terrorism. It must have a specific goal, the action must be disruptive. It is not necessarily about the action, but more about the intent of the terrorist (group). It is cyberterrorism when there is a terroristic aim. There are not specific acts that can be qualified as cyberterrorism".[54] Bits of Freedom is the least strongest opponent of this position, but they do not entirely rule out the possibility that cyberterrorism might happen in the future.[55] But for now, "I predict that, without any knowledge of the future of course, it is a hyped problem or an exaggeration to act on the internet, on the part of the government. […] Cyberterrorism is in this way a mean to argue for (more) control over communication methods and such on the internet".[56]

This third and last position can be characterised by those actors that see there is some reason to look at cyberterrorism as a threat, but because in their opinion terrorists have not yet the capabilities, resources and knowledge needed to carry out a cyberterrorist attack, it is not an immediate threat to worry about.

Framing danger in cyberspace as cyberterrorism

Ton Siedsma of Bits of Freedom has made an important remark: is cyberterrorism being hyped or framed as a threat? Constant Hijzen also says: "funding and investments have been enormous for cyber related research and activities. The danger is that people within government who need funding 'frame' their problem as being a cyber-related problem".[57] The literature review shows that there is a large academic debate about whether cyberterrorism is a threat or not. However, this research goes beyond that debate and looks at how cyberterrorism

[52] Ibid.
[53] Ibid.
[54] Ton Siedsma, interview, 28 April 2015, Amsterdam.
[55] Ibid.
[56] Ibid.
[57] Constant Hijzen, interview, 1 June 2015, The Hague.

has been framed, or as Jarvis, Macdonald and Nouri put it: "as a hyperbolic media construction" (2014, 69). Cyberspace inhabits not only good things, but it can also inhabit actors with malicious intentions. The question is whether these actors are or can be terrorists.

Cyberspace is a vulnerable domain. Cybersecurity is probably not at the level where it should be in the Netherlands. Public and private actors can do a lot more to be more secure in cyberspace. But does this lead to terrorists taking advantage of these vulnerabilities? This research argues that the likelihood of this happening is not that great. Terrorists do not have the acquired knowledge and capabilities to carry out a cyberterrorist attack at the moment. The methods they currently use are limited to DDoS-attacks and defacements.[58] These measures are not damaging enough to disrupt society, to create fear or anxiety among the population, or to create deaths or wounded. Furthermore, the cost-benefit analysis is usually not in favour of terrorists. While the costs of the above mentioned cyberattacks may be low, the chances of inflicting the damages that can be done through physical attacks are very slim. Regardless of these facts, this chapter has shown that there are many actors that argue that cyberterrorism is a genuine security threat.

Now the question remains why these actors have framed cyberterrorism as a genuine security threat. Therefore the next chapter goes in depth into the sociological background of the actors involved in the discourse of cyberterrorism and look at their levels of technological capital, legitimacy, and authority.

[58] Ministry of Defence, interview, 29 May 2015, The Hague.

Chapter 4: Sociology of the Actors of Cybersecurity

This chapter analyses the findings of the previous chapter through the interpretive level of sociological discourse analysis. This entails connecting the actors within the three positions with their sociological background, i.e. the levels of technological capital, legitimacy and authority they possess (high, average or low). For Bigo, naming what security is (and thus what a genuine security threat is), is not determined by a dominant actor, but rather the result of bureaucratic competition within the field of the management of 'unease' (Bigo and Tsoukala 2008, 5). These actors have different forms of capital and legitimacy as well as different interests in defining what security is (Bigo and Tsoukala 2008, 4-5).

This research argues that these different levels of technological capital, legitimacy and authority have resulted in different interests as to why actors argue that cyberterrorism is a genuine security threat. Private actors compared to public actors have a combination of interests in arguing that cyberterrorism is a genuine security threat, while public actors have the protection of the Dutch cyberspace and the Dutch society as a primary interest.

Sociological background: technological capital, legitimacy and authority

This research focuses on the concepts of technological capital, legitimacy and authority. These concepts are defined as qualities of the actors involved in the discourse of cyberterrorism. Technological capital is defined as "the portfolio of scientific resources or technical resources that can be deployed in the design and manufacture of products" (Bourdieu 2005, 194). Technological capital matters because, as Paul Ducheine argues: "several actors make a contribution to protect society. Sometimes that are private actors in those places or areas where the government does not have a role or does not have the necessary knowledge".[59] However, "technical capabilities [of public actors] are ahead of the authorisations that government has".[60] This can create problems because the government's level of technological capital is high, while they are not able to use it because legislation is lacking. Eric Luiijf argues that technological capital is also needed in the ICT sector and "means are, in general, not very expensive".[61] While there is agreement amongst the interviewees that technological capital is important for public as well as private actors, there is more disagreement about the concepts legitimacy and authority.

[59] Paul Ducheine, interview, 21 April 2015, Amsterdam.
[60] Paul Ducheine, interview, 21 April 2015, Amsterdam.
[61] Eric Luiijf, interview, 13 May 2015, The Hague.

According to Wouter Jurgens, "these concepts play a role, but [the discourse] is subject to changes".[62] Because cybersecurity is, prominently, a domain in which public-private cooperation is necessary, the discourse changes because (the influence of) the actors in it change. Because public order and security are civil rights, citizens expect the government to take care of them. This essentially gives the government the legitimacy and authority to be influential in the discourse of cyberterrorism. Technological capital and knowledge are, however, mostly concentrated in the private sector.[63]

A higher level of technological capital or more legitimacy does not automatically result in more influence in the discourse: "sometimes it is just coincidence: one headline in the media, one scandal can result in a change in the discourse".[64] Technological capital and knowledge thus do not always decide if an actor has a role in the discourse. Although the levels of legitimacy and authority of private actors could rise "if the problem/issue is materialised by private actors that can actually show what and how a cyberterrorist attack could harm a company and what the consequences would be".[65]

Level of technological capital

Between the interviewees there is some disagreement as to which actors, public or private, have the highest level of technological capital. Ton Siedsma, for example, argues that "the most advanced malware is currently not being used by private companies or terrorists, but by governments themselves. […] The resources and knowledge for developing these systems lay with governments".[66] Ronald Prins, however, argues that "the Intelligence and Security Services have the systems needed to detect a cyberattack. What is missing, however, is the capacity to process all the material, and the material itself […] and resources, money and legislation".[67]

<u>High</u>

The public actors with high technological capital are the AIVD and MIVD, the NCSC, the NCTV, and the High Tech Crime Unit of the police. The private actor with high technological

[62] Wouter Jurgens, interview, 2 June 2015, The Hague.
[63] Ibid.
[64] Constant Hijzen, interview, 1 June 2015, The Hague.
[65] Ibid.
[66] Ton Siedsma, interview, 28 April 2015, Amsterdam.
[67] Ronald Prins, interview, 8 May 2015, Delft.

capital is Fox-IT, because it is the only private cybersecurity company that has enough knowledge and capabilities to determine if cyberterrorism is a threat or not.

Average

There are also actors who have some technological capital, but are not amongst the actors that have many technological capabilities and access to relevant databases. These actors are the Ministry of Defence, the Ministry of Security and Justice, the vital infrastructure sector and Nederland ICT.

Low

"Private actors do not have the knowledge that the AIVD and MIVD have in arguing that there is a threat or not".[68] This is true for most private actors, such as Bits of Freedom, Buro Jansen & Janssen, think tanks and academia. Some public actors also have low technological capital, such as the Ministry of Foreign Affairs and the Ministry of Economic Affairs. This is because they are not technologically involved in the discourse of cyberterrorism. The same is true for the public-private partnership, the Cyber Security Council.

According to Bourdieu, "technological capital is effective only if it is associated with other kinds of capital. This no doubt explains the fact that victorious challengers are very seldom small, emerging firms and, where they are not product from mergers between existing firms, they originate in other nations or, particularly, from other subfields. It most often falls to the large firms to effect revolutions – firms which, by diversifying, can take advantage of their technological competences to present a competitive proposition in new fields. So the changes within a field are often linked to changes in the relations with the exterior of that field" (Bourdieu 2005, 203).

This quote explains nicely why Fox-IT is the only cybersecurity company that has been able to compete successfully in the discourse of cyberterrorism in the Netherlands[69]. It is one of the largest cybersecurity companies in the world, and definitely the largest in the Netherlands. However, Fox-IT must have other qualities that have enabled them to be convincing in the discourse of cyberterrorism. Because many of the actors with a low level of technological capital also argue that cyberterrorism is a threat, thus technological capital alone

[68] Ton Siedsma, interview 28 April 2015, Amsterdam.
[69] Constant Hijzen, interview, 1 June 2015, The Hague.

cannot explain why actors rightfully argue that cyberterrorism is a genuine security threat. Therefore, this research also looks at the concepts legitimacy and authority.

Level of legitimacy

Legitimacy is understood as the acceptance by a population of an authority. According to the Ministry of Defence, "there is little trust in what the government and its representatives have to say: what people with power say, cannot be true, should be doubted and questioned by default. […] Legitimacy and authority are thus not always larger for public actors than private actors".[70] Private actors may sometimes have more legitimacy and authority because they are able to provide examples of what a cyberterrorist attack could look like. Public actors are not likely to publish this information, because it may jeopardise their (international) reputation.

However, this is a very cynical view. In general, public actors have more legitimacy than private actors. Although society is sometimes very critical of public actors, society is usually more inclined to accept the verbal and non-verbal discourse of cyberterrorism uttered by public actors than private actors. This is because society puts more trust into public actors. They are usually more distrustful of private factors because they cannot be hundred per cent sure about what their interests are in the discourse of cyberterrorism. Fox-IT may be an exception because it has such a high level of technological capital that that may also result in a high level of legitimacy.

Level of authority

Authority is the power that an actor has to implement laws and measures or perform certain practices. The Ministry of Defence claims that "it is fundamentally wrong to say, as deconstructivists such as Foucault and Derida do, that there should be no authority and power to 'govern the world'. There should be one or multiple authorities that govern a country in order to avoid chaos and anarchy".[71]

According to Ton Siedsma, (certain) public actors have an advantage in this area: "when the AIVD and/or MIVD say that something is a threat, or that there is a threat somewhere, I would not put that into question. […] I have more trouble being convinced by private actors, because their interests are not always clear and equal as those of the AIVD and MIVD".[72]

[70] Ministry of Defence, interview, 29 May 2015, The Hague.
[71] Ibid.
[72] Ton Siedsma, interview, 28 April 2015, Amsterdam.

In conclusion, it can be said that public actors have more legitimacy and authority than private actors, with the exception of Fox-IT. Constant Hijzen says that he does not think that Fox-IT needs to exaggerate the threat of cyberterrorism to do their work: "there is enough to do already".[73] The levels of legitimacy and authority of Fox-IT are higher, because they do not need to argue that there is another threat in cyberspace, namely cyberterrorism, if they did not think it is a genuine security threat.

The level of technological capital is more difficult to determine. Especially (cyber) security companies, such as Fox-IT, might have more technological capital than certain public actors, such as the Ministry of Economic Affairs, who is not per se technologically involved in the discourse of cyberterrorism. Table 3 provides an overview of the levels of technological capital, legitimacy and authority all the actors have.

[73] Constant Hijzen, interview, 1 June 2015, The Hague.
Ronald Prins, interview, 8 May 2015, Delft.

Table 3: Levels of technological, legitimacy and authority of all actors

	Technological capital	**Legitimacy**	**Authority**
High	Fox-IT AIVD MIVD NCSC NCTV High Tech Crime Unit	Fox-IT AIVD MIVD NCSC NCTV High Tech Crime Unit Ministry of Defence Ministry of Security and Justice	Fox-IT AIVD MIVD NCSC NCTV High Tech Crime Unit Ministry of Defence Ministry of Security and Justice
Average	Ministry of Defence Ministry of Security and Justice Vital infrastructure Nederland ICT	Ministry of Foreign Affairs Ministry of Economic Affairs Cyber Security Council Nederland ICT Vital infrastructure Bits of Freedom Buro Jansen & Janssen	Ministry of Foreign Affairs Ministry of Economic Affairs Cyber Security Council
Low	Ministry of Foreign Affairs Ministry of Economic Affairs Bits of Freedom Buro Jansen & Janssen Cyber Security Council Academia Think tanks	Academia Think tanks	Bits of Freedom Buro Jansen & Janssen Nederland ICT Academia Think tanks Vital infrastructure

Interests

The final question of this research is whether these different levels of technological capital, legitimacy, and authority have resulted in different interests that actors have in arguing that cyberterrorism is a genuine security threat.

On the basis of this research, a distinction can be made as to which interests the actors have in arguing that cyberterrorism is a genuine security threat. First of all, the public actors

take a more ethical point of view in the discourse of cyberterrorism.[74] They have as a primary interest the protection of the Dutch cyberspace and Dutch society.[75] According to the Ministry of Defence, "government institutions will not and cannot overstate the threat since that is governed by laws that require factual statements".[76]

Private actors, on the other hand, have multiple interests in arguing that cyberterrorism is a genuine security threat. These interests are the protection of the Dutch cyberspace and Dutch society, but also consists of a self-interest. For example, because they have an interest in increasing the demand for their own products and services and they want to protect their (international) reputation.[77] Paul Ducheine argues that "most companies have a commercial motivation, but also an interest in keeping the society going and their own services safe, especially if they are companies in the vital infrastructure. They get called upon when their services are not working and held responsible. It is socially undesirable, but also bad for business".[78] They thus have a moral interest in keeping Dutch cyberspace safe, commercial interests, but they also care about their (international) reputation.

Private actors have indeed multiple interests, according to Ton Siedsma: "their intentions are both their worry as well as more commercial interests in saying so, because they can make money from this worry".[79] However, this is a very cynical view. Ronald Prins says that "they who name cyberterrorism as a threat, realise that a cyberterrorist attack could happen. Actors who earn their money in this field already earn enough, they do not need to name cyberterrorism as a threat to survive economically".[80]

Eric Luiijf adds another possible interest that actors may have in arguing that cyberterrorism is a genuine security threat: "they have a self-interest in that they want publicity. They want their name in the media and possibly sell their own products and services".[81] This is also one of the arguments Constant Hijzen gives as to why civil rights foundations are involved in the discourse of cyberterrorism and might argue that it is not a threat or might argue that others are exaggerating the threat. Furthermore, "they need to 'earn'

[74] Ton Siedsma, interview, 28 April 2015, Amsterdam.
[75] Ibid.
Eric Luiijf, interview, 13 May 2015, The Hague.
Wouter Jurgens, interview, 2 June 2015, The Hague.
[76] Ministry of Defence, interview, 29 May 2015, The Hague.
[77] Ibid.
Ronald Prins, interview, 8 May 2015, Delft.
Paul Ducheine, interview, 21 April 2015, Amsterdam.
[78] Paul Ducheine, interview, 21 April 2015, Amsterdam.
[79] Ton Siedsma, interview, 28 April 2015, Amsterdam.
[80] Ronald Prins, interview, 8 May 2015, Delft.
[81] Eric Luiijf, interview, 13 May 2015, The Hague.

their right to existence and therefore might frame certain issues or points of view by using certain terminology. This can influence the discourse heavily".[82]

Public actors' sole interest to argue that cyberterrorism is a genuine security threat is thus their 'civic duty' to provide protection to Dutch citizens in cyberspace, the protection of cyberspace itself, and the protection of the vital interests in the Netherlands. Private actors, however, have a combination of interests to argue that cyberterrorism is a genuine security threat. These interests are the moral interest public actors also have, a commercial interest because they need to make a profit, publicity for other opinions and points of view they have, and they want to maintain and possibly even improve their (international) reputation.

[82] Constant Hijzen, interview, 1 June 2015, The Hague.

Conclusion and Discussion

This section gives an answer to the research question: *How and why has 'cyberspace' been constituted as a source of danger and a location for legitimate security practices in the Netherlands?* as well as an proposed vision for further research. Finally, this thesis will conclude by arguing for the implementation of cybersecurity norms.

Since the 1990s there is an intensive debate about whether cyberterrorism is a genuine security threat or not. Instead of engaging in this particular debate, this research has taken the research a step further by looking at the discourse of cyberterrorism. There is a need for such research because none of the opponents in the original debate have been able to provide an explanation as to why actors argue that cyberterrorism is a genuine security threat, while it is arguably not a threat. This research has contributed in answering this question by researching the discourse of cyberterrorism in the Netherlands in an attempt to find out which interests the actors in this discourse have when they argue that cyberterrorism is a genuine security threat and if their statements are based on their technological capital, legitimacy and authority.

In chapter 3 it became clear that three types of positions in the discourse of cyberterrorism can be distinguished. First, the Ministry of Defence and the MIVD argue that cyberterrorism is not a threat. Second, Fox-IT, a private actor, argues that cyberterrorism is a threat right now. Third and lastly, all other actors involved in the discourse of cyberterrorism argue that it can be a potential threat in the future. Chapter 4 then showed that the levels of technological capital, legitimacy and authority differed among the actors. The actors with high levels on all three concepts are: Fox-IT, the AIVD, the MIVD, the NCSC, the NCTV, the High Tech Crime Unit of the police, the Ministry of Defence, and lastly the Ministry of Security and Justice. In contrast, the actors with average and low levels on the three concepts are: Bits of Freedom, Buro Jansen & Janssen, Nederland ICT, academia, think tanks and companies in the vital infrastructure sector. However, all actors in this second group argue that cyberterrorism is or can be in the future a genuine security threat. The actors within the first group, with the exception of the ministry of Defence and the MIVD, argue the same.

The actors in the first group argue that cyberterrorism is or can be in the future a genuine security threat on the basis of their high levels of technological capital, legitimacy and authority. However, the same cannot be true for the second group because of their average and low levels on these three concepts. This means that there must be another explanation for why these actors argue that cyberterrorism can be a genuine security threat.

On basis of this research, this thesis argues that the actors in the second group have multiple interests compared to the actors in the first group.

The primary interest of the actors within the first group is the protection of the Dutch cyberspace and the Dutch society. The actors in the second group, however, have a combination of interests when they argue that cyberterrorism is a genuine security threat. This combination of interests consist of the protection of the Dutch cyberspace and society as well as the serving of their self-interest in trying to sell their products and services, their search for publicity, and the protection of their (international) reputation.

This research started with an assumption that was formed into the following hypothesis: *The own interests of actors with technological capital, legitimacy and authority have resulted in the framing of cyberterrorism as a genuine security threat.* Through my research I have found support for this hypothesis for the actors that have average and low levels of technological capital, legitimacy and authority but do argue that cyberterrorism is or can be a genuine security threat. These actors do not only have the protection of Dutch cyberspace and the Dutch society as an interests, but they also sometimes need to make a profit, search for publicity for their own cause, and/or want to protect or enhance their (international) reputation. By arguing that there is a danger in cyberspace that comes from terrorists, they have framed cyberterrorism partly on the basis of their self-interest instead of on the basis of their technological capital, legitimacy and authority.

For the actors with high levels of technological capital, legitimacy and authority, I have found no support for the hypothesis through my research. These actors have, on the basis of these high levels, the acquired knowledge, capabilities, legitimacy and authority needed to rightfully argue that cyberterrorism is or can be in the future a genuine security threat. Therefore they have not framed cyberterrorism as a genuine security threat, while this is arguably not the case, but they have the necessary background to argue the reality of cyberterrorism being a (potential) threat.

Cyberspace has thus been constituted as a source of danger and a location for legitimate security practices in the Netherlands. On the one hand, this is rightfully done by those actors with high levels of technological capital, legitimacy and authority. They have argued that cyberterrorism is or can be in the future a genuine security threat because they have the protection of Dutch cyberspace and the Dutch society as their sole interests.

On the other hand, there are actors with average and low levels of technological capital, legitimacy and authority who have framed cyberterrorism as a genuine security threat, while they do not have the necessary background to argue this. They have thus framed

cyberterrorism on the basis of other interests. These interests are sometimes the need to make a profit, the search for publicity for their own cause, and/or they want to protect or enhance their (international) reputation.

Illiberal Practices in the Netherlands?

One of the questions on my mind for further research is: has the framing of cyberterrorism led to illiberal practices in the Netherlands, which is a liberal regime? On the basis of this research I would argue that the Dutch government is not engaging in illiberal practices because it has the necessary background (high levels of technological capital, legitimacy and authority) to argue if cyberterrorism is a (potential) threat or not. Other actors without this necessary background, however, are possibly engaging in illiberal practices by framing cyberterrorism. However, further research on these actors needs to be done to argue if this really is an illiberal practice. Furthermore, there is also a possibility of public actors engaging in illiberal practices if they themselves resort to cyberattacks in general, and cyberterrorist attacks in particular against other states or non-state actors. However, this is another direction in the debate about cyberterrorism.

Discussion: The Need for Cybersecurity Norms

Liesbeth Holterman made an important statement regarding norms in cyberspace and cybersecurity: "what is interesting to look at is the document of Microsoft about cybersecurity norms. Microsoft argues that there need to be norms about behaviour on the internet. Now there are cyberattacks and possible cyberterrorist attacks being done by state actors, while there is no war. What is going to happen when there is war? Norms and values are needed to regulate behaviour in the cyber domain".[83] This is an interesting argument for discussion. If there are norms to guide behaviour in the cyber domain, this could entail that states and affiliated organisations are less likely to resort to cyberattacks in general, and cyberterrorist attacks in particular. If there are norms and rules for the cyber domain, this would mean that they can be held accountable for their actions. Now this is not the case and are states thus 'free' to decide for themselves how they act in the cyber domain. The difficulty of implementing norms and rules is, however, that agreement on which norms and rules is very hard to reach. Moreover, criminals and terrorists are not likely to cohere to such norms.

[83] Liesbeth Holterman, interview, 22 April 2015, The Hague.

References

AIVD. 2015a. "Cyberterrorism." https://www.aivd.nl/onderwerpen/cyberdreiging/cyberterrorisme/ (10 June 2015).

AIVD. 2015b. "Annual Report 2014." https://www.aivd.nl/english/publications-press/@3251/annual-report-2014/ (10 June 2015).

Ashton, Kevin. 2009. "That 'Internet of Things' Thing." *RFID Journal*. http://www.rfidjournal.com/articles/view?4986 (9 June 2015).

Bendrath, Ralf. 2003. "The American Cyber-Angst and the Real World – Any Link?" In *Bombs and Bandwidth: The Emerging Relationship Between Information and Technology and Security*, ed. Robert Latham. London: The New Press, 49 – 73.

Benschop, Albert. "Cyberterrorisme: Dodelijk geweld vanaf het toetsenbord." http://www.sociosite.org/terrorisme.php (8 March 2015).

Betz, David J. and Tim Stevens. 2011. "Chapter Three: Cyberspace and War." *Adelphi Series* 51(424): 75 – 98.

Bigo, Didier. 2008. "Globalized (in)security: the Field and the Ban-opticon." In *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*, eds. Didier Bigo and Anastassia Tsoukala. New York: Routledge, 10 – 48.

Bigo, Didier. 2012. "International Political Sociology." In *Security Studies*, ed. Paul Williams. London: Routledge, 116 – 129.

Bigo, Didier and Anastassia Tsoukala. 2008. "Understanding (in)security." In *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*, eds. Didier Bigo and Anastassia Tsoukala. New York: Routledge, 1 – 9.

Blane, John. V. 2003. "Cybercrime and Cyberterrorism: The Netherlands. In *Cybercrime and Cyberterrorism: Current Issues*. New York: Novinka, 17 – 20.

Bonelli, Laurent. 2008. "Hidden in Plain Sight." In *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*, eds. Didier Bigo and Anastassia Tsoukala. New York: Routledge, 100 – 120.

Bourdieu, Pierre. [2000] 2005. *The Social Structures of the Economy* [Les structures sociales de l'économie]. Trans. Chris Turner. Cambridge: Polity Press.

Bourdieu, Pierre. [1979] 2011. "The Forms of Capital [in French]." In *Cultural Theory: An Anthology*, eds. Imre Szeman and Timothy Kaposy. Oxford: Wiley-Blackwell.

Bouwmeester, Hans and Hans Folmer and Paul Ducheine. 2012. “Cyber Security and Policy Responses.” In *Cyber Warfare: Critical Perspectives,* eds. Paul Ducheine et al. The Hague: T.M.C. Asser Press, 19 – 23.

Brickey, Jonalan. 2012. “Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace.” *CTC Sentinel* 5(8): 4 – 6.

Chen, Thomas M. and Lee Jarvis and Stuart Macdonald. 2014. *Cyberterrorism: Understanding, Assessment, and Response*. New York: Springer.

Collin, Barry. 1997. “The Future of Cyberterrorism: The Physical and Virtual Worlds Converge.” *Crime and Justice International* 13(2): 15 – 18.

Committee of Experts on Terrorism (CODEXTER). 2007. “Cyberterrorism – The Use of the Internet for Terrorist Purposes: Netherlands.” *Council of Europe,* 1 – 3. http://www.coe.int/t/dlapil/codexter/Source/cyberterrorism/Netherlands.pdf (15 March 2015).

Conway, Maura. 2007 “Cyberterrorism: Hype and Reality.” In *Information Warfare: Separating Hype From Reality*, ed. Leigh Armistead. Dulles: Potomac Books, 73 – 93.

Conway, Maura. 2011. “Against Cyberterrorism: Why Cyber-based Terrorist Attacks Are Unlikely to Occur.” *Communications of the ACM* 54(2): 26 – 28.

Cronin, Audrey Kurth. 2003. “Behind the Curve: Globalization and International Terrorism.” *International Security* 27(3): 30 – 58.

Cyber Security Council. 2015a. “Cyber Security Council.” http://www.cybersecurityraad.nl/ (9 June 2015).

Cyber Security Council. 2015b. *CSR Magazine* 1(1).

Denning, Dorothy. 2001. “Is Cyber Terror Next?” Washington DC: Social Science Research Council. http://fas.org/irp/congress/2000_hr/00-05-23denning.htm (10 May 2015).

Denning, Dorothy. 2007. “A View of Cyberterrorism Five Years Later.” In *Internet Security: Hacking, Counterhacking, and Society*, ed. K. Himma. Boston: Jones and Bartlett Publishers, 123 – 139.

Ducheine, Paul and Frans Osinga and Joseph Soeters. 2012. *Cyber Warfare: Critical Perspectives*. The Hague: Asser Press.

Dunn Cavelty, Myriam. 2008. “Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate.” *Journal of Information Technology & Politics* 4(1): 19 – 36.

Fox-IT. 2015. "About us." https://www.fox-it.com/en/about-us/ (11 June 2015).

Furnell, S.M. and M.J. Warren. 1999. “Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?” *Computers and Security* 18: 28 – 34.

Giacomello, Giampiero. 2004. “Banks for the Buck: A Cost-Benefit Analysis of Cyberterrorism.” *Studies in Conflict and Terrorism* 27(5): 387 – 408.

Heickerö, Roland. 2012. *The Dark Sides of the Internet: On Cyber Threats and Information Warfare*. Frankfurt am Main: Peter Lang.

Heickerö, Roland. 2014. “Cyberterrorism: Electronic Jihad.” *Strategic Analysis* 38(4): 554 – 565.

Jarvis, Lee and Stuart Macdonald. 2014. “Locating Cyberterrorism: How Terrorism Researchers Use and View the Cyber Lexicon.” *Perspectives on Terrorism* 8(2): 52 – 65.

Jarvis, Lee and Stuart Macdonald and Lella Nouri. 2014. “The Cyberterrorism Threat: Findings from a Survey of Researchers.” *Studies in Conflict & Terrorism* 37(1): 68 – 90.

Luiijf, Eric. 2014. “Definitions of Cyber Terrorism.” In *Cyber Crime and Cyber Terrorism Investigator’s Handbook*, eds. Babak Akhgar, Andrew Staniforth and Francesca Bosco. Waltham: Elsevier, 11 – 16.

Lourdeau, Keith. 2004. “Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI before the Senate Judiciary Subcommittee on Terrorism, Technology and Homeland Security. Washington DC: Senate. http://www.fbi.gov/news/testimony/hearing-on-cyber-terrorism (10 May 2015).

Manheim, Jarol B., Richard C. Rich, Lars Willnat, Craig Leonard Brians, and James Babb. 2012. *Empirical Political Analysis*. Essex: Pearson.

Ministry of Defence. 2015a. "Threats in the Digital Environment." https://www.defensie.nl/english/topics/cyber-security/contents/threats (10 June 2015).

Ministry of Defence. 2015b. "Defence Cyber Strategy." https://www.defensie.nl/english/topics/cyber-security/contents/defence-cyber-strategy (10 June 2015).

Ministry of Defence. 2015c. "Cyber Command." https://www.defensie.nl/english/topics/cyber-security/contents/cyber-command (10 June 2015).

Minister of Security and Justice. 2013. *Antwoorden Kamervragen over het bericht dat de Verenigde Staten al langer zuchten onder cyberaanvallen.* Den Haag: Ministerie van Veiligheid en Justitie.

MIVD. “Annual Report 2014.” http://www.rijksoverheid.nl/documenten-en-publicaties/jaarverslagen/2015/04/21/jaarverslag-mivd-2014.html (9 June 2015).

National Coordinator for Security and Counterterrorism (NCTV). 2010. *Jihadisten en het Internet*. The Hague: Ministry of Security and Justice (10 June 2015).

National Coordinator for Security and Counterterrorism (NCTV). 2011. *De Nationale Cyber Security Strategie (NCSS): Slagkracht door samenwerking*. The Hague: Ministry of Security and Justice, 1 – 15.

National Coordinator for Security and Counterterrorism (NCTV). 2014. "What is Terrorism?" The Hague: Ministry of Security and Justice. http://english.nctv.nl/themes_en/Counterterrorism/what_is_terrorism/ (10 May 2015).

National Coordinator for Security and Counterterrorism (NCTV). 2015. "Meten is Weten: Cyberaanvallen Geanalyseerd." *Magazine Nationale Veiligheid en Crisisbeheersing* 13(2):

National Cyber Security Centre. 2015. "Cybersecuritybeeld Nederland." https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten/cybersecuritybeeld-nederland-4.html (10 June 2015).

Nederland ICT. 2015. "Cyber Security." http://www.nederlandict.nl/?id=9156 (9 June 2015).

Osinga, Frans. 2012. "Introducing Cyber Warfare." In *Cyber Warfare: Critical Perspectives*, eds. Paul Ducheine et al. The Hague: T.M.C. Asser Press, 1 – 9.

Peoples, Columba and Nick Vaughan-Williams. 2010. "Securitization Theory." In *Critical Security Studies: An Introduction.* London and New York: Routledge, 75 – 88.

Peoples, Columba and Nick Vaughan-Williams. 2010. "Technology and Warfare in the Information Age." In *Critical Security Studies: An Introduction.* London and New York: Routledge, 149 – 165. 22 - 24.

Rogers, Paul. 2012. "Terrorism." In *Security Studies*, ed. Paul Williams. London: Routledge, 221 – 234.

Rothman, Maarten and Theo Brinkel. 2012. "Of Snoops and Pirates: Competing Discourses of Cyber Security." In *Cyber Warfare: Critical Perspectives*, eds. Paul Ducheine et al. The Hague: T.M.C. Asser Press, 49 – 68.

RTL News. 29 October 2014. "Hoe kwetsbaar is Nederland voor cyberaanvallen?" http://www.rtlnieuws.nl/nieuws/binnenland/hoe-kwetsbaar-nederland-voor-cyberaanvallen (8 March 2015).

Ruiz, Jorge. 2009. "Sociological Discourse Analysis: Methods and Logic." *Forum: Qualitative Social Research* 10(2): 1 – 21.

Singer, Peter W. November 2012. "The Cyber Terror Bogeyman." *Brookings* http://www.brookings.edu/research/articles/2012/11/cyber-terror-singer (8 March 2015).

Singer, Peter W. and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs To Know.* Oxford: Oxford University Press.

Wardlaw, Grant. 1982. *Political Terrorism: Theory, Tactics and Counter-Measures.* Cambridge: Cambridge University Press.

Wæver, Ole. 1995. "Securitization and Desecuritization." In *On Security*, ed. Ronnie Lipschutz. New York, Chichester: Columbia University Press, 46 – 76.

Appendix A: List of questions used for interviews

1. Wat is volgens u cyberterrorisme? En hoe staat cyberterrorisme in verhouding tot andere vorm van cybercrime, zoals hacken en DDoS-aanvallen?
    a. Is cyberterrorisme een uitbreiding van 'regulier' terrorisme, met een andere plaats van aanval, of is het totaal iets anders?

2. Is cyberterrorisme een daadwerkelijke bedreiging voor Nederland?

3. Wanneer werd er voor het eerst gesproken over cyberterrorisme in Nederland?

4. Welke actoren hebben een aandeel in de discourse rondom cyberterrorisme in Nederland?

5. Welke actoren hebben volgens u een aandeel gehad in het benoemen van cyberterrorisme als een dreiging voor Nederland? En waarom juist deze actoren?
    a. Zijn dit overheidsactoren en/of ook private actoren?

6. Wat onderscheidt deze actoren van andere actoren die cyberterrorisme niet als een dreiging zien?

7. Welke rol spelen technologische capaciteiten, legitimiteit en autoriteit van actoren in de discourse van cyberterrorisme?

8. Wat zijn de (voornaamste) belangen van actoren die cyberterrorisme als een dreiging voor Nederland zien?

9. Denkt u dat het beschermen van de Nederlandse cyberspace het belangrijkste belang is van deze actoren?

10. Welke maatregelen zijn er, volgens u, genomen om (de dreiging van) cyberterrorisme tegen te gaan?
    a. Zijn deze maatregelen gerechtvaardigd volgens u?

Appendix B: Transcripts of Interviews

Q: question asked or statement made by interviewer.

A: answer or question asked by interviewee.

Paul Ducheine, professor Cyber Operations at UvA and NLDA

Q: What is cyberterrorism, according to you? Also in light of the larger phenomenon of cybercrime and cybersecurity. Do you believe it to be an extension of 'regular' terrorism or do you think it is something totally different?

A: Originally I am a lawyer and my PhD dissertation is about military counterterrorism, in which terrorism does not play a very big role, but it is mostly about counterterrorism and the role of the military in that. I have chosen for an arbitrary definition of terrorism which was based on the UN report of the High Level Panel of the Secretary-General. This is a definition that is used by several countries, sometimes slightly edited, and laid down in criminal law. The central element is "an act that is intended to cause death or serious bodily harm to civilians or non-combatants, when the purpose of that act is by its nature or context to intimidate a population or to compel a government or an international organisation to do or to abstain from doing any act." The most important element is to create deaths and/or wounded. This is my starting point. This should give already some answers. I find it very dangerous to, because of a very unpleasing phenomenon: the fact that terrorists use the internet, or the use of internet by terrorists, to call this cyberterrorism when the internet is only being used as a mean for a terrorist act. I am opposed to terrorist actions, and for counterterrorism in every possible way, but I find it dangerous to qualify the use of internet in itself, as a mean, as cyberterrorism. Also when the internet is being used to solely create fear or anxiety, without the physical component attached to it, I do not think it is cyberterrorism. It is a different story when that fear is created with the help of the physical component, in which the internet plays a big role. Put simply: no, it is not cyberterrorism when terrorists use the internet, but some use of the internet can be crucial in creating fear through physical acts that create fear. When I send a tweet about that I hate Roman Catholics, and I am an extremist Muslim group, then I do not think that it is cyberterrorism. Cyberterrorism is doing terrorism in which the physical is being carried through or in cyberspace. The physical action is thus taking place in cyberspace, for example the placement of a bomb on Amsterdam Central Station or a logical bomb in the Amsterdam Internet Exchange which results in damage. This creates legal problems, such as what is damage? Is it only physical damage, or also the unavailability of

servers? I have a more liberal view on this, for example when the servers of the Amsterdam Internet Exchange are being shut down, it would argue that this can equal physical damage and can thus be understood as cyberterrorism. Because the server does not work or exist anymore. This means abandoning the definition provided earlier.
Q: Death of injury can then be the indirect result. For example, when hospital servers are attacked.
A: When the IRA was planning a bomb attack, they called first so that people could leave. But the bomb still went off and caused damage, therefore it was called terrorism. Regular use of the internet by a terrorist is not cyberterrorism, but rather how he uses it. Dutch criminal law says that terrorism should have the objective to create fear within a population, a government or international organisation to coerce them to doing something or to abstain from doing something or to disrupt society, a government or an organisation. The intended effect of a terrorist act should manifest itself in or through cyberspace for it to be called cyberterrorism. The cyberterrorist attack takes place within cyberspace or produced through cyberspace.
Q: The place of attack shifts in comparison with 'regular' terrorism.
A: Yes. The place of attack becomes the internet or the internet is used to carry out a physical attack. This second part is more difficult. Cyberspace is a layered phenomenon. It consists of people on the planet, accounts in cyberspace, hardware on the planet, and these accounts connect with the hardware. The whole is called cyberspace, it thus consists of people, accounts, data, operating systems, software and the hardware on locations. Attacks on people, hardware and locations are physical, and was already known as terrorism. Cyberterrorism consists of attacks on accounts, data, operating systems and software. The attacks on Digi-D/DigiNotar could be considered as a cyberterrorist attack, if it would have led to (deathly) injury or damage. To go further than Dutch criminal law currently does, I would qualify the elimination of services or facilities, with the intention to create among the population, as cyberterrorism. Maybe it is not yet possible to prosecute these types of crimes, but that might happen later. There has, however, been very little terrorism in cyberspace. There have been very little cases in which there were injuries, deaths or damage caused, with a terrorist objective.
Q: There have been numerous claims that cyberterrorism is happening, has already happened, will happen, but evidence is hardly ever provided. Recently, a report came out that the Ministry of Defence has been digitally attacked by several countries/organisations. Could that qualify as cyberterrorism?

A: No and if ISIS decapitates someone and puts it on YouTube, then it is also not cyberterrorism. The act on itself is a terrorist act and it is carried to create fear and that is reinforced by posting it online. But that is not the terrorist act. To penetrate into government systems to spy is not terrorism, it is espionage. To penetrate banks to hack accounts is a criminal act. If it happens in an armed conflict, for example to penetrate a hostile system and plant a virus to disrupt that system, it is an act of war. There are maybe not always clear boundaries, but there are distinct categories. Cyberterrorism is then a distinct category. Terrorism is a very extreme measure, mainly because of the severe effects.
Cyberterrorism is a form of cybercrime, the same as that terrorism is a form of crime. The response is usually that it is a crime, however, also Intelligence agencies have an interest in monitoring terrorism. Criminal investigation departments see those acts as a criminal offense and (try to) prosecute. Intelligence agencies are mostly concerned with monitoring and mapping those acts and protect international security from those acts, which does not necessarily lead to prosecution. Hacking and DDoS-attacks could be part of cyberterrorism, but it depends on the objective, which must be terroristic. Cyberterrorism is an extension of 'regular' terrorism with a different place of attack, or the mean is essential to carry out the attack.
Q: Do you believe that cyberterrorism is a threat to the Netherlands?
A: Considering the history, I do not think so. On the other hand, when I see that cybercrime is one of the largest violations of our part of cyberspace, which is visible in Nationaal Cybersecurity Beeld Nederland. Crime and foreign espionage are the main forms. Which needs to be taken into account, is that people will use those techniques for cyberterrorist purposes. Similarly to the fact that someone can detonate a bomb at Amsterdam Central Station. It happens not that often, almost never in the Netherlands. But somewhere else that does happen, maybe with a different intention. But terrorism happens, cybercrime happens, how long will it take for terrorists to carry out cyberterrorist attacks with the intention to create fear. And maybe it has happened, but we did not recognise it as cyberterrorism.
Q: Detection is difficult.
A: Yes, but it sometimes shuts down it gets noticed. The cause might not be clear right away, but a terrorist is usually inclined to claim responsibility. The hack on TV5 has been claimed by several parties. The same usually happens with 'regular' terrorist attacks.
Q: Does the internet enforces the anonymity of terrorists?
A: On the one hand, the internet offers opportunities to be anonymous or to enhance anonymity. On the other hand, terrorists want to reveal themselves to see what the effects are,

even if they act anonymous. There is a task at hand to verify whose is responsible, because some attacks are claimed by several people or groups.

Q: Which actors take part in the discourse of cyberterrorism in the Netherlands?

A: I do not know for sure, because I have not followed the discourse that good. What comes to my mind are the AIVD and MIVD, who are interested in terrorism, and the NCTV. Furthermore, the Public Prosecutor's Office is interested; the departments of the Ministry of Security and Justice who are interested in criminalisation of terrorism and cybercrime; think thanks such as ICCT, Clingendael, and faculties of some universities. But private security companies also play a role in the discourse, possibly only subtle and indirect. If those companies wish to sell their products, people and organisations need to be convinced that that product is needed and that there thus is a dangerous situation. Vital infrastructure, which is largely owned by private companies, also thinks about these things. For example, a company as Tennet, who suffered from a power-out recently, no doubt thinks about the digital disturbance of their systems or supply of power.

Q: What is the foremost interest of private companies to name cyberterrorism as a threat to the Netherlands? For example, the protection of the Dutch society, or also commercial.

A: Most companies have a commercial motivation, but also an interest in keeping the society going and their own services safe, especially if they are companies in the vital infrastructure. They get called upon when their services are not working and held responsible. It is socially undesirable, but also bad for business.

Q: The fact that private companies have that commercial aspect, is that a reason for why private companies might be more or faster inclined to argue that cyberterrorism is a threat?

A: Not all private companies argue that. For example, small companies are less aware and might not be subject to such a threat. Security companies who deliver a security product need to make people aware that such a product is needed and they need to invest in it. The need for such a product is only there with parties that are aware of the risk and have the financial resources available. The customers need to be sure that the product they are buying works. The security companies need to show through their track record that they can make something that can be effective. There needs to be insecurity, there needs to be a product and that product needs to be effective. And there needs to be a customer that is aware of that insecurity and wants to fix that.

Q: Needs such security companies to be seen as legitimate and have the technological capacities to protect the Dutch society?

A: Yes or pieces of that society. Several actors make a contribution to protect that society. Sometimes that are private actors in those places or areas where the government does not have a role or does not have the necessary knowledge. Public-private corporation is important. Resources are not necessarily the problem, because the government still has to pay, whether it is developed by themselves or bought from a private company. The knowledge sometimes lacks in the government, but sometimes it is a private task from which the government makes use of. Sometimes private companies are needed because they have the necessary infrastructure. We all want internet, but the government does not have internet providers. The government purchases that from private companies, who need to provide their products and services in such a way that the government can safely make use of them. Therefore, communication is necessary. And private companies also need to provide safe products and services to other parties, because we all need to have a certain amount of protection in cyberspace.

Q: Which standards are needed for such products?

A: It does not really matter who the customer is, but what the product or service is. If that product or service is being used in vital infrastructure it needs a better protection than for email programmes. It needs to be a matter of life and death or vital infrastructure. There are a few vital interests in the Netherlands: physical security of people and goods, economical security, ecological security, territorial security, and the political-social equilibrium. If a party through terrorist activity, while making use of internet/cyberspace, can start a fear campaign, we need to protect ourselves against that. The use of internet is not the cyberterrorist activity, but the internet is the facilitator in the creation of fear. There is the possibility of stopping unwanted activities on the internet by terrorists, without it being a counterterrorist measure.

Q: It might be unwanted that terrorists can access the systems which controls dikes.

A: Yes. Only the rightful owner needs to access such systems, no one else. Anyone who violates such systems, commits a criminal act. The intent of such a violation defines whether it can be qualified as a cyberterrorist act.

Q: There are also actors who do not view cyberterrorism as a threat. What is the difference between these actors and those actors that do view cyberterrorism as a threat? Why would private or government actors not view cyberterrorism as a threat?

A: I do not exactly know who do and who do not view cyberterrorism as a threat. The danger is sometimes stressed while the risk is arguably smaller. There was a time when everyone was scared for a cyberversion of 9/11 or Pearl Harbor. That has not happened yet. It is not to say that it is not possible. In hindsight it is easier to say that it was exaggerated. On the other

hand, it is not to say that the risk is not there just because it has not happened yet. Maybe it is difficult, through this domain, to result in such heavy effects. The chance of the event is smaller. But if the impact is high, the risk is also high.
Q: Are the measures to counter cyberterrorism mainly preventive instead of reactive, especially because it has not taken place yet?
A: When sometimes goes wrong in the digital domain, reaction is always needed. The same as in the physical world, for example when there is a fire, it needs to be extinguished. The reaction on events, whether there is a small or big risk, small chance, big chance, the reaction is always appropriate. Reaction is needed. If prevention is also preferred, money is needed. The questions are how the resources need to be implemented and how the level of security can be improved. The necessity of resources, such as people, money, and legislation needs to be balanced against the suspected level of insecurity. Do we expect these efforts to raise the level of security? These are political choices, money can only be spent once.
Q: Some people say that the government increasingly violates privacy. In which direction do you think that the balance between privacy and security, which is hard to get right, is going?
A: I do not know if that balance will shift in a direction. The legislator in the Netherlands chooses the balance between the government as a provider of security, and therefore it needs to admissibly violate some freedoms of people, and people needs to allow that. We all need to benefit from it; it needs to improve prosperity. In the 2nd strategy there is a triangle, which is a balance between security, freedoms, and welfare/prosperity. At the Global Conference on Cyberspace this triangle was also highlighted in the speech of Foreign Minister Koenders. The legislator determines, on the basis of human rights conventions, to what extent security can go, and how much privacy do we want. Do we all benefit, as a whole? In terms of security, and in terms of privacy. The determination of this balance is a very difficult task of the legislator and parliament members. I do not think it is decent to demand from the government to provide security, without giving that government authorisation to violate privacy for citizens. I do not think it is morally justifiable to demand security without wanting to give up some privacy. The same goes for citizens: they want security, but they need security for that, without security he cannot be free. Freedom does not mean very much if every hacker can access my piece of cyberspace and the government is not doing anything to stop that. Freedom does not mean anything, if it cannot be protected or secured. It are several balances. It is a triangle. Demanding security without willing to give up some privacy is amoral. And freedoms do not mean anything if it is not safe or secure. Citizens also need to have a certain mind set, such as is implied in the social contract between citizen and

government. A citizen gives up some of his freedoms so that the government can provide security. These freedoms are physical, property rights, fundamental rights etc. I am convinced that this balance will stay 'right' and will not tilt in any direction. We have parliament members who supervise and operate careful.

Q: Could anarchy exist, for example because legislation lags behind on technical capabilities?

A: Technical capabilities are ahead of the authorisations that government has.

Q: What is a cyberterrorist attack takes place and there is not yet legislation? What to do with the perpetrator(s)?

A: A distinction needs to be made. If we wish to prosecute (a) perpetrator(s), we have to deal with criminalisation and authorisations for surveillance and detection. That is a task for the police, the public prosecutor's office and the High Tech Crime Unit of the police. To prevent such attacks and to hinder them, we have the Intelligence agencies. They also need authorisations to monitor these type of threats and to predict. If we have the expectations that these organisations to this, but we do not give them the resources to do it, we have unreal expectations from the government. Parliament and government need to make a move. If the gap between what can be done and what is allowed needs to be resolved, the legislator needs to act quick and there needs to be a basis for it. The balance between security, freedoms, and welfare/prosperity is still under construction before legislation can be approved in the Second and First Chamber. There is a gap in authorisation because the technical capabilities cannot be exploited to its fullest because legislation does not allow that yet. The hope is that this gap will be closed soon, and until then these capabilities cannot be implemented as they would like to. Concerning the criminalisation of cyberterrorism, possibly some issues need to be fixed. The detection is more difficult: for detection in cyberspace more authorisations are needed that are not available yet. A new law must have detection possibilities for police. The Intelligence agencies also need to get more authorisations for monitoring and possibly prevention. Intelligence agencies can technically do some things, but they are not allowed to and thus they will not do that. Luckily, we live in a rule of law in which these Intelligence agencies and government are compliant.

Q: The practices of the NSA are not likely to happen here.

A: The NSA also operates within the boundaries, mandate and authorisations it received. But these could be greater/wider than it is the case here in the Netherlands. Each country has specified these boundaries, mandates and authorisations differently, but usually Intelligence agencies operate within a rule of law.

Q: Do you think the police and intelligence agencies search for the boundaries of their mandates?
A: Yes. The norms and authorisations given are formulated in an abstract way. This is normal, because we cannot provide in detail what we will expect to happen in the future. The authorisations are formulated in neutral terms, and in practice they need to see how those authorisations are in proportion to the terms from the abstract terms. This can lead to question marks. For example, necessity plays a big role with the implementation of certain measures. Is a certain measure really necessary, or is a 'lighter' measures also available or enough? How intelligence agencies fill in these abstract terms brings them to the boundaries of what is allowed and they examine them. In hindsight, they are sometimes corrected by the supervisor (Commissie van Toezicht). Either, they have to obey by the original rules in the future or the legislator decides to amplify the norms and authorisations. It is a constantly moving process. Because the balance between security, freedoms and welfare/prosperity is sometimes moving, interests need to be balanced also.
Q: Do you think there are enough people who critically view the measures and actions Intelligence agencies undertake to counter cyberterrorism and cybercrime? There are a few companies and think thanks, but is this enough? We, for example, do not have a whistle-blower such as Snowden.
A: Maybe we do not need such a person. It is complex. There are not many people how have enough insight into how the connections and relations are and can give a clear explanation. Usually, they solely focus on one side of that triangular balance. From the position they have on that angle, view their opinion or vision as complete. The search for neutral parties often leads to academics, who are not always very neutral, and think thanks who do research and have a vision. For example, every law faculty has a vision on this. Also political scientists and public administration students do research. Furthermore, academic agencies of political parties. The public opinion is the most difficult, because one-liners are difficult to make because of the complexity of the subject. Some nuance is needed. Not everyone can form a balanced opinion.
Q: Do you think that this is part of the problem that people have little interest in this subject?
A: I do think that the digital domain is strongly occupied by technical people and engineers. However, in the four years that I have studied this domain, I see an increase in policy oriented attention and research. It is a discourse that spills over into other academic domains and social structures. The vital sector does know that there is a problem that needs to be addressed (further). Smaller companies do not really have that realisation yet. But there are employers'

organisations who are facilitating in knowledge and know-how. There is growth in many places. There are a few masters on this subject that are expanding from solely technical to more policy oriented.

Liesbeth Holterman from Nederland ICT

Q: What is cyberterrorism, according to you? Also in light of the larger phenomenon of cybercrime. Do you believe it to be an extension of 'regular' terrorism or do you think it is something totally different?

A: My vision of cyberterrorism is essentially the same as my vision of terrorism. Many deaths is not necessary per se, but a group needs to have an aim of disrupting the society. The way in which this happens can differ, for example a hack or a DDoS-attack. A state or non-state actor that wishes to disrupt society.

Q: The place of attack is then the internet, instead, for example, a train station?

A: No, because a train station can also be closed, for example, through a hack. The internet is connected to everything. Terrorism does not necessarily have to be that someone shoots at people directly, or sets of a bomb. It can also be that they hack the points of rails and make two trains strike into each other and create deaths and/or wounded and possible fear.

Q: Does the goal needs to be societal disruption?

A: Yes. Terrorism does not need to necessarily cause deaths, although I do think that terrorists would appreciate when that happens, but that does not has to be the main goal. The main goal needs to be to create fear, for example that people do not want to take the train anymore because terrorists have hacked the points of rails.

Q: Do you believe that cyberterrorism is a threat to the Netherlands?

A: Yes. I do believe that terrorists do not realise yet that it is possible. I think that terrorists are naïve in thinking that societal disruption can only be caused by a physical attack or presence.

Q: When cyberterrorists come to that realisation a cyberterrorist attack will happen.

A: I hope that they do not come to that realisation, but yes.

Q: Do government and private actors have to guard themselves before terrorists come to that realisation?

A: Terrorism can also come from state actors, for example North Korea could also come to a similar realisation. Terrorism does not necessarily come from non-state actors. A distinction also needs to be made between a cybercriminal and a cyberterrorist. That divide is difficult to make and sometimes fluid. A cybercriminal is usually out for a profit, however, cyberterrorists are also making a profit, for example kidnappings. A cybercriminal can be a cyberterrorist and vice versa.

Q: Definitions indeed often overlap.

A: It depends on the goal and/or aim of the act, whether I would classify someone/a group as cybercriminal(s) or cyberterrorist(s).
Q: Which actors play a role in the discourse of cyberterrorism in the Netherlands? Are this government actors and/or private actors? What are their intentions in saying that cyberterrorism is a threat to the Netherlands?
A: I see the (securing of) cyber domain especially as a task for public-private partnership. A good example is the Cyber Security Council (founded by former minister of Security and justice Ivo Opstelten), in which government, industry and academia work together to talk about and solve problems in the cyber domain, especially strategically. Nederland ICT represents the ICT sector, the Ministry of Defence takes part, the NCSC, the NCTV, Tennet represents the vital infrastructure in the Netherlands, Shell as a representative of multinational companies. There is a lot of thought put into who should be in this Cyber Security Council. The people in it also have the knowledge and are representative for their sector that they are good participants in the overall discussion about the cyber domain. The Cyber Security Council is very important in this discussion. The NCSC needs the public-private cooperation for their existence. It is a totally shared responsibility. On the one hand, the government needs to set frameworks in which companies can do their work. On the other hand, companies need to make sure that they deliver safe products and the government needs to ask for those safe products. Because there is a chain of government and companies, everyone in that chain needs to be protected, otherwise everyone in that chain can be affected by an attack. It is not realistic that a company is not connected to the internet. A lot is possible on the internet, as long as you realise what is possible and thus also what harm others can do to you. Internet is an opportunity, and the Netherlands has seized that opportunity. However, their needs to be a realisation that cyberspace encompasses other dangers that the physical world.
Q: Does anonymity on the internet also play a role?
A: Yes. Because you do not see it, you do not know it. On the one hand, it is good that people are naïve because then they can move freely on the internet. On the other hand, that is also a danger because they expose themselves to danger without knowing it.
Q: Can instruction play a role in this?
A: Yes. We from Nederland ICT, specifically argue that cybersecurity needs to a concern for the top of any organisation. People need to be aware of cybersecurity at the top so they can lead by example, or otherwise said it needs to be a top-down movement. What we often hear in large organisations is that cybersecurity needs to be something that the IT-department deals with. It is not IT, it is organisation.

Q: Is there a realisation missing that what happens in the cyber domain can affect real-world relationships between countries?
A: The innovations in cyber, such as the Internet of Things, the cloud, the Snowden-affair, have made it possible that the cyber domain is being looked at from a juridical, ethical and societal point of view. ICT used to be controlled by the ICT-people, but now it is more from the organisation as a whole. What is interesting to look at is the document of Microsoft about cybersecurity norms. Microsoft argues that there need to be norms about behaviour on the internet. Now there are cyberattacks and possible cyberterrorist attacks being done by state actors, while there is no war. What is going to happen when there is war? Norms and values are needed to regulate behaviour in the cyber domain. Concretely, I find you interesting. I want to get a complete picture of you, through social engineering, and I build a vacancy that is specified for you. However, now there is a move. Instead of targeting an individual, now everyone with a Samsung telephone, for example, is being targeted. What is needed are norms and values so that not everyone, with a Samsung telephone for example, is targeted, but behaviour needs to be regulated in order to abolish the exploitation of weaknesses that affects everyone. Only those targets that are interesting need to be targeted. At the start of WW II, the Germans had modern and innovative weapons, while the allied countries mainly relied on old weapons. This is asymmetrical warfare. The same is happening now. GCHQ has probably hacked Belgacom to get access to phone records and metadata about communications in and to the Middle East. This is not who we should act towards each other. Therefore we need norms and values in the cyber domain. Stuxnet is another example.
Q: Is it like looking for a needle in a haystack?
A: Yes. Also there is a lot less controversy when the USA or the UK conducts operations like this. When for example China or Russia would have hacked Belgacom, it would be a lot faster classified as terrorism.
Q: Classic enemies, like Russia and China, are more easily accused and targeted than allied countries.
A: Yes, because the USA, and the UK, and Belgium are alliances in NATO.
Q: A coalition like NATO builds on the premises of mutual trust.
A: I would say keep that view on the world, but it may be a little naïve. I believe that we should develop norms and values, but it may be an utopia. On the other hand, it would be good that countries can be hold accountable on the basis of those norms and values, if a country might not act accordingly. More global discussions are necessary about what we expect from other. This has as an effect that cyberterrorism becomes scarier because we have

agreed that state actors do not engage in it. So when a cyberterrorist attack then takes place, it must be done by a non-state actor.
Q: Can the international secretariat on cyber that is being founded in the Hague play a role in the development of these norms and values? Because it is a cooperation between countries, and also companies.
A: I find that difficult. On the one hand, yes. On the other hand, it will only employ a few people. Let's hope so.
Q: It actually needs more people to be taken seriously?
A: Yes. China and the USA, and Huawei and Microsoft need to take the lead and then the rest will hopefully follow their example. These countries are frontrunners in cyber and innovations and if they thus develop norms and values it will be a sign that everyone needs to take them seriously. On the other hand, I am proud that the Netherlands is the host of such an organisation, because we are usually seen as neutral when it comes to international peace and justice. But the initiative for norms and values needs to come from these countries and companies.
Q: Does power of big countries play a role in this?
A: The big countries and companies need to be supporters and preferably frontrunners, when it comes to developing norms and values, otherwise they might not be taken seriously.
Q: Which actors see cyberterrorism as a threat to the Netherlands?
A: Everyone with some sense of the cyber domain see that there are threats in it. There are, however, differences in how they view these threats as big or not. Everyone that takes part in the Cyber Security Council views cyberterrorism as a threat, otherwise it might not be of use to take part in the discussion. However, if someone has a view with solid argumentation on why cyberterrorism is not a threat, they need to be taken seriously and be given a podium within the Cyber Security Council.
Q: The actors that see cyberterrorism as a threat, do they differ in the extent to which they see cyberterrorism as a threat?
A: The Ministry of Defence, the Cyber Security Centre and the AIVD already view it as a threat and they explicitly say that and that we should guard ourselves against it. A lot of members of Nederland ICT also see cyberterrorism as a threat and they are working on protecting and further securing their systems that have been attacked by cybercriminals/cyberterrorists. That are banks, vital infrastructure etcetera.
Q: Is it about prevention and/or detection?

A: Yes, it should go more towards prevention. What is happening now is that companies hire other companies to solve gaps or leaks in their systems after they have been exposed. Now there is a movement going on that companies realise that they need to secure their systems in such a way that they are not prone to cyberattacks or that their systems are vulnerable to cyberattacks. Prevention becomes more important than detection. The Netherlands should focus more on prevention, and we should make sure that we are not interesting for cybercriminals/cyberterrorists to attack. There is again a need for public-private partnership in which the government should lead by example. A government needs to conduct real-time auditing. And the government should act as a principal for companies and these companies need to on the top of their game. The 'game' between government/private actors on the one hand, and cybercriminals/cyberterrorists on the other hand, goes back and forth. And regularly the government and private actors are lagging behind and are being attacked.

Q: Do you think that there are companies who have an interest in maintaining those gaps and leaks, for example for profit?

A: No. Every member of Nederland ICT argues that we all benefit if we have a safe cyber domain. Trust in cyber is essential. A company that wishes to benefit from cyber insecurity, is a criminal.

Q: We all benefit from a safe and secure cyberspace.

A: Yes. We have in 2012 taken the initiative for responsible disclosure, because we then already saw that trust is essential in cyberspace. Ethical hackers need to be given the chance to report vulnerabilities. The government has also taken this up and carry it out, for example on the Global Conference on Cyberspace. Not only the reporting of vulnerabilities is important, but there needs to be immediately the opportunity to secure the gap or leak.

Q: So, not only detection, but also the possibility to repair.

Q: Have government and private actors with high technological capital, legitimacy and authority been more convincing in arguing that cyberterrorism is a genuine security threat? For example, a company that has the technological capabilities to secure government (systems) has a larger chance of convincing in the discourse of cyberterrorism than those companies that do not have the same level of technological capital.

A: Public as well as private actors have a responsibility. The hack at KPN from a few years ago has created a lot of awareness that other companies may be vulnerable to. The government must then not argue that these companies do not have their act together. The government needs to support openness. The Cyber Security Centre takes the lead in this.

Q: Small companies may not have the resources to secure themselves properly. Big companies need to take the lead in this.
A: Yes. 100% security does not exist, similarly to a bank vault. What is important for a company to realise is what information and/or which systems are most important to them and what thus needs to be secured most. Those things need to be protected the most and the best.
Q: To build a structure, similarly to the pan-opticon idea of Foucault, the build of a round prison with vision everywhere. And with several levels of information according to importance of protection.
A: Yes. What needs to be most protected and secured needs to be in the centre.
Q: Is cooperation between AIVD and MIVD a good thing, e.g. in the Joint Sigint Cyber Unit?
A: Yes. On the one hand, it is proactive. On the other hand, it is reactive. We must not argue that the Netherlands is solely defensive, they are also working offensively.
Q: We cannot say that what Russia or China are doing, for example, is not right, while we at the same time are also working offensively.
A: Yes. It depends on the extent and the norms and values and the methods.
Q: Does that depend on the targeted country? Is there a difference in the use of methods when it concerns allied countries and 'enemies'?
A: In the Netherlands, there is a 'aanwijzingsbesluit', a cooperation between different ministries. The countries and non-state actors that we need to look at are specified in there, as well as the methods and operations that can be used. There are a lot of steps involved before these can be used. The chance that a NATO-country is in there is more slim.
Q: Methods and measures that are employed need to be in proportion to the threat one poses.
A: Yes, that goes for the physical and cyber realm. The difficulty in the cyberspace is that is global and it is thus easier to hide where you really are. Tornetworks and more advanced encryption methods are being developed and that is a good thing, but they are more difficult to trace. However, not only governments and companies make use of them, but also terrorists. The threats in the cyber domain are different than threats in the physical world. Terrorists do not realise the full potential, but there comes a point when they do.
Q: Can this create a spillover?
A: Yes. When one terrorist can do it, others will soon follow. With the recent black-out in Amsterdam, there was the fear with a lot of Ministries and companies that it was a cyberattack. Luckily, it was a technical problem with Tennet. This shows that a lot of people see cyberterrorism/cybercrime as a genuine security threat. It was a relief that it was only a technical problem.

Ton Siedsma from Bits of Freedom

Q: What is cyberterrorism, according to you? Also in light of the larger phenomenon of cybercrime and cybersecurity. Do you believe it to be an extension of 'regular' terrorism or do you think it is something totally different?

A: We, from Bits of Freedom, see cyberterrorism as an digital exponent of 'regular' terrorism.

Q: Is it terrorism with a digital component, similar to hacking, or does it need a specific goal?

A: (Cyber)terrorism must have a specific goal, the action must be disruptive. It is not necessarily about the action, but more about the intent of the terrorist (group). It is cyberterrorism when there is a terroristic aim. There are not specific acts that can be qualified as cyberterrorism.

Q: Do you think that cyberterrorism is a threat to the Netherlands?

A: That is a very interesting question, about which I have thought about before. I would say that the threat of cyberterrorism is not really there (meevallen) to the Netherlands. Looking at the annual report of the AIVD, they argue that the threat of cyberterrorism becomes larger, and that there is a bigger chance that something happens. If you look at terrorists, then the aim is usually not hack into a system, do something do the system and then leave. That does not create enough fear among people. This will only happen if a terrorist carries out a large-scale attack, for example attacking and shutting down critical/vital infrastructure. And that is very difficult to accomplish. I do not except that this will happen. Now more and more things are connected to the internet, the chance increases that something goes wrong. At the same time, more thought is put into which things should and should not be connected to the internet. A few years ago, all SCADA-systems were connected to the internet. Unfortunately, some are still connected. This makes it fairly easy to operate a bridge from a distance. But this is not a very disruptive activity. I am assuming that thought is put into it that it is not fairly easy to access these type of things on the internet. This is not to say that the possibility will not exist in the future, but I think the chances are slim.

Q: Maybe terrorists do not want to disrupt these systems, especially because they use them their selves.

A: I think that terrorist(s) or (a) terrorist group(s) do not want to carry out cyber-related attacks just yet. However, they might use the internet and disrupting certain systems, for example the shutting down of an electrical plant, to reach their goal/aim. I believe that, at the moment, they prefer to do something that is not cyber-related. That is similar when someone hacks credit card data and use that in a malicious manner. Hacking into a security camera system can be done by them, but I do not qualify that as cyberterrorism.

Q: Which actors play a role in the discourse of cyberterrorism in the Netherlands? And which actors see cyberterrorism as a threat to the Netherlands? What are their intentions in saying that cyberterrorism is a threat to the Netherlands?
A: I believe that the AIVD/MIVD sees cyberterrorism as a threat to the Netherlands and that is a good thing, because they have more possibilities and capabilities to see whether it is a threat or not. Other organisations, such as The Hague Security Delta and Interpol, sometimes argue that cyberterrorism is a threat, thus European and international organisations. Government organisations as well as corporations say on occasion something about cyberterrorism. Their intentions are both their worry as well as more commercial interests in saying so, because they can make money from this worry. This is especially the case with private security companies. A very cynical view would be to say that it is a good selling point for their product. A less cynical view would also argue this, but then it would be more like an example in the discourse, because they need to say it is a (possible) threat in order to sell their product and/or services. If you are providing products and/or services associated with cybersecurity, you do not argue that there is no problem, because then you will not sell anything.
Q: So it is about the combination of interests, commercial as well as morally, at least with private companies.
A: It is a combination of commercial interests, mostly found with private companies, and more ethical points of view, usually found with government agencies. That the government is avoiding risks also plays a big role. Looking from this point of view, it is logical that the government is worried about cyberterrorism and thus wants to avoid risks and counter it. Also because it is unknown territory and it is not really clear what cyberterrorism is.
Q: Terrorism is usually difficult to define, also in criminal law. And cyberterrorism is then defined as terrorism with a digital component. Does this make it also difficult to determine what it exactly is and to claim whether it is a threat or not?
A: Yes. For example, I would not view a DDoS-attack as cyberterrorism, because it does not creates fear amongst people. It may cause difficulties for people, but it is not of the same disruptive nature as actual (cyber)terrorism is.
Q: (Cyber)terrorism must (have the intention to) kill people.
A: Yes. Deaths of people would be more an indirect consequence of cyberterrorism rather than a direct consequence. Recently, I read an article of Oerting. He nicely describes what we can be afraid of concerning cyberterrorism, for example it might happen that they shut down a hospital etcetera. It might happen like that, but it can also happen by the placement of a bomb

and that results in more damages. […] I predict that for now, without any knowledge of the future of course, it is a hyped problem or an exaggeration to act on the internet, on the part of the government. For example, by implementing prevention measures against something of which we do not exactly know what it is. And that is problematic. Cyberterrorism is in this way a mean to argue for (more) control over communication methods and such on the internet. It is a way of saying we need to know what is going on and therefore we need to look at everything. Whether such measures are proportionate and acceptable is a different point of debate. Whether new measures are needed depends on the definition of cyberterrorism. If cyberterrorism is what I believe it to be, then the current measures might be enough.
Q: The security and intelligence agencies are already countering terrorism via or with the help of the internet, so why would we need extra measures to counter cyberterrorism?
A: The law on Security and Intelligence Agencies is being revised and there you can see that the security and intelligence agencies (and the government) wants to be able to tap cable communications. Partly, they want to do this to detect malware, especially the MIVD. This would be a possible measure as counter cyberterrorism.
Q: It is still difficult to think of what measures might be needed.
A: The most advanced malware is currently not being used by private companies or terrorists, but by governments themselves, especially the American government. I am not necessarily saying that that is wrong, but this is essentially what I mean. The resources and knowledge for developing these systems lay with governments. It can be worrisome when other organisations acquire the necessary resources and knowledge, but that still begs the question if that is harmful and does a lot of damage.
Q: Terrorists indeed do not have the necessary knowledge and resources to develop something that does a lot of harm.
A: Yes. I do believe that there are terrorists that are capable of hacking, but I do not think that they are capable of developing such advanced malware. I do not know for sure, but I can hardly imagine that that is the case.
Q: It might be difficult for hackers to join a terrorist organisation because they need to be convinced of the ideology of such a group.
A: Yes and cyber can be not really appealing for terrorists.
Q: Maybe terrorist would want to die as martyrs and that would be difficult from behind a computer.

A: That is much harder to do through cyberterrorism. The mind set of terrorists is to create fear and anxiety, especially in the physical world. This is much harder to achieve through/on the internet and is thus less appealing.
Q: The internet is a real hype and what you can do with it, also in a harmful way. But terrorists continue to use the internet in a more traditional way.
A: That is not (cyber)terrorism. The internet cannot be used for placing a bomb somewhere. That is not specific to terrorism, but goes for all people. Terrorists usually make use of the internet for propaganda, and that is not (cyber)terrorism. A cause for concern is making the concept of cyberterrorism too broad. The focus must be on the intention of the terrorists.
Q: Do you think that the actors involved in the discourse of cyberterrorism who have been able to convince that cyberterrorism is a threat, have the technological capital, legitimacy and authority to develop the knowledge about cyberterrorism and the resources to develop technical systems?
A: When the AIVD/MIVD say that something is a threat, or that there is a threat somewhere, I would not put that into question. In their yearly reports they argue that the threat is becoming larger, but the chance that it will happen is just not really big. They convince me that the cyberterrorism threat is becoming larger, but that the problem is not really that big. Private actors do not have the knowledge that the AIVD/MIVD have in arguing that there is a threat or not. I have more trouble being convinced by private actors, because their interests are not always clear and equal as those of the AIVD/MIVD. Private actors also have a commercial interest in saying or doing something. The theoretical possibilities are great, but what is possible in practice is very different and there is usually less possible. Theory and practice do not coincide with each other.
Q: The government has the protection of the Dutch cyberspace/society as their number one interest. This is more difficult to determine concerning private actors.
A: Yes. These private actors develop products and services to also protect the Dutch society and cyberspace, but they would also like to make a profit. These products and services must be safe to use, for example for the government, to sell them. There is always an interest to enhance the demand for their products and services.

Ronald Prins from Fox-IT

Q: What is cyberterrorism, according to you? Also in light of the larger phenomenon of cybercrime and cybersecurity. Do you believe it to be an extension of 'regular' terrorism or do you think it is something totally different?

A: I do not think that we have seen anything that resembles cyberterrorism. For me, when we will see cyberterrorism, it will be when terrorists meet their goal of bloodshed and the creation of fear through the manipulation of digital systems. The effect must be that a lot of people notice it, for example when people cannot access their money at banks, or it must have an effect in the physical world, such as disrupting the train systems. Cyberterrorism is not when terrorists use the internet for their media campaign.

Q: Do you believe that cyberterrorism is a threat to the Netherlands?

A: Yes. I have been saying for over five years that there is a lot of potential for terrorists to use the internet to reach their goals/aims. That potential is there because of vulnerabilities on the one hand, and because terrorists are able to gain the knowledge needed to use those vulnerabilities on the other hand. But it has not happened yet. So it may seem weird that I keep repeating that we are vulnerable and this might happen. But I believe that something serious is going to happen in the future. The hacking of TV5 le Monde in France was a small example of terrorists that hack. What we do not realise is how we are digitalising. Where there used to be physical cables tied to each other, this is now a Windows computer that controls everything. In more and more places regular Windows computers are being placed that terrorists can use to realise their effects.

Q: Will the knowledge and resources needed for an attack be used more and more by terrorists?

A: There needs to be knowledge and skill and there needs to be something to be done. Terrorists already have the skills for some while, and the effects of what they do with those skills is getting bigger. Because of the 'Internet of Things' it will be more and more easier to create fear/anxiety.

Q: When and by whom has there been spoken of cyberterrorism in the Netherlands?

A: Well, I do not hear anyone saying that cyberterrorism is a threat. The tendency is: as long as it has not happened, it is not really there. Especially the government has a whole lot of other 'cyber stuff' to deal with, such as cybercrime, cyber espionage. There are state actors who are willing to engage in cyber conflict, for example Russia. There is already a lot to do concerning cyber. From this point of view I understand that there is not a lot of attention for cyberterrorism. On the other hand, on the defensive side, it does not really matter whether it

are terrorists who want to do harm or states, measures that counter cyberattacks are beneficial in countering every 'bad' actor. I hear a lot that cyberterrorism has not happened yet, but that they do realise that terrorists will make the step towards cyberterrorism. From the point of view of terrorists, it is not really weird to create fear via the internet because they already have the knowledge, it is a lot safer for themselves than carrying out a physical attack, it is a lot less expensive than digitally placed attacks. And there are favourable scale advantages, especially when an attack can happen at several places at the same time. It creates a feeling of insecurity and disruption of society. One of the difficulties of explaining the possibilities is that the chance exists that terrorists might carry out my own predicted scenario.

Q: What do you think of the idea that terrorists want to die as martyrs, for example through suicide bombings?

A: I believe that suicide is not the goal itself. Furthermore, that is the easiest way to place and detonate a bomb somewhere.

Q: The actors that speak of possible cyberterrorism, are they usually governmental actors or also private actors?

A: Think thanks not so much. The oil- and gas sector is more afraid of (h)ac(k)tivism than (cyber)terrorism. Essentially, I am the only one who is claiming that cyberterrorism is a threat.

Q: If actors in the future argue that cyberterrorism is a threat, are they then those actors with technological capital, legitimacy and authority? For example, security and intelligence agencies should have the necessary systems to detect a cyberterrorist attack. Do you believe that they already have those systems?

A: No. The security and intelligence agencies are mainly focused on (cyber)espionage and not so much on (cyber)terrorism. Even in that area they are not able to see everything that is going on. That has partly to do with the fact that these agencies do not have all the necessary authorities to do so, for example cable bound interception.

Q: They are working on it, through the revision of the law on security and intelligence agencies.

A: Yes and that is why I believe that cable bound interception should be allowed to give them the ability to see which threats there are to the Netherlands.

Q: Is there a focus on state actors, rather than non-state actors with these agencies?

A: Yes.

Q: Is that not a weird situation?

A: There must be something to look at for the agencies. On the one hand, they try to keep an eye on terrorist organisations and returned Syria fighters and if they are planning to carry out a cyberattack the agencies can respond accordingly. The agencies will not, however, systematically search for (possible) cyberattacks. The physical channels are being locked on the defensive side, but the digital channels not. The agencies do not systemically check if terrorists bring in digital 'packages' for an attack.
Q: Is this work that needs to be done?
A: If you ask Bits of Freedom, they will say no. That is a political choice. I believe that it needs to be done. For me, it does not matter for which actor we protect ourselves, the same action needs to be undertaken on the defensive side.
Q: Is it possible that private actors will provide the systems needed to detect a cyberattack?
A: Who provides the systems does not really matter. The agencies already have the systems needed to detect a cyberattack. What is missing, is the capacity to process all the material, and the material itself, meaning the interceptions they can take a look at.
Q: Do they lack the necessary resources and money.
A: Yes and legislation. If that legislation will be developed, the agencies will want more money. For three years they have been claiming that they need to be able to tap cable bound communication. If that is made possible through legislation, than the money needed to do it must also be made available. More investments and personnel are needed. Anglosaksian countries are investing a lot of money, for example the NSA and GHCQ, not only into their offensive capabilities, but also defensive. I am convinced that because they see with their offensive capabilities how 'easy' it is to enter systems of other countries, they realise they also need to invest in the securing of their own systems.
Q: Is there friction between the wish to enter easily into other countries' systems and the wish that other countries cannot enter your own systems easily?
A: Yes, but I believe that it is an eye-opener because of the realisation that it is fairly easy to access digital systems and to gain (classified) information.
Q: The cyber domain is fairly young, compared to the world itself. In a few decades we have seen many developments. Is there for terrorists more to gain than in the physical world?
A: I would not say more, but it is a different way of creating fear. People who monitor terrorists usually argue that there needs to be bloodshed, deaths. That is the way of creating fear. I believe that the way of creating fear can work differently if we are threatened in a different manner, such as via the internet. A consequence of the disruption of banks may be that people extract their money and that can have seriously economic consequences.

Similarly, if important news agencies are shut down we might panic because we cannot know what is going on.

Q: What is the main interest in naming cyberterrorism as a threat? For example, the protection of the Dutch cyberspace/society or commercial interests.

A: They who name cyberterrorism as a threat, realise that a cyberterrorist attack could happen. Actors who earn their money in this field, already earn enough, they do not need to name cyberterrorism as a threat to survive economically. When I say that cyberterrorism is a threat, I also argue that we need a plan B. Namely, an analogue backup system. Instead of investing in more digital means of security, make sure you have a non-digital backup, such as typewriters instead of computers.

Q: We defend ourselves digitally against (possible) cyberattacks. Do you think there are also physical ways of defending ourselves, for example infiltration in a terrorist organisation?

A: No. What is the best option on the defensive side, is to make sure that there is an (analogue) alternative. On the offensive side, infiltration is possible.

Q: For some facilities, such as vital infrastructure, it might be better to keep to the analogue systems and not digitalise.

A: Yes. The wish of the government is that the Netherlands in 2018 is the most digital country in the world. On the contrary, they also want to be the most cyber securitised country in the world in 2017. That are nice ambitions, but it is not impossible to reach both of these goals at the same time. The safest cybersecurity country is not digitalised. If you do not have the internet, you know for sure you are the safest when it comes to cybersecurity.

Q: In the Netherlands 90-95% of the people have an internet connection. But the Netherlands is also the country in which the most cyberattacks take place.

A: Russian hackers have discovered that when they hack into a Dutch laptop, they have a 90% chance that the owner does Internet banking on that laptop, the highest percentage in the world. In this way we make ourselves a target for ‘bad’ actors. Diginotar is a good example of how vulnerable the Netherlands is.

Q: One single terrorist or a small terrorist organisation can do a lot of damage.

A: It is much easier for a terrorist to see whether they can shut down KPN, for example, than to walk onto a busy market with a bomb. You would expect that a cyberterrorist attack should already have happened. But it seems that terrorists do not realise the full possibilities, they are only involved in minor stuff, such as hacking of twitter accounts.

Q: The internet is very anonymously. Do you think that this is dangerous?

A: Yes. There are a lot more possibilities to do harm of to create fear. Especially in the Netherlands, because we are very dependent on digital systems. First, something has to go wrong before you can react accordingly.

Eric Luiijf from TNO

Q: What is cyberterrorism, according to you? Also in light of the larger phenomenon of cybercrime and cybersecurity. Do you believe it to be an extension of 'regular' terrorism or do you think it is something totally different?

A: The definition of cyberterrorism I believe to be true I have written down in my article, which is derived from the definition of terrorism the AIVD has provided. The most important part is the intended effect and the intention. The intention must be to disrupt society or another terroristic aim. These two elements are what separates cyberterrorism from other forms of cybercrime. ICT can be a mean, weapon and target. People must be afraid to go outside, for example take the train, or have no trust in the ICT that controls such things. This must be the intended effect, but that is not easy to reach. We have never seen this before. In the book 'Jihadists and the Internet', the NCTV talks about how terrorists make use of the internet. However, that is not cyberterrorism per se. The media is quick to talk about cyberterrorism when usually it is terrorists making use of the internet, just like every other person does (with possible malicious intentions). For example, the media claimed that we had the first cyberterrorist attack in 1995, which turned out to be a 'simple' DDoS attack on a Ministry.

Q: It might be dangerous to argue that cyberterrorism is widespread. 'Regular' terrorism is also not widespread.

A: Yes. What we see is that the Americans are also exaggerating. Sometimes they argue that DDoS attacks have shut down drinking water supplies, while only the outer systems were attacked and not critical or vital ICT (systems).

Q: Do you believe that cyberterrorism is a threat to the Netherlands?

A: It can always be a threat. When terrorists realise that they can achieve their aims and goals by conducting cyberterrorism, then we will have to be ready for that. In the 1970s we also did not know it was possible to hijack a train, but it happened. There have also been two attacks on the gas industry in the 1960s. But we have forgotten these events. They appeared out of the blue. Similarly, terrorists might be able to hijack train control systems and crash two trains into each other. Terrorists must acquire the technique (and technical skills), and have the intention to carry out such an attack. Terrorists have achieved their aim when people are afraid to take the train.

Q: Similarly, we did not see the attacks of 9/11 coming, but they happened anyways.

A: So yes, an attack is possible. But the likelihood is very low. However, we do need to realise that the Netherlands can be a target. There is very large IT infrastructure, but we are

also highly dependent on it. So terrorists might be able to achieve their aims. We also have some specific targets, for example when Geert Wilders realised his film, there were worries for DDoS attacks. With situations like this, we have to realise that we might become a larger target for terrorists to achieve their aim. Terrorists might also carry out a bomb attack, while at the same time target information systems of banks to create more anxiety among people. This has a magnifying effect, because people cannot access information about the disaster.
Q: Is the Netherlands an easier target because we are relatively well connected to the internet?
A: Not every vital ICT infrastructure is connected to the internet. 95% of ICT in the Netherlands is not connected to the internet. Train- and metro systems are not connected to the internet, possibly only via via. But if terrorists find another way to break into these systems or shut them down, it will be disastrous. Cyberterrorism can attack much more than solely the internet, which is only a small part of ICT, a lot of which is hidden. Internet is only a small part of cyberspace, this realisation is important. ICT is implemented in much more things that we realise now, such as cars. When terrorists are able to hack into these type of systems, the damage can be far greater than when they only attack the internet. Also, more and more systems are becoming intertwined, which makes it sometimes more difficult to find the source of the 'problem' or attack and which systems is being compromised, and who is thus responsible for fixing it.
Q: When became cyberterrorism a subject of conversation in the Netherlands? And which actors take part in the discourse of cyberterrorism in the Netherlands?
A: Around 1995 in the media. Regularly they report about cyberterrorism. However, they do not know what they are actually talking about and what cyberterrorism is. They use the term because it appeals to people and it is a catching title. The government, and especially government organisations/departments that are not in the centre of counterterrorism, also write about this. In the United States they regularly have exercises against cyberterrorism, because everything that is out of the ordinary is viewed as terror in the US since 9/11. They are really afraid that terrorists might shut down their power supply, while their systems are too easily compromised by other factors such as squirrels and the wind. I think they should focus on improving their systems against these types of 'accidents' first, before worrying about (cyber)terrorism. The Netherlands also takes parts in these exercises against cyberterrorism. However, they types of attacks they are trying to protect themselves from are solely other forms of cybercrime, such as hacktivism or criminal hackers. The most important thing is to label correctly, which is often not being done. There is very little reflection about

what terror actually is. That is why I advocate that we should talk about the definitions first, before worrying about possible threats.

Q: Many studies talk about cyberterrorism as being a genuine security threat. Especially the Americans, and also to a lesser extent the British, have 'framed' cyberterrorism as a threat. A survey has also shown that Americans believe that terrorism is the number one cause of death in the US, while that is not the case at all. Is there something wrong with the perception of (cyber)terrorism and how it is viewed by governments as well as the public?

A: The Americans might something exaggerate about (cyber)terrorism, however, in the Netherlands we are sometimes a little naïve about (cyber)terrorism, we pretend that it does not really exist. The tendency is to focus on the terrorism of yesterday, of the day before we have already forgotten, but we forget to look at what can happen tomorrow and in the future. We have been very busy with looking at Al-Qaeda and IS(IS), but we are not looking at what might face us in the next 10-15 years. We are constantly surprised by a new wave of terrorism, like we were surprised by the Rote Armee Fraction and the train hijacking by the Molukkers. Therefore I argue that we should look ahead at what the next wave of terrorism might be, which could be cyberterrorism.

Q: The focus is now essentially solely on jihadist terrorism, while extreme right-wing and extreme left-wing terrorism is being forgotten.

A: There is no capacity to look at these groups besides a few politicians that argue that we should look into biker gangs and such. I argue that we should look at (cyber)terrorism, but then in the right proportions and definitions.

Q: Before predicting if it might happen, we need to be sure what it exactly is we are talking about.

A: And there might come little groups into existence that might take advantage of people with the necessary skills to do harmful things. We know that Al-Qaeda was moving in that direction, for example hiring high-tech personnel and writing fatwa's. Cyberterrorism is only less visible than 'regular' terrorism, for example exploding a bomb in the market square. Therefore we, on the other side, should be thinking about what it is and what it can do.

Q: It might happen, but terrorists have not come to the realisation that they can do it. They can, arguably, create even more damage than with regular means.

A: Terrorists have already seen the potential of hacktivism. For example Bin Laden has expressed the wish to shut down financial markets for a longer period of time, which can cause a lot of damage. The idea was there, it has not been carried out (yet). With cyberterrorism the aim might not be to cause bloodshed, but rather to largely disrupt society.

There is however some vagueness into whether this is to be named cyberterrorism of activism, or other forms of crime. There is some overlap between different forms of cybercrime. In the physical domain distinctions might be more easy to make.
Q: What kind of role do technological capital, legitimacy and authority play in the discourse of cyberterrorism?
A: Technological capital is needed for ICT. Means are, in general, not very expensive. Legitimacy is not a concern for terrorists, they usually make use of fatwa's to legitimise their actions. Terrorists usually do not constrain themselves by laws and legislation.
Q: My research is focused on the technological, legitimacy and authority of the actors that claim that cyberterrorism is a genuine security threat. I research whether there is a difference between government and private actors on these concepts and whether they play a role in whether an actor argues that cyberterrorism is a threat or not.
A: I do not think that these concepts play a role in that. In case of an event, there are a few things that need to be considered. First of all, there needs to be consensus on whether the event qualifies above a certain violence threshold. Second, can we figure out what the intentions are of the attackers. Do these terrorists have the intention to disrupt society or to manipulate political decisionmaking? After a bombing on a train in Barcelona, Spanish politicians decided to withdrawal from Afghanistan. This is an event in the physical domain, but the same can be done through a cyberterrorist attack. The focus should be on the intention and the intended effect. Important is what is affected. Is that social cohesion, government functioning, utilities, railway? Ultimately it is about the disrupting of society.
Q: Something I have the idea that too much attention is given to (cyber)terror, while 'regular' crime is overshadowed.
A: Not only 'regular' crime, but altogether. Safety and security is too often deemed not important enough and not enough attention is paid to it. Also the communication systems, such as the broadcasting systems of stations, and the communications skills of executives is often deficient. These are simple things to tackle. For example, the mayor of London was very good in convincing the public to still take the subway after the bombings, because he showed that he was not afraid to do so himself. One of the most important things is to display confidence and trust, as well as sympathy. And this can be thought and improved. First, the basis security needs to be improved, which entails removing some vulnerability to attacks. Something still might happen, but the chances are slimmer and in hindsight it can be said that the basic security was thought of. That is thus self-interest. People who argue that cyberterrorism is a threat to the Netherlands have a self-interest in that they want publicity.

They want their name in the media and possibly sell their own products and services. But let us first consider the basics, before talking about cyberterrorism.
Q: Do we might exaggerate cyberterrorism and make it something that it is not? For example, making it 'bigger' than others forms of cybercrime.
A: Eventually, the effects can be severe. For example, influencing physical layers through digital layers. Attention needs to be paid to this. Security has to be good, regardless of what terrorists might or might not (be able to) do. A virus might have the effect as a cyberterrorist attack. When basic security is in order, then the likelihood of being a good target decreases.
Q: Do you believe that the protection of the Dutch cyberspace is the foremost interest of these actors?
A: It must be about everyone's welfare. Cyberbeeld Nederland already indicates enough other problems. When we deal with those problems, we almost automatically also deal with the potential effects a cyberterrorist attack can have.
Q: Which measures have been taken, according to you, to counter the threat of cyberterrorism?
A: There is a good structure of crisis management, the Incident Response Team, we have early detection. Exploration is needed to find possible threats. This all is intended to decrease the likelihood of being a 'good' target.
Q: 100% is maybe a fairy tale, although we might strive for it.
A: That costs simply too much. And we should not want that as a society. Innovation is necessary and ethics needs to be taken in consideration. There is hardly being learned from mistakes in the past. We make the same mistakes as we did in the past. Innovation is sometimes being triumphed by security. Adding security in hindsight never works well. Developing high-tech products and being the first to bring these products to the markets is deemed more important.
Q: Commerce triumphs security.
A: We need to learn from the past. When was the first headline about cyberterrorism in De Telegraaf?
Q: Somewhere in the nineties?
A: Already in 1977, which indicates that it has been on the agenda for a while. Historical awareness would be a good thing.

The Ministry of Defence

This interview was not recorded and this transcript is therefore not as similar to the others. Furthermore, some shared information was confidential and is therefore not displayed in this transcript.

A: Let me first start by saying what I do. I research the interests and stakes of the Ministry of Defence and the Defence industry, related to cyber. Although we do not use the word 'cyber'. That is divided into three strands. First all, we research and counter digital espionage; second, we research military-offensive capacity of other actors; and third, we have a cooperation with the Defence Cyber Commando. We have two approaches in our research. First, we look from the point of view of the perpetrator. The Netherlands is a country in which deliberation and cooperation between organisations and public and private partners is very common. Therefore, there is a division within this point of view: the police's concern is criminals; when a state actor is involved it is the concern of the Ministry of Defence and especially Defence intelligence; and a third concern is anyone whose aim it is to target the Dutch troops at home and abroad. The second approach is from the point of view of the victim(s), which is the Defence industry at large.

Q: What is cyberterrorism, according to you? Also in light of the larger phenomenon of cybercrime and cybersecurity. Do you believe it to be an extension of 'regular' terrorism or do you think it is something totally different?

A: Essentially, here we see cybercrime as e-crime. We do not use the word cyber here. But cyberterrorism we see as the terrorist use of cyberspace as an extension for actions with a terrorist aim or goal. With terrorist(s) we mean groups and affiliated individuals who act with terrorist means.

FireEye, an American cybersecurity company, has stated in public that ISIS is using the dark net to advocate the use of cyberspace for terrorist aims/goals.

http://www.ft.com/cms/s/0/92fb509c-3ee7-11e4-adef-00144feabdc0.html#axzz3bjWRvECc

On this dark net ISIS can purchase cyber weaponry for thousands or tens of thousands of dollars, and it does not take a lot of means or expertise.

A concern are people with a personality disorder that train themselves extremely in one speciality. This speciality can thus be cyber. If those people radicalise in such a way that they involve themselves with terrorist activity or terrorist organisations, they could pose a real threat. Current attacks, however, are mostly limited to DDoS-attacks and defacements.

Q: Do you believe that cyberterrorism is a threat to the Netherlands?

A: Private companies as well as individuals or government institutions are often not properly secured against cyberattacks. An important concern is the vital sector, which uses ICS/SCADA systems. If they are infiltrated, they can be manipulated. However, we have not seen any cyberterrorist/e-terrorist attacks. The US, for example, is often an interesting target because of their position in the world. IS has as a goal to create fear/anxiety, so naming cyberterrorism as a threat would mean giving exposure to them and other terrorist organisations. The Cybersecuritybeeld Nederland shows that the Netherlands is a target for (potential) cyberattacks, but it has not yet materialised,.

Q: Why would terrorists engage in cyberterrorism and is it feasible for them?

A: There are a few elements to consider. First of all, cyberterrorism involves a lot of things. Second, the effect of conducting an attack is great and the chance to get caught is low. Third, it is important to define the starting point, such as the definition of cyberterrorism and what is the status of the terrorist(s) (organisation(s)). And finally, the intentions of the terrorist(s) (organisation(s)) matter, what is their aim/goal? Cybersecuritybeeld Nederland shows that people have specialised in cyberspace and what is possible in a criminal or terrorist manner. It also says that digital attacks are used as support for other physical attacks. Terrorists are engaging themselves more and more in cyberspace and technology. They are taking lessons in hacking, there is more information to be found online and digital attacks are fairly simply to carry out. And they are planning to attract more funds to advance their digital capabilities.

Q: Which actors take part in naming cyberterrorism as a threat to the Netherlands? Are these private actors, and/or also private actors?

A: The Dutch department of Defence usually does not mention the name cyberterrorism, and thus does not think that cyberterrorism is an existential threat at the moment.

Q: What are the interests of private actors that argue that cyberterrorism is a threat?

A: Commerce is an interest of private actors. Although they also do care about protecting the Dutch society and cyberspace, but they are interested in making a profit. In general, government institutions will not and cannot overstate the threat since that is governed by laws that require factual statements.

Q: What kind of role do technological capital, legitimacy and authority play in the discourse of cyberterrorism?

A: The rumours about the cooperation of the BND and the NSA, which led to the tapping of cables in Frankfurt, also states that KPN was under surveillance by the BND and NSA because of this tapping. The Dutch minister of Interior stated that there are no signs that Dutch targets were under surveillance. However, most of the popular media and public did

not believe him. Until a weblog ‘De Correspondent’ published an article on the evening of 28 May stating that there is no proof that this tapping has happened. ‘De Correspondent’ argues that we do not know if Dutch cables have been tapped, we do not know what this tapping would entail and we do not know from who the data is that would be tapped. And there is no indication of the scale of the tapping. On social media there was applause for this weblog, but the minister for the Interior harshly had credibility in the eyes of the public. This example shows that there is little trust in what the government and its representatives have to say: what people with power say, cannot be true, should be doubted and questioned by default. The media were publishing big headline stories about economic espionage and mass surveillance. However, it was not until this article was published, by one online news agency, that other media and the public believed that there was no proof for this alleged tapping. Legitimacy and authority are thus not always larger for government (organisations) than private companies/organisations. Furthermore, I believe that it is fundamentally wrong to say, as deconstructivists such as Foucault and Derida do, that there should be no authority and power to ‘govern the world’. There should be one or multiple authorities that govern a country in order to avoid chaos and anarchy.

Q: Which measures have been taken, according to you, to counter the threat of cyberterrorism?

A: There is a lot of capacity to deal with terrorism in general, and also more and more for cyber related research. Irrespective of the perpetrator, research on attacks is being intensified, and so it should be. The relevance is to research what the aim or goal of the manipulation is, who is behind it and how we can counter the threats we are facing.

Constant Hijzen, PhD candidate from Leiden University

Q: What is cyberterrorism, according to you? Also in light of the larger phenomenon of cybercrime and cybersecurity. Do you believe it to be an extension of 'regular' terrorism or do you think it is something totally different?

A: I am an historian and I write a PhD dissertation on Intelligence and Security Services in the Netherlands and I teach classes on political violence and terrorism. I think that cyberterrorism is similar to the definition of terrorism. There must be a certain goal or ideology behind it. This is also what divides public policy and extremist issues; a motivation to disrupt society or the status quo. This divide can also be found in the cyber domain; the presence of an ideology determines whether an attack is a cyberterrorism or cybercrime. This ideology must be economically, politically or socially motivated for it to be cyberterrorism.

Q: Do you believe that cyberterrorism is a threat to the Netherlands?

A: I am not informed enough to make a good judgment about this, but from what I have read, for example the yearly reports of the AIVD and MIVD, the cyber component is becoming larger. Our vital infrastructure has an increasing digital component, which makes us more vulnerable. It can be argues that if terrorists would like to carry out an attack, it must have a cyber-component. I believe that the chance of an attack is realistic. The greater the dependency on cyber and the internet, the greater the vulnerability.

Q: Recently, I have talked to someone from the Ministry of Defence and he argued that cyberterrorism is not a topic that is under consideration there and is also not mentioned in the yearly report of the MIVD. However, in the yearly report of the AIVD it is mentioned that the intention for cyberterrorism is present and that the potency is growing and that cyberterrorism is thus a worry for the future. Can you think of other actors who have said anything about cyberterrorism?

A: For example the NCTV, do they name it as such? Have you looked into them?

Q: The focus of my research is the discourse of cyberterrorism, so who has said anything about it and why.

A: Have you figured why at the Ministry of Defence they do not use the word cyberterrorism?

Q: The person I spoke to has said that they word 'cyber' is not being used at all. Which is why it is a bit strange that they have the Defence Cyber Commando. They prefer to talk about e-crime and e-terrorism, which could result in a different definition. At the Ministry of Defence is the focus, logically, on the interests of the Defence (industry). Their focus is mainly on state actors and state-sponsored terrorism. Therefore it may be harder to research cyber related actions. I have to do more research in order to fully comprehend why it is not a focus for

them. What he also said was that by expressing the term cyberterrorism we might give exposure to terrorists and might bring them to an idea they have not thought of themselves. By expressing the term cyberterrorism, which has not happened yet, we might make it a bigger problem than it actually is.
A: At the AIVD they do explicitly talk about cyberterrorism. The AIVD might have more vigour than needed for this problem.
Q: The AIVD has a more broad perspective than the MIVD, because they look at how terrorism impacts and disrupts society as a whole, while the MIVD solely focuses on the Defence (industry).
A: The difference can indeed be this difference in focus. If the consideration indeed is that the term cyberterrorism in itself implies a certain meaning or action, then the MIVD might not be inclined to use it because it can give too much power to the word alone. A similar course of action was chosen by the BVD, the predecessor of the AIVD, on terrorism. Performativity entails that labelling something changes the way people view it. Naming the phenomenon changes the phenomenon. Terrorism was therefore named by the BVD as 'politically violent activism'. This performativity might also be the reason why the Ministry of Defence does not mention the name cyberterrorism. Cyber- and cyberterrorism might be a fear creating label which has a certain effect and therefore we need to be reserved in using it. I can imagine that because the AIVD has a broader view than solely the Dutch forces, they give more attention to the subject. A suggestion is to look how the NCTV views this subject, for example in the most recent Dreigingsbeeld Terrorisme Nederland.
Q: The NCTV does indeed mentions the name cyberterrorism.
A: And look also at which terms the National Cyber Security Centre uses. Are they reserved in using this terminology or not?
Q: They do mention the name cyberterrorism. They do say that it has not happened yet in the Netherlands. The threat is not that bit right now, but similar to what the AIVD argues, the potency is growing. Predictions are always hard to make, but in a few decades it might be a bigger threat than it is right now. The AIVD and NCTV largely agree with each other.
A: It is interesting to look at which actor(s) does and which actors) does not use the label 'cyberterrorism' because your thesis focuses on the discourse of cyberterrorism. I do not have extensive knowledge on the subject, but it should not be too hard to find it.
Q: Do you know which private actors might use the name cyberterrorism?
A: Companies such as Fox-IT, who make a profit in this domain. Are there any other participants in this field?

Q: Not that I can think of. Most companies that deal with these types of subjects are American or British.
A: Symantec is such a company that provides the Norton antivirus software. They sometimes make statements about these subjects in the American press and how the current state of affairs are in the American cyber domain.
Q: The focus of my research is the Netherlands to delimit the scope of the research. Doing research abroad was not possible.
A: Who would be a contender of Fox-IT in this domain I would not know. There are not many companies who exclusively focus on cyber security.
Q: What would be the interest of Fox-IT to name cyberterrorism as a threat?
A: It has an effect. The influence of such a company on the government can be quite large. Because the government cannot possess all the know-how, and expertise that is needed. For a small country such as the Netherlands it is very difficult to acquire all of that solely within the government. The government is no matter what dependent on private actors for this. It is important how they treat, label and talk about the problem. If they would avoid using the word cyberterrorism, because then we would make it into a problem or treat it is not, and will not cooperate in doing anything about it, then this is a substantive message. Because of the big dependency on private actors, private actors can influence the discourse quite immensely.
Q: Does it also play a role that they are a private actor, and that they thus have a commercial interest in the naming of cyberterrorism?
A: That is possible. Every private actor has some sort of commercial interest. However, I do not think that that is the main interest of companies such as Fox-IT. I do not think of them as a party that exaggerates (the threat of) cyberterrorism to make a profit. There was one advice company on terrorism that create world maps of where in the world terrorist attacks had taken place in one year. This was very unsubtle because a country as Russia was totally red because a few attacks had taken place that year. However, because Russia has such a large territory the perception of the treat was larger than the reality of the treat. This is an obvious example of exaggeration the treat to attract more clients and eventually make more profit. They are making money from a problem that they actually should counter. If they would argue that it is a small problem, they would have no or little work to do. But I do think that there is some ethical consideration in arguing what is a treat, because there are enough treats as it is. A problem or possible problem does not have to be exaggerated to create demand for a private company's products and services. There is enough vulnerability in the cyber domain to continue the work for many decades. I do not think a company such as Fox-IT needs to

exaggerate the treat of cyberterrorism to continue their work. I imagine that there is consultation between the government and private actors in which the government makes use of the expertise and know-how of those private actors on these type of issues. There is a risk that private companies exaggerate the treat, but I do not think that it happens often, because there is enough to do already.

Q: What interest have civil rights foundations, such as Bits of Freedom or Buro Jansen & Janssen, in naming (the treat of) cyberterrorism?

A: They are exponents of civil society that are an addition to the more formal supervisory structure there is in this domain as well. They have taken on the task to check and examine the practices of the government. I find it really important what they do. They structurally write reports, read and review reports of government organisations, and do research themselves or by others. If they claim that either the government is exaggerating the problem or dismisses the severity of the problem, it is an important signal. I find that their influence on the discourse is thus great and that is as it should be. They can make statements in the press and organise and be part of events. Since they claim that there is a (minor) problem, does mean that it is a problem that exists and there should thus be attention paid to it. It is thus not a problem that has been put forward to give people and companies something to do.

Q: Some people speculate that civil rights foundations, such as Bits of Freedom and Buro Jansen & Janssen, might exaggerate the threat of cyberterrorism to either gain more exposure for themselves or to argue that the government and/or Intelligence and Security agencies do too little or too much to counter this threat.

A: I do think that there is some truth to that. Such foundations do need their time in the media and they need to place their issues on the public and government agenda. They derive their right to existence from these type of issues. For example, Bits of Freedom has called the expansion of the Law on the Intelligence and Security Agencies for a long time ‘seine surveillance’ (sleepnet surveillance). This type of terminology does thicken the discussion. They take this stance in the debate, but the effect of them doing that is quite big. It does not clarify the discussion, as they would like to do, but thickens it. By using these types of words they suggest that with this new law everyone can (and will) be audited. But this is just not the case. So there are some valid points brought forward by those that argue that these foundations might exaggerate the threat. On the other hand, for policy officers/advisers it is already more difficult to cope with such foundations, who have different interests. These type of foundations need to ‘earn’ their right to existence and therefore might frame certain issues or points of view by using certain terminology. This can influence the discourse heavily.

There needs to be hope, however, that there are (some) sensible people working for such foundations that are capable of cooperation or consulting with policy officers/advisers. There need to be some critical points of view, but there also needs to be possibilities for cooperation and consultation between these foundations and the government (organisations).
Q: You stated earlier that if certain actors have the acquired knowledge they can influence the discourse (heavily). Do concepts such as technological capital, legitimacy and authority also influence the discourse of cyberterrorism (heavily)? When a company has a lot of technological capital, such as Fox-IT, can they influence the discourse more than others?
A: That is a difficult question. The underlying question is how the discourse takes shape, which is difficult to answer. In the last 10 to 20, maybe 50 years, the media and Parliament are important actors that can influence, shape or change a discourse. The framing of many complex policy issues, which are the work areas of politicians, policy officers/advisers and employees of relevant companies, is difficult to place in a discourse. The formation of a discourse is not always coupled with the complexity of the problem/issue that is the subject of the discourse. Indeed, usually the discourse does not do justice to the complexity of the problem/issue. The debate about intelligence and security in the United States is heavily politicised, and the debate is so far off from the real problem. The availability of frames from which people can choose from is very limited. The decisions are made within that debate and later on that political decision needs to be translated into practice for the Intelligence and Security Agencies. From this point of view I do not think that more technological capital or more legitimacy results in more influence in the discourse. Sometimes it is just coincidence; one headline in the media, one scandal can result in a change in the discourse. I doubt whether actors with high technological capital, legitimacy, and seniority have the largest influence on a discourse. I do not think so actually.
Q: These concepts are part of my hypothesis. I am researching whether these concepts play a role with actors that have said something in or about the discourse of cyberterrorism. There are a few actors that could play a role in the discourse based on these concepts, but are actually not taking part. For example, companies such as Tennet or KPN, who are in the field of vital infrastructure and ICT. Within these fields many knowledge is missing about cybersecurity in general. Their main focus is on technological innovation, and not so much on security in the digital domain. A lot of those companies would like to do something or more with cybersecurity, but they often do not know how. I believe that when these companies would focus more on cybersecurity and cybercrime, they could have a larger role in the discourse. Private actors have not (fully) realise the necessity that it is important to focus on

cybersecurity. The main focus is still on physical security. The reason for this could be that cyberspace and the internet is a relative young phenomenon, but there are many vulnerabilities in the cyber domain.
A: In this manner it can be a change in the discourse. The threat perception, what is a cyberterrorist attack, could become clearer if the problem/issue is materialised by private actors that can actually show what and how a cyberterrorist attack could harm a company and what the consequences would be.
Q: The abstraction level could decline. Now it might be hard to imagine what a cyberterrorist attack actually is and what it could do, but in this way it could become more concrete. Also because a cyberterrorist attack has not taken place yet. Some argue that there have been cyberterrorist attacks, for example Stuxnet or the hack of TV5 Monde, but all of them are actually forms of cybercrime or state (-sponsored) attacks without terrorist associated effects. It depends largely on the definition of (cyber)terrorism that is used. The disagreement is largely on whether a cyberterrorist attack should have deaths/wounded as a result or if the creation of fear in a population or the disruption of society is 'enough' for it to be an effect of a (cyber)terrorist attack. Maybe this disagreement about cyberterrorism is even larger than with 'regular' terrorism.
A: Well, the disagreement about the definition of terrorism is already going on for 30 years. The same discussion is going on in the cyber domain.
Q: One of the biggest questions is how to create deaths by using the cyber domain or by attacking it.
A: Maybe it is creating deaths/wounded by shutting down vital infrastructure in traffic or public transport.
Q: My interviewee at TNO talked about trains colliding and thereby creating deaths/wounded. However, this could also be qualified as an indirect attack on physical infrastructure. It is very complex. Mostly we see that cyberterrorism could be employed as terrorism with cyber as a mean to reach a terrorist aim/goal.
A: Funding and investments have been enormous for cyber related research and activities. The danger is that people within government who need funding 'frame' their problem as being a cyber related problem. This increases the complexity of the issue and thickens it.
Q: It is one of the few fields in which investments were widespread over the last few years. A lot of budget cuts on the Intelligence and Security Agencies were announced, and maybe in this way they can receive more funding anyway. This is part of the framing, exaggerating the problem or threat.

A: This is not an rarity within the government (organisations): focusing on the same problem/issue, only with a different name. The same has happened with the 'Vogelaar-wijken'. These districts were offered funding and help to improve. The consequence of this policy was that other districts or areas that did not necessarily were the focus of this policy tried to meet the criteria. To receive funding, the focus of a problem/issue is put on a cyber element and sometimes it indeed works.
Q: Which measures have been taken, according to you, to counter the threat of cyberterrorism, or do they fall under the measures to counter cybercrime in general?
A: One of the measures is thus the increase in funding within the Ministry of Defence. This is not only done for securing (defensive capabilities, but investments are also made into offensive capabilities. Both Intelligence and Security Agencies (AIVD & MIVD) have allocated their focus towards the cyber domain and have invested in this domain. Cyberterrorism as a phenomenon has a role within this. I do not know whether the taught was 'cyberterrorism is a problem and we need to focus on it'. I believe that the move towards focusing on the cyber domain was already ongoing and cyberterrorism is an exponent of the digitalising of daily life. Thus it is logical that Intelligence and Security Agencies focus on it and research it. Besides the move towards focusing on cyber within the existing agencies, the National Cyber Security Centre was established to exclusively focus on the cyber domain and coordinate the joint efforts of all ministries and government organisations.

Wouter Jurgens, Head of International Cyber Policy, Ministry of Foreign Affairs

Q: What is cyberterrorism, according to you? Also in light of the larger phenomenon of cybercrime and cybersecurity. Do you believe it to be an extension of 'regular' terrorism or do you think it is something totally different?

A: According to us, cyberterrorism is, if it exists at all, the achievement of kinetic effects through cyber. An attack with ICT-means. In that way it is similar to 'regular' terrorism, in methodology because the effect of an attack is the same: creating damage or deaths/wounded, as well as with the same of creating fear/anxiety in society. Many other countries see cyberterrorism as the use of internet for propaganda, recruiting, attracting financial resources by or for 'regular' terrorists or for terrorist activities, by people who some consider radicals and others name them proponents of the freedom of speech. In the international debate, which is for the Ministry of Foreign Affairs, of course the most important, there is a big difference between two sides. On the one hand, authoritarian regimes focus on cyberterrorism as the use of internet for freedom of speech, the spreading of ideology/ideas, recruiting and funding, on the other hand there are democratic countries like the Netherlands that consider cyberterrorism to have (kinetic) effects caused by cyber. In comparison to cybercrime, hacking, DDoS-attacks, the difference with cyberterrorism is not in the use of ICT, but in the intended effects of an attack. Creating fear through kinetic effects is the terrorist element. Cyber is the mean that is used to carry out the attack. It is a relevant mean, because we think that cyber has a wide reach. With relatively little means, it can have large effects. The element 'creating fear' or 'disrupting society' has a lot of potential. I call it potential, because until now it has not happened yet. The achievement of kinetic effects with the aim of creating fear or disrupting society we have not seen in the way of classical terrorism. What we do see is that state actors undertake actions that have these kinetic effects, but because they are state actors we do not call it terrorism. Other terms such as political pressure, destabilisation are used for these type of actions. Concrete examples are the attacks on Estonia, Georgia, and Ukraine now, whereby actors from other countries (proxies or states), as part of a broader political crisis, use cyber to apply (political) pressure. We do not see this as terrorism, but as the use of cyber for these purposes. If non-state actors , for example IS or other terrorists organisations, could apply this into practice, it would be cyberterrorism. Now that is not happening. Terrorists organisations use cyber for propaganda or to undermine the communication of others, for example the hack on TV5 Monde, hack of the NATO website. We do not view this as terrorism, but it is the deployment of cyber as part of their communication strategy, and in some way a strategy to intimidate. It is a grey area, and there could be a moment when the use

of cyber has kinetic risks and/or effects. We do take into account that it could happen. At the same time, the state has considerable capabilities to counter such actions. Until now we do not see that terrorist (organisations) have the organisation or resources to conduct such advanced attacks, but we should not exclude the possibility in the future.
Q: Do you believe that cyberterrorism is a threat to the Netherlands, to the state and/or also to society, for example public transport?
A: Until now we do not see it as a real threat, but as a potential threat in the future. If vital infrastructure and things that are important for society, such as telecommunications, power supply, internet providers, banking, are jeopardised or disrupted, it could potentially have very large destabilising effects. If terrorists would be able to break into these type of systems, it would be a real threat to the Netherlands. So not now, but potentially in the future.
Q: When became cyberterrorism a subject of conversation in the Netherlands, or cybercrime in general?
A: Not an exact moment, because this field is fairly new to me. In the Netherlands, cyber and cybersecurity gained a lot of attention in the media, and in politics and society, at the time of the hack on DigiNotar in 2011. It was not terrorism, but an incident in which the vulnerability of the Dutch society for cyberattacks became clear. Following this incident, a lot of measures were implemented, an increase of capabilities, the establishment of the National Cyber Security Centre. This was a catalysing incident. Before this incident there were others, but not in the Netherlands. Those drew attention, but did not result in a response. DigiNotar was a defining moment for the Netherlands. Since then, we have begun to realise that this vulnerability is growing because we are increasingly digitalising and because more and more of our daily of life, for example the 'Internet of Things', is going online. Our identity, our health care, everything is going digital. This will lead to an increasing worry about vulnerabilities. But if that is solely a worry for terrorists. At this moment, I think we worry more about state actors and cybercrime, than about terrorism.
Q: Which actors take part in the discourse of cyberterrorism in the Netherlands? Are these private actors, next to government actors?
A: I think that the private sector has been concerned about this much earlier than the administration and much earlier have invested in it (cybersecurity). Now there is a realisation that the private and public sector should work together. The chain is not a strong as the weakest link in the cyber domain, but there is the realisation that collective actions need to be taken to make the whole system more secure. In the field of awareness, detection, countermeasures, and evaluation. I believe that this is working well. The discourse is

consciously organised between public and private actors. The technical community, the people who control the infrastructure of internet itself, are closely involved. Not only nationally, but also with their international network. Since DigiNotar more and more ministries are involved, as well as private actors. What can be done to secure the system more without making it hard to access or hard to understand. Attention needs to be paid to rights, economic potential.

Q: Which ministries exactly are involved? The Ministry of Foreign Affairs, Ministry of Internal Affairs, Ministry of Defence, and the Ministry of Security and Justice seem logical to me, but are other ministries involved? Do these other ministries have their own tasks and programs or is it coordinated by the previously mentioned ministries?

A: The Ministry of Economic Affairs is also involved. These five ministries are the most important ones. The other ministries are, in their own field, working with ICT and cyber. For example, security plays a big role in the electronic patient file, or self driving cars need to be secure. So the subject is becoming more widespread, but these five ministries are the most involved. At the Global Conference on Cyberspace the ministries of Foreign Affairs, Defence, Security and Justice, and Economic Affairs were involved. The Ministry of Internal Affairs is mainly involved through the AIVD and was therefore not present as the Ministry itself. From within the Ministry of Defence the MIVD and the Defence Cyber Commando are also involved as separate departments.

Q: The MIVD at the Ministry of Defence does not talk about the term cyberterrorism. What do you think is the reason for this? The AIVD, on the other hand, does use the term cyberterrorism, for example in the yearly report; the potential is growing.

A: That is to some extent speculation. But if I see at how the MIVD, and the Ministry of Defence, approaches cyber then that is mostly at the role of cyber in their own operations, and the protection of their own ICT and infrastructure. Much less in a broader sense, like the AIVD does. The AIVD operates from their responsibility for the national security of the Netherlands and therefore looks at and researches a broad palette of threats. I think they have identified cyberterrorism, and I do believe as growing, but I do not think that it is one of their main priorities. I think they look at possible spill-over effects of traditional terrorist organisations who first use cyber for propaganda, but possibly also for disruption of society. They are attentive, but I have not seen a cyberterrorist attack yet.

Q: That is one of the difficulties of this research: to look at something that has not happened yet. That is one of my pitfalls, because it is about predicting something of which we might not know if it will ever happen and when potentially. This makes it difficult. It is hard to give

rendition to. What I found interesting was that at the Ministry of Defence, my interviewee said that at the moment we are going to talk about cyberterrorism and use the term as if it is a (possible) threat, we give exposure to terrorists in a way they might not have imagined themselves. Do you think that this is the case?
A: I think that we realise that we are broadly vulnerable. By becoming more digitalised, we become more vulnerable. In general, I think that there is a notion that the offensive party has the upper hand as opposed to the defensive party, because more power (and resources) can be aimed at a small part of the defence. This is not specific to cyber, but in the cyber domain it is even more the case. Also, I think we realise that not only states (actors) can do these things, but in the future also non-state actors. I do not think that the use of the term in a yearly report (of the MIVD) will lead to more actions by terrorists. We need to focus on how we deal with these types of threats and how we can make sure, in a proactive and reactive manner, that these things cannot and will not happen. From the perspective of the Ministry of Foreign Affairs it is very important to come to agreements between states as to what our responsibilities are for actions that are being carried out from within our own territory. Cyber has long been considered as a fifth domain that is essentially 'nowhere', where there is no sovereignty. Now we see that the taught is that cyber is a new phenomenon, but cables, servers, routers and such that are placed somewhere. States have a responsibility for what is carried out from within their territory. We are not there yet. It is about international judicial obligations, how it can be determined where an action/attack comes from, also called attribution. There are a lot of problems to be solved, but the idea is that if states come to agreements, states can be hold accountable on the basis of those agreements, also if proxies carry out actions/attacks.
Q: Does the existence of dark nets and Torrents complicates makes arrangements between states, because of the anonymity and attribution problems?
A: The main problem in cyber and with making arrangements is attribution. A lot of time and energy is put into doing something with this. Cybercrime is usually being researched through digital forensics. Cyber conflict deals with the problem of attribution. Problems can usually be assigned to the fact that cyber is very virtual, it is nothing until it is being used or deployed. In addition, it is not possible to count cyber weaponry, such as malware, as opposed to regular weaponry such as tanks or guns. The principle of 'trust, but verify' does not exist in the cyber domain. These two issues are the main problems that have to be dealt with. Regardless of these problems, a norm can be implemented between states to apply ordinance in order to have control over non-state actors.

Q: What are the foremost interests of those actors that see cyberterrorism as a threat to the Netherlands? I can imagine that for government (organisations) it is about letting people know that it is something we are researching. What would be the interest of private actors in arguing that cyberterrorism is a threat to the Netherlands?
A: It is a discussion that takes place in the public-private cooperation. From within the private sector I think it is about their primary work being dependent on ICT and cyber, or if they have obligations to supply products and/or services to consumers, governments or companies that can be disrupted by cyber. In the world of insurance there is a debate about risk estimation and vulnerabilities, and the connection to an insurance premium. I think that this is a strong incentive to worry about cyber. There is still the question of efficacy. I do think that it brings us to a debate about the quantification of these types of risks. The government, considering vital infrastructure, needs to worry about and have the responsibility to think of what is important to keep going in times of crisis. There are different layers, much like a panopticon, in which layer is most important. The most important layer directly infringes upon the daily life of the population. More thought is put into it in Hollywood, such as a movie in which all traffic lights turn to red, which is very destabilising. I think that there are also many vulnerabilities of which we are not aware of.
Q: Is commerce an interest that plays a role in the private sector? Private companies need to make a profit. Would this be an incentive to exaggerate the threat?
A: It would be possible, but I have not seen it. I have not seen that (cyber)terrorism is being exaggerated, been put on the agenda from this perspective. There is always a debate about the interests of organisations that invest in security, by naming insecurity. There is a fine line. I think that the risks that are being named in the field of cybersecurity are realistic. They are rather underestimated than overestimated. So my answer is no, they do not do this from a profit interest.
Q: What kind of role do concepts such as technological capital, legitimacy and authority, applied to those actors that see cyberterrorism as a threat, play in the discourse of cyberterrorism? So, if there is a contradiction between a government (organisation) and a private company, usually the government (organisation) is given more legitimacy. Does this play a role in how much influence an actor can exert on the discourse of cyberterrorism and can convince in this discourse?
A: It does play a role, but it is subject to changes. In the basis, especially in the Netherlands, but also in Europe, we realise that this is a domain in which cooperation is necessary. If only because, in the Netherlands, 95% of the internet infrastructure is not owned by the

government, but privately owned. There is a shared interest for joint action to improve security. Over the last year the government has taken on a controlling role for a number of core functions of society for which the government is responsible. Public order and security is something of which citizens expects from the government that there are some guaranties. The government needs to make an effort to make sure that citizens are secure. This is done in cooperation with the private sector, but there is a debate about where self-regulation ends and where the government is needed to set boundaries. The government is more inclined to set the boundaries, which also means initiating legislation, setting minimum standards. Some private companies are opposed, others want the government to do this (more). For example, because they want to have minimum standards which they have to meet and others as well, and they can thus be held accountable if they do not meet these standards. Until now I think this cooperation works well. I do think that one of the actors has more credibility than the others in this debate. But looking from the perspective of different roles and responsibilities, and very important costs. The National Cyber Security Centre is an organisation that the government must deliver to society, and for which the government is responsible. The reporting of incidents is a responsibility of private companies as well as of the government. They both need to be aware of each other what the vulnerabilities are. It is not good if they both become victims of the same attack, while if one warned the other the second disturbance could have been avoided or refuted. Responsible disclosure is something for which the government is developing legislation and measures, because companies do not report such vulnerabilities or attacks naturally, because they are afraid of reputation damage. If they are obligated to report, they cannot avoid it.

Q: Are technological capital and know-how/knowledge concentrated within the private sector or the government?

A: In general, in the private sector. They can switch more easily, of which commerce is often the motivation. But private companies also largely invest in reducing the risks for their primary work, either because they have to of because their survival or existence depends on it. Banks invest a lot in the security of their ICT systems, because otherwise clients do not trust them or do not use them. Similarly in many other sectors. But, and that is why the cooperation works so well, the government has specific knowledge about types of threats. The Intelligence and Security Agencies, the National Cyber Security Centre, the High Tech Crime Unit of the police all have specific knowledge on perpetrator profiles, attack profiles etc. They know what to pay attention to. They also have international networks to which private companies have no or much less access to, or only via the government (organisations). The exchange of

those types of information, on a confidential basis, through established procedures, is very useful for both sides. The government can deliver very specific services that the private sector cannot deliver or can only deliver if enormous investments are made.
Q: Are there specific measures been implemented, according to you, to counter the threat of cyberterrorism, or are they part of measures to counter cybercrime in general?
A: Measures in the area of cybersecurity focus on the resilience of systems against every type of attack, so also against cyberterrorist attacks. But I think the main concern needs to be about protecting vital infrastructure against breaches from anyone. State actors are more the focus than non-state actors. Those measures could potentially also be aimed at countering cyberterrorist attacks. Because we view it as a less advanced and less developed threat we focus less on this type of threat than on threats coming from states. But eventually the aim is to prevent anyone from accessing vital systems, for example the systems of a nuclear installation. The wall that is being built must keep everyone out. But the threat against vital infrastructure is viewed more coming from state actors than non-state actors.
Q: I have also talked to civil rights foundations, such as Bits of Freedom and Buro Jansen & Janssen, who are strong proponents of privacy and freedom. Are these measures a violation of privacy or are the employed means justified against the purpose of their employment? The purpose is to make the Dutch society and cyberspace more secure and in return citizens have to give up some piece of their freedom(s).
A: There are two aspects. I think that the cybersecurity measures are very defensive, such as on the level of individual ICT systems the countering of breaches. There is not as much overlap with the above mentioned debate. But when we try to be cyber aware, and be aware of which threats are coming our way, we are monitoring the net to see what is happening, This can be at the expense of individual freedoms, however, I do see that we are more concerned with the monitoring of patterns than the monitoring of individuals. The discussion about security and freedom, as we have also seen on the Global Conference on Cyberspace, is very important for the Ministry of Foreign Affairs. I think that we have good legislation and a good balance between national security and individual freedoms in the Netherlands. An example is that privacy is in the Constitution, but it is not absolute. It is possible to deviate from it, for example if it is a matter of national security, but it is only possible under specific conditions. There are very strong legal warranties in the Law on Intelligence and Security Agencies and when the police can act, that make it possible for citizens to object to the manner in which their privacy is being violated or not. The problem is internationally. Edward Snowden has covered it broadly. The government can talk to other countries and in international

partnerships, but citizens have very limited options, for example when the NSA violates their privacy they actually cannot protest or something. And this is an allied country, imagine if it is done by countries such as Russia, China, Iran etc. We do believe that there needs to be a balance between security and freedom. There is a debate about the expansion of the capabilities of the Intelligence and Security Agencies. We believe, together with these agencies, that this is only possible if the safeguards are also expanded or made stronger. We are under the impression that this is the case within this new law. I also think that the one enhances the other if it is organised well. Without privacy there is no security, and vice versa. I think they are more aligned than is sometimes portrayed. Bits of Freedom warns rightfully that a government that monitors everything, much like Big Brother, with security as motivation, is not good. We also do not approve that. There are also limitations necessary and the AIVD and MIVD also agree. That a government makes different choices than a NGO, such as Bits of Freedom, would prefer is part of the debate. That debate should take place in Parliament and in the media. Although the NSA has suffered from (reputation) damage, we are more aware of the vulnerabilities or our systems and how much cyber is integrated in our daily life.

Q: Maybe we do not even realise how vulnerable we really are with all the technology that surrounds us.

A: And how this vulnerability increases more and more in the future. Although I do think that the average citizen has to be more worried about Google than the NSA.

Q: Companies such as Google and Facebook do know almost everything about you. On the other hand, if you have nothing to hide, the Intelligence and Security Agencies will not have any interest in you.

A: I think so too.

Q: We have more to fear from within the private sector than from within the public sector.

A: Well, maybe not fear, but they arguably do know more about you than you do. But they also use that information in a manner for which you never explicitly gave permission other than agreeing with the Terms (of use). How the private sector uses or violates privacy we have to be aware of. Legislation is originally intended to protect citizens against too much power for the state, but we also have to look at too much power for the private sector.

Q: In my opinion, the private sector is growing in this area. Companies do know more and more about you. It is very intrusive that ads on Facebook display exactly what you did earlier that day or week. Maybe you do not have anything do hide, but it is noticeable.

A: This has been taken very far.

Q: It is not only about what you are doing now, but also about what you did in the past, even before you were on the internet yourself.
A: It is difficult to avoid. In the future your coffee maker is connected to the internet.
Q: More and more things are connected to the internet. Not only in your personal life, but also in society as a whole. Therefore vulnerability increases automatically.
A: Eventually you choose for it yourself. On average, a Dutch citizen carries 1.7 mobile devices with him that registers every move.
Q: Do you think the measures that have been taken to counter cybercrime (and cyberterrorism) are justified? Especially in light of the balance between privacy and freedom. This question is linked to my bachelor thesis which was about the Joint Sigint Cyber Unit. This Unit has been established, but the Law on Intelligence and Security Agencies has yet to be updated. The desire/intention is that it is also possible to tap cable-bound communication, which is not allowed by the current version of this law. Therefore, the revision is necessary. My focus in that thesis was if this Unit would already start by tapping cable-bound communication although it was not allowed by law yet, and what the effects on privacy would be. It was not easy to research. At university you learn to be critical, and my assumption that they would do this secretly. But through my research, especially after talking to Sebastian Reyn the head of that Unit at the time, I found that this was not the case. The warranties in the Netherlands are well taking care of, arguably better than I expected. After talking to some organisations, such as Bits of Freedom, you might get the impression that it is not properly arranged in the Netherlands, but actually it is, especially in comparison to other countries.
A: If it did go wrong, the system corrected it. For example, when journalists were being tapped, a judge has decided that the course of action was not correct, and therefore it is thus not allowed. Actually it should not happen, but if it happens, it is important that it not happens again. This proves that the checks and balances in the system work. But we need NGOs such as Bits of Freedom, and the media to unveil these events. This does not (always) happen automatically. This is also a issue of engineers. At the moment when more is possible, they want more. But if that is always justified, is an issue to consider. A report of the AIV (Adviesraad Internationale Vraagstukken) stated that if we want to be credible internationally, we have to 'practice what we preach'. Nationally, you do not need to do what you do not want other countries to do, internationally.