# Hacking in the Netherlands

## *Considerations of the Parties Involved*

Master Thesis Crisis and Security Management

Faculty of Governance and Global Affairs

Universiteit Leiden

Universiteit Leiden

Author: Matthijs Balder

Studentnumber: s1629271

E-mail: mkbalder@gmail.com

Supervisor: Jaap Reijling

# Table of Contents

# 1. Introduction

Society is becoming more and more digitized. The rise of the internet especially has had a tremendous impact on the way we live. Not only in our daily lives do we now depend greatly on technological advancements, the public as well as the private sector relies heavily on information systems. And while digitization has brought us many advantages, it has also made society vulnerable. Cybercrime and cyber-attacks are relatively new problems, but their significance cannot be denied. Hackers and other criminals employ an ever increasing variety of methods and tactics to commit crimes – abusing, disrupting, sabotaging or exploiting information and computer systems. The damage to society is considerable to say the least; estimations of the annual costs for the global economy in 2013 by cybercrime run between the 375 and 575 billion dollars (Center for Strategic and International Studies 2014). Notwithstanding its impact and cost, governments have been struggling to adequately respond to cybercrime.

At the same time, there are scores of actors trying to improve the security of information and computer systems. Apart from governments, there are companies and individuals dedicating time and energy into cyber security efforts. One of the ways in which they do so is through hacking. Although this might seem paradoxical, hacking can also be used to improve rather than abuse information systems. Hackers do so by finding flaws in information systems, often via the same methods used by hackers with criminal intent, and reporting rather than abusing them. Hence, the term 'hacker' can refer to both criminals, and individuals with good intentions. To discern between the types of hackers, an often used categorization by researchers and cyber security experts is to refer to hackers by the color of their 'hats'. Derived from old Western movies, researchers have coined the terms 'black hats', 'white hats' and 'grey hats'. In this regard, a black hat hacker is a hacker with criminal or illicit intent. Black hats use their hacking skills either for personal gain or to inflict damage to information systems or society at large. A white hat hacker is someone who uses his or her hacking skills to inform owners and operators of flaws in information systems. They are mostly driven by an ideological desire to improve cyber security. Finally, the grey hat hacker falls somewhere in between these two categories. This type was added later by researchers to address the category of hackers that are mainly driven by

economical gains, but refrain from intentionally doing harm. In the following chapters, the different categories will be discussed at length, but the introduction to this categorization of hackers here, serves to illustrate the diffuse nature of the concept hacking. Moreover, it shows that hacking does not have to be a bad thing. When hackers adhere to a certain set of 'ethics', many cyber security experts agree that hacking can be considered a viable means to increase cyber security. However, this does not mean that everyone agrees. Governments, companies and the general public often have a negative view of hackers, associating them with black hat hackers. The fact that the term hacker nowadays has a negative connotation, has to do with the significant rise in the number of black hat hackers in the end of the 1990s and the early 2000s and the reporting on it in the (Western) mass media. In doing so, the mass media has offered the general public a one-sided view of hackers. Hence, governments and companies still seem to be focused on discouraging hacking.

There are signs however that some governments are changing their perspectives on hacking. One of the main reasons why, is because governments have had little success in the prosecution of hackers and other cybercriminals (Mehan 2014, 68). The internet has often been compared to the American Wild West, a place of anarchy, where there are no rules or laws and no one to enforce them (Mehan 2014, 14). The internet has proven notoriously difficult to govern and secure, and as a result the cyber security industry is booming (Jardine 2015, 1). In 2013 alone, the private sector spent an estimated 58 billion dollars on cybersecurity, a figure that has rapidly increased in the years since (Center for Strategic and International Studies 2014). Governments are also increasingly investing in cybersecurity (Jardine 2015, 1). Especially in Western Europe and the United States, governments are employing or encouraging a wide variety of cybersecurity measures. Several states have invested in national cyber defense units, cyber crisis centers and other state-centered cyber security efforts (Computer Fraud and Security 2013, 3). However, some suggest that state-centered efforts such as cyber defense units are not enough to protect even the state's own information systems, let alone the information systems of society as a whole (Computer Fraud and Security 2013, 3). The mere scale of cyber security efforts needed to protect governmental information systems seems too daunting to be done by cyber defense units. On average, governments have many tens and even hundreds of thousands of websites

across all of their sub-entities (Computer Fraud and Security 2013, 3). Monitoring and securing all of them even with a team of several hundred cyber security personnel would be near impossible. Hence, ethical hacking is a promising potential means to improve cyber security, especially because it shifts part of the burden from governments to private companies and individuals.

The potential benefits of ethical hacking and responsible disclosure – as the act of ethical hacking is also called – are substantial. The discovery and potential exploitation of vulnerabilities in information systems by unauthorized, unethical, or criminal individuals can have a serious impact on the system operator and user in terms of increased costs and reputational damage (Mehan 2014, 70). By stimulating ethical hacking, the vulnerabilities in information systems are found and – hopefully – fixed before malicious hackers have the opportunity to find them. Nonetheless, there are experts who argue that the usefulness of responsible disclosure is questionable (Ozment 2005, 2). These experts believe responsible disclosure is ineffective in enhancing cyber security (Ozment 2005, 2-3). They claim that 'vulnerability hunting', as the search for flaws in information systems is also known, does not necessarily result in a more secure system (Ozment 2005, 2-3). Those favoring responsible disclosure disagree because they think there is a significant chance that the vulnerabilities will be rediscovered and abused by malicious actors.

Nowadays, most experts assume that responsible disclosure is useful at least to some extent. Illustrative of this assumption is the fact that several big tech companies, especially in the United States, have started 'bug bounty' or 'vulnerability reward' programs. These programs are published on companies' websites and are intended to stimulate ethical hackers to find and report specific vulnerabilities through responsible disclosure (Burningham 2016). For example, in 2015 Google paid more than two million dollars to approximately 300 ethical hackers through its Vulnerability Reward Program (Nava 2016). Apart from the big tech sector, many companies in the telecom, banking and IT sector have also started vulnerability reward programs (National Cyber Security Centre 2015, 7). In their wake, a steadily increasing number of companies in other sectors is following. These types of programs can be seen as an encouragement of ethical hacking. But how do companies actually view hackers? Are those that have started vulnerability

reward programs doing so reluctantly or have they embraced the concept ethical hacking? For policy regarding ethical hacking to be effective, it is paramount that the positions of private companies, governments and (ethical) hackers are determined.

To answer that question, Travis Hirschi's theory of social control theory might offer some insight. In 1969, Travis Hirschi published his book "Causes of Delinquency". In this book Hirschi, a famous criminologist, presented his take on what would become one of criminology's most influential theories: the social control theory (Weerman 1998, 13). Social control theory assumes that "delinquent acts occur when an individual's bond to society is weak or broken" (Hirschi, Causes of Delinquency 1969, 16). This means that people are more likely to resort to criminal activity when they have a weak bond with society. According to Hirschi, there are four different 'elements' with which people are connected to society: attachment, commitment, belief and involvement (Hirschi, Causes of Delinquency 1969, 16-26). Using Hirschi's social control theory will help understand how the parties involved think about hackers, and more importantly, help understand what they believe should be done to encourage ethical behavior on the one hand, and discourage delinquent behavior on the other.

A government that has acknowledged the potential benefits of ethical hacking is that of the Netherlands. The Dutch central government wishes to encourage and stimulate responsible disclosure, as it regards responsible disclosure as one of the most important cyber security tools (Nationaal Cyber Security Centrum 2013, 3). However, as in most countries, the act of hacking is still strictly forbidden in the Netherlands (National Cyber Security Centre 2015, 13). The law also does not allow for any exemptions regarding ethical hacking. Nevertheless, although it is still forbidden by law to engage in methods of responsible disclosure, the Dutch government will refrain from starting a criminal investigation "in case of legal rehabilitation between the discloser and the relevant company" (National Cyber Security Centre 2015, 13). In practice, this means that responsible disclosure is actually possible if ethical hackers adhere to a certain set of rules, which have been set out in a 'best practice' guide. In this guide, set out by the Dutch National Cyber Security Centre, the involved discloser and organization have been given a set of rules that both need to follow. But how should ethical behavior be encouraged? And how can illicit activity be discouraged? Moreover, do the three most important parties involved in hacking agree on

how this should be done? That is what this research will be about. The central research question of this thesis will therefore be as follows: *What are the considerations of the parties involved in hacking in the Netherlands – i.e. hackers, companies and governments – regarding the discouragement of illicit activity and the encouragement of ethical behavior of hackers, and how can these be explained?*

Finding an answer to this question will shed light on the considerations of the parties involved in ethical hacking, offering suggestions for the direction in which policy should be headed. To find said answer, empirical research will be done. First of all, the Dutch ethical hacking community will be consulted. What are their experiences regarding ethical hacking in the Netherlands, and what do they believe should be done to encourage ethical and discourage illicit behavior? Additionally, representatives of various companies will be consulted. What are their considerations? Finally, I will discuss the Dutch government´s policy on ethical hacking with representatives of government institutions. Why was the current policy shaped as it is and do they believe there are other possibilities to stimulate the use of responsible disclosure as a cyber security measure in the Netherlands? During this process, Hirschi´s social control theory will serve as a theoretical lens through which to assess the considerations of each party involved.

Regarding the relevance and benefit of this research, there are some remarks to be made. First of all, the added benefits to society are evident, because more ethical behavior and less delinquent behavior by hackers will reduce costs to society and improve the overall state of cyber security in the Netherlands. From an academic perspective, there are also gains to be made. First of all, little empirical research has been done into ethical hacking and responsible disclosure more particularly. Also, using Travis Hirschi's social control theory to research ethical hacking is something that has not been sufficiently done. Scholars have often used Travis Hirschi's later work on self-control theory, together with Michael Gottfredson, to explain the behavior of hacking, but his earlier classic theory has received far less attention. I believe social control theory can offer an interesting insight into ethical hacking, and vice versa. Because illicit hacking is a very particular type of delinquent behavior, it will be interesting to see whether Hirschi´s theory is capable of convincingly offering answers. It might be that Hirschi´s theory needs updating to deal with a phenomenon like illicit hacking, a type of activity Hirschi could not possibly have foreseen.

Alternatively, if it should prove to be suitable, it will reemphasize the prevalence of this classic criminological theory.

This thesis will be structured as follows. In the first chapter, I will define the key concepts used in this research and provide background information on ethical hacking where needed. Furthermore, the theoretical framework used for this research will be discussed, where the focus will be on Travis Hirschi's social control theory. In the second chapter, I will present my empirical approach and discuss the various sources that will be used as data. Chapter three will include a systematic analysis of the data and a discussion of the results. Also, it will include an answer to my research question. In the last chapter, I will offer a discussion of the limitations of the research.

# 2. Theoretical Framework

In this chapter, I will provide background information for this research. First, I will discuss the most important concepts, such as ethical hacking and responsible disclosure. Furthermore, I will review the existing academic literature regarding hackers and their motivation. I will discuss the prevalent theories to explain hacking behavior, before discussing at length what will be the core of my theoretical framework; Travis Hirschi's social control theory. More importantly, I will argue how Hirschi's social control theory can serve as a stepping stone to explaining how responsible disclosure as a cyber security measure can be stimulated.

## 2.1 Concepts

### 2.1.1 The (Ethical) Hacker

The act of hacking is generally considered illegal in many countries. But what exactly is hacking and what makes hacking 'ethical'? Generally speaking, hacking in today's world constitutes an "unsuccessful or successful attempt to gain unauthorized access or unauthorized use to a computer system" (Sharma y Dalal 2007, 35). But hacking did not always have a negative connotation, as the previous definition suggests. To fully understand who the ethical hacker is and what he does, we need to go back to the origin of computing and follow the historical trajectory of 'the hacker'. Because what the term hacker entails, depends greatly on the time in which the term is used. The fact that the term hacker nowadays has a negative connotation, has to do with the widespread emergence of malicious hackers in the end of the 1990s and the early 2000s and the reporting on it in Western mass media. The mass media has offered the general public a one-sided view of hackers and in doing so helped create a stereotype of the hacker as the socially inadequate criminal loner in his teens or end of his twenties (Fitch 2004, 8). In reality, this stereotype merely represents one of many categories of hackers described by scholars, called 'script kiddies' or 'cyber punks' (Fitch 2004, 6; Rogers 2005, 3).

Originally, the term hacker was used to describe a group of highly skilled computer programmers in the 1960s who mostly hailed from the universities of Berkley, Stanford and MIT (Sharma y Dalal 2007, 36). The early stages of hacking had absolutely nothing to do with illegal activities or cybercrime. The reason the early hackers hacked was to analyze and improve information systems (Leeson y Coyne 2005, 512). When the term was first introduced, hacking was used as a positive label for somebody extremely skilled in developing highly efficient, creative programs and algorithms (Bachmann 2010, 643). The rise of the internet expanded the concept of hacking to also describe the process of exploring and experimenting with computer networks (Pike 2013, 67). This began to change in the early 1980s, when personal computers were becoming affordable and the availability of the internet was becoming more widespread (Leeson y Coyne 2005, 513). Hackers start to realize the personal benefits that can be obtained by hacking computers and information systems. Not only individuals realize the possible gains to be made from illicit hacking activity. The most important hacking development of the 1980s is the emergence of 'hacker gangs' (Leeson y Coyne 2005, 513). In the United States, notorious hacker gangs like *414*, *Legions of Doom* and *Masters of Deception* break into computer systems on a large scale, including the system of the Los Alamos National Laboratory where nuclear weapons are developed (Leeson y Coyne 2005, 514). In 1984, the havoc that the hacker gangs wreak and the damage they inflict prompts the United States government to make it a crime to gain unauthorized access to computer systems (Leeson y Coyne 2005, 514). But hackers would only increase in numbers from then on. By the end of the 1990s, the damage that hackers inflicted would become more and more serious and costly. In 1995 for example, two Russian hackers steal roughly $10 million from a bank in a cyberattack (Leeson y Coyne 2005, 514). Although it had previously largely been limited to the US and Western Europe, by the turn of the century, hacking had started to spread across the globe.

The steady increase in the number of hackers was paralleled by an increase in the number of hacker categories. In 1988, researchers recognized three types of 'black hat hackers', as hackers engaging in illicit activity are often referred to; 'pirates', 'browsers' and 'crackers' (Sharma y Dalal 2007, 36). Pirates were the least skilled hackers and limited their activity to pirating software and violating copyrights. Browsers had a moderate technical ability, but did not

usually damage or copy files. The last type, the cracker, was very skilled and abused his technical abilities by copying files or damaging systems (Sharma y Dalal 2007). By 2005, researcher Marcus Rogers had constructed a more updated 'taxonomy' of hackers, in which he increased the number of hacker types to seven, categorizing each type based on both skill and motivation (Rogers 2005, 2). Categories vary from the 'Novices', who have very little programming skills and whose primary motivation is based on thrill and ego stroking, to the more dangerous and highly skilled 'Professional Criminals' and 'Information Warriors', whose motivation is respectively financial gain and patriotism (Rogers 2005, 3-5). Another category Rogers recognizes is the so-called 'Old Guard'. The Old Guard hacker appears to have no criminal intent and embraces the ideology of the first generation hackers, whose goal was to improve information systems (Rogers 2005, 4). However, Rogers also faults the Old Guard hackers for writing and publishing code and scripts for other groups in the hacker society to use (Rogers 2005, 4).

The Old Guard category can be seen as a forerunner of the 'White Hat' or ethical hacker. As was explained in the introduction, hackers can be categorized by the 'color of their hats'. The usage of the 'hat' analogy has become a very popular one among academics and experts in the cyber security field. Simply put, white hat hackers use their hacking skills for good, signaling weaknesses in information systems and offering insights on how to solve them. The white hat hacker has a few traits that separates him or her from the black hat hacker. First of all, the white hats work within the laws of hacker ethics, the essence of which is to do no harm (Fitch 2004, 2). They see the need to protect the public by actively discovering vulnerabilities or flaws in information systems and make the public aware of these issues (Fitch 2004, 2). However, contrary to hacktivists, white hats work together with the vendors or operators of information systems to solve the issue. White hats will allow the vendor or operator to fix the system and offers cooperation, even if it takes a long time to do so (Fitch 2004, 3). Nonetheless, even though the intentions of white hats are good, the unauthorized intrusion into computer or information systems that is required to discover the vulnerabilities, is still an illegal act.

Black hats use their skills for personal gains or political aims, their activities can be described as criminal, illicit and delinquent. Of the taxonomy by Rogers, all but the Old Guard can be categorized as black hat hackers. That leaves only the last category, the grey hats. This

category has been introduced by experts to account for hackers who seem to fall in between the previous categories. There is no complete agreement on what exactly constitutes a grey hat hacker (Sharma and Dalal 2007, 38). Definitions differ decidedly, some referring to grey hats as those who hack for economic gains, but refrain from causing harm, and others to those who report vulnerabilities, but without having asked explicit permission prior to gaining access (Sharma and Dalal 2007; Bachmann 2010). The important point however, is that classifying the actions of hackers is not straightforward.

So when is hacking ethical? According to the current widespread perception of ethical hacking, whether hacking is ethical has nothing to do with the legality of the act. If legality was a prerequisite for ethical hacking, all hacking would be unethical. What can make hacking ethical, is the motivation of the hacker and the harm he inflicts. The biggest differences between black hat hacking and white hat hacking, are that the ethical hacker's motivation is non-malicious and that the ethical hacker fixes or reports rather than exploits vulnerabilities in information systems (Bachmann 2010, 645). Furthermore, the historical record of hackers shows that while the concept of ethical hacking might be a new phenomenon, the idea of using hacking for good is not. The first hackers in the 1960s hacked to improve computer and information systems, and the Old Guard of the late 1980s did not intend to do harm either. In conclusion, the prevalence of the ethical hacker is not the rise of a new phenomenon, but the return of an old one.

### 2.1.2 Responsible Disclosure

Another concept that needs clarification is responsible disclosure. This section of this chapter will start by explaining what responsible disclosure exactly is. Furthermore, it will provide an explanation of what the main differences are between responsible disclosure and full disclosure. Finally, it will offer the definition of responsible disclosure that will be used for this thesis.

Responsible disclosure is now regarded by most experts in the field of cyber security as an invaluable cyber security measure. But what exactly is responsible disclosure? The act of responsible disclosure is closely intertwined with ethical hacking and white hat hacking. Simply put, responsible disclosure can be defined as "reporting the discovery of vulnerabilities or flaws

in information systems" (Knight 2009, 39). One of the key aspects of responsible disclosure is the cooperation and coordination of the vulnerability discoverer with the system operator. For a hack to fall under the category of responsible disclosure, the vulnerability must be conveyed to the system operator. Cooperation between the two parties concerned is essential, because this is where the difference lies between responsible disclosure and the closely related full disclosure. Full disclosure, contrary to responsible disclosure, does not involve the cooperation and coordination of the hacker with the operator of the system (Conrad 2012, 7). The philosophy behind full disclosure is to force organizations to improve their information system or software by publicly shaming them (National Cyber Security Centre 2015, 7). Instead of communicating the vulnerability to the system operator, the vulnerability is made public. The goal of the hacker practicing full disclosure, is to inform the general public or users of the information system of the potential risks they face due to the vulnerability (Conrad 2012, 8). The big difference is that in this scenario, the system operator is not informed beforehand about the vulnerability and has therefore not been given the chance to fix said vulnerability. The resulting consequences can be devastating. With the vulnerability made public, other hackers with malicious intent may learn of the vulnerability and consequently exploit it. In addition to the prior, there is another scenario that constitutes full disclosure, but that might seem like an act of responsible disclosure at first. There are some hackers who, when finding a vulnerability, do actually have the intention to coordinate with the system operator. They inform the system operator of the vulnerability, just like an ethical hacker would for responsible disclosure, but get frustrated when the flaw is not fixed quickly enough. Instead of giving the system operator the time to fix the vulnerability, the repair of which could take several months, they publish the flaw anyway (Fitch 2004, 3). Responsible disclosure means full cooperation and refraining from publishing anything without the consent of the system operator.

## 2.2 Hackers and Theory

The popular image of the hacker is one that is shrouded in mystery. Unsurprisingly, many criminologists and other academics have tried to unravel this mystery by attempting to pinpoint

who hackers are and what it is that makes them tick. The following section will provide a discussion of the various theories that have been used to understand the phenomenon of hacking, as well as give an overview of the empirical research that has been done thus far.

The explosive rise of computer hacking in the 21st century is a direct result of the widespread usage of computers throughout society and the advancement of computer-networking technologies like the internet (Xu, Hu y Zhang 2013, 64). Considering the damage hackers inflict on our societies and economies, it is obvious that their attempts must be thwarted. But who are these hackers and what is it that motivates them? Although the popular stereotype of the hacker as the clever, sinister and socially inapt loner in his early twenties is greatly oversimplified, it actually does include some elements that seem to be wide-spread traits of many in the hacking community (Bachmann 2010, 644). Empirical research about hackers is quite scarce, so the following is based on the findings of the few empirical researches into hackers that have been recognized by other scholars as reliable. Many of the researchers themselves acknowledge that empirical research is tricky for a number of reasons, the main being that surveys and interviews are considered the best way to collect information on hacker profiles and motivation (Leeson and Coyne 2005, 515). While surveys and interviews might normally be perfectly viable methods for empirical research, members of the hacking community are notorious for lying to journalists and researchers about how they work (Leeson and Coyne 2005, 515). Apparently, many hackers seem to "get a kick" out of lying to researchers (Leeson and Coyne 2005, 515-516). Nonetheless, there are some careful conclusions and generalizations that can be made.

First of all, research shows that, coinciding with the popular stereotype, indeed an overwhelmingly large portion of the hacking community consists of young, mostly college-age individuals (Xu, Hu and Zhang 2013, 643). Also, figures from practically all empirical researches show that the vast majority of hackers is male. Only a very small percentage of hackers is female, less than ten percent according to various studies (Leeson and Coyne 2005, 516). Apart from these two demographic classifications, hackers are believed to possess two general characteristics. The first widely agreed upon trait hackers are thought to have, is a "heightened need for cognitive challenges" (Bachmann 2010, 644). This trait is ascribed to them because

hackers are eager to learn about the "technical intricacies" of systems and processes, enjoy exploring them, and thrive on overcoming the technical challenges involved in circumventing their functions and limitations (Bachmann 2010, 644). The second characteristic is thrill-seeking. Hackers are believed to derive pleasure and excitement out of the thrill of overcoming barriers and gaining access to other systems (Bachmann 2010, 644). This characteristic especially applies to black hat hackers. The risks their illicit activities involve only increase the excitement and thrill (Bachmann 2010, 644). Hackers are more prone to engage in potentially risky behavior than members of the general population (Bachmann 2010, 652). In addition to these two generally agreed upon traits, research by Michael Bachmann shows that rational thinking is another characteristic of hackers (Bachmann 2010, 652). According to his empirical research, done through surveys at a well-known hacking convention, hackers tend to prefer rational thinking styles over more intuitive approaches (Bachmann 2010, 652).

In conclusion, the average hacker has some distinct characteristics. The average hacker is a young thrill-seeking, rationally thinking male with a propensity for cognitive challenges. Understanding the personality of the average hacker can help us understand his motivation, which will be discussed in the next section.

## 2.3 Motivation and Behavior of Hackers

Pinpointing what it is that motivates hackers and assessing their behavior, is something that scholars have been attempting to do for some time. A wide variety of criminological theories have been suggested to explain the motivation and behavior of hackers. This section will discuss the most important ones.

The most commonly used theories to study hackers are – unsurprisingly – criminological theories. Although most researchers studying hackers have used criminological theories as a lens for analysis, their research and assumptions decidedly differ. One of the theories most often used to study hackers is rational choice theory. Rational choice theory is used to explain the motivation and behavior of individuals in multiple fields of study, one of which is the criminological field. Despite not being the first to discuss rational choice theory as a way to

explain criminal behavior, D. Green and I. Shapiro in *Pathologies of Rational Choice Theory* convincingly argue the relevance of using rational choice theory to explain criminal behavior. According to Green and Shapiro, rational choice theory holds that individuals try to maximize expected value based on a utility function or scale when making decisions involving multiple options (Xu, Hu and Zhang 2013, 67). Moreover, individuals are able to rank the available options, and their decisions, preferences and tastes are relatively stable over time (Xu, Hu and Zhang 2013, 67). As discussed in the previous section, one of the propensities of hackers is to make rational decisions. In his empirical study using surveys to determine characteristics of hackers, Michael Bachmann discovered that rational thinking is indeed a trait that nearly all hackers have (Bachmann 2010, 652). However, as Bachmann's research also showed, rational thinking is hardly the only trait hackers tend to possess, suggesting that the rational choice theory is not sufficient to explain hacking motivation and behavior. Apart from rational decision making, Bachmann showed that risk taking was another trait most hackers had (Bachmann 2010, 652). Coincidentally, rational decision making and a propensity to take risk are two of the six characteristics that Travis Hirschi and Michael Gottfredson ascribe to individuals with an inclination to perform criminal activity in their influential self-control theory – not to be mistaken with Hirschi´s social control theory (Hirschi and Gottfredson 1990).

Bachmann therefore suggests in his article that empirical research should be done to include the other four characteristics Hirschi and Gottfredson recognize in their self-control theory. The theory assumes that the primary difference between criminals and normal individuals is a lack of self-control (Hirschi and Gottfredson 1990). This is because individuals with weak self-control are assumed to be more likely to respond to stimuli in their environment and as a result are seduced by the thrill and excitement of criminal acts (Hirschi and Gottfredson 1990). However, quantitative empirical research has found that self-control is not a convincingly strong enough predictor to explain hacking behavior (Xu, Hu and Zhang 2013, 67). The same research suggested that social learning theory is a much stronger predictor of hacking behavior. Social learning is another classic criminological theory, which assumes that individuals learn criminal behavior by associating with other criminals in personal and social groups (Xu, Hu and Zhang 2013, 66). In associating with criminals, individuals' likelihood to engage in criminal

activities increases as they imitate criminal behavior and justify such behavior by applying the norms and beliefs of the criminals. Many hackers are known to be active in hacking communities, so do hackers in fact start out by imitating the behavior of more experienced hackers? More than one research has been done into hackers and their communities. Not only social learning theory has been used in attempting to understand hacking behavior through online hacking communities, researchers have for example also used social organization theory and the imagined community theory (Jordan and Taylor 1998, 758; Skinner and Fream 1997, 501; Xu, Hu and Zhang 2013, 66).

There are some general conclusions that can be derived from these separate researches. First of all, individuals engaged in illicit hacking activity do seem to imitate each other's behavior, or at least share character traits that would suggest they are prone to such behavior (Skinner and Fream 1997, 505). Additionally, hackers do have personal and social ties with other hackers to some extent (Jordan and Taylor 1998, 759). However, these ties are never very deep or strong. Most hackers act alone, as there is little evidence of teamwork (Xu, Hu and Zhang 2013, 67). Furthermore, groups have no extensive histories, so one researcher describes hackers as acting as 'colleagues' rather than a social organization (Xu, Hu and Zhang 2013, 67). So although there are strong indications of an active hacker community, research suggests that the social ties between hackers are not very strong. The ties of hackers amongst each other are not very strong, but what about the social ties to society as a whole? Few research has looked at Travis Hirschi's influential social control theory to explain hacking behavior. The next section will discuss Hirschi's social control theory in more depth and explain why I believe his theory is fit to use as a theoretical lens to use for this research.

## 2.4 Hirschi's Social Control Theory

The previous section looked at some of the popular criminological theories used to research the behavior of hackers. In this section two things will be done. First, I will briefly relay the main assumption of control or bond theories in general. Thereafter, I will discuss at length Travis Hirschi's influential social control theory, focusing on the four elements that form its cornerstone.

Finally, I will explain how Hirschi's theory will be used as a theoretical lens to help formulate an answer to my research question.

When Hirschi published his social control theory in the book *Causes of Delinquency*, there were three dominant perspectives on delinquency and criminal behavior. The first perspective were the so-called 'strain' or 'motivational' theories, which held that legitimate desires that conformity could not satisfy would force a person into illicit behavior (Hirschi 1969, 3). The second perspective were the 'cultural deviance' theories. According to cultural deviance theories, individuals engage in criminal behavior because they conform to a set of standards not accepted by society at large (Hirschi 1969, 3). The third perspective were the bond or control theories, to which Hirschi's theory would also belong. According to the bond theories, individuals would commit illicit acts because their ties to the conventional order had somehow been broken (Hirschi 1969, 3). At the time, theories of crime would often contain elements of at least two of the main perspectives, but Hirschi believed the concurrence of one or more theories led to difficulties. Therefore, he presented his social control theory, decidedly choosing the perspective of the bond or control theories.

The main vantage point of control theories can be traced back to the 17$^{th}$ century philosopher Thomas Hobbes. In his seminal work *Leviathan*, Hobbes famously asks the question: "Why do men obey the rules of society?" (Hirschi 1969, 10). Hobbes believed all men to be evil and that a form of authority was needed to keep them in check. Control theorists also ask this question. Why is it that men do obey the rules of society? Control theorists expect deviant behavior, conformity to the rules is not expected and must therefore be explained (Hirschi 1969, 10). To explain conformity to the rules, control theorists assume that "delinquent acts occur when an individual's bond to society is weak or broken" (Hirschi 1969, 16). So people refrain from engaging in illicit activity when their bond to society is not weakened but normal or strong. This assumption also forms the cornerstone of Hirschi's social control theory.

There are several things that set Hirschi's social control theory apart from other bond or control theories (Weerman 1998). First and foremost are Hirschi's four 'elements of the bond'. The cornerstone of his social control theory, Hirschi argues that there are four elements that

determine the strength of the individual's bond to society: attachment, commitment, involvement and belief (Hirschi 1969, 16). So what do these elements pertain exactly?

### 2.4.1 The Four Elements

The first element, attachment, relates to the fact that it is our attachment to others that keeps us from resorting to deviant behavior (Hirschi 1969, 18). Hirschi argues that morality is not something that we magically possess. Instead, it is the internalization of the norms of society. To violate such norms is to act contrary to the wishes and expectations of other people (Hirschi 1969, 18). Hirschi also explains attachment as the "sociological counterpart of the conscience" (Hirschi 1969, 20). Should a person not care about the wishes of other people – in other words, if he is insensitive to the opinion of others – because he lacks attachment to them, he is not bound by their norms (Hirschi 1969, 18). Therefore, he will be free to deviate from desired behavior, or in other words, refrain from engaging in illicit activity.

The second element Hirschi recognizes is commitment. Commitment refers to the fact that sometimes men "obey the rules simply from fear of the consequences" (Hirschi 1969, 20). Commitment in this sense is the "rational component in conformity", as Hirschi puts it (Hirschi 1969, 20). If attachment is the sociological counterpart of the conscience, commitment is the counterpart of common sense (Hirschi 1969, 20). This means that if a person invests time and energy in a certain activity – for example getting an education, building a career or acquiring a good reputation – he would consider the negative consequences that deviating behavior will have for this activity. Assuming the individual is rational, he would outweigh the benefits of criminal behavior to the risks and costs. Moreover, when outweighing the benefits and costs, not only does the individual take into accord current activities, but also that what he hopes to obtain (Hirschi 1969, 21). In other words, ambition or aspiration can also play an important part in producing conformity. Hirschi offers "educational and occupational careers" as clear examples of things that individuals would not want to compromise. These are therefore strong influences on the avoidance of deviant behavior.

The third element in Hirschi's social control theory is involvement. This element relates to the fact that individuals have a limited amount of time to spend each day. The more involved or engrossed an individual is in conventional activities, the less time he has to engage in criminal behavior (Hirschi 1969, 22). The individual involved in conventional activities has to make time for appointments, deadlines, plans, etcetera, so there is decidedly less time to perform illicit activities. That is why many bond theorists advocate recreational programs, especially for youths (0Hirschi 1969, 22). Keeping them busy means they do not have time to resort to deviant behavior.

The final element of Hirschi's social control theory is belief. Control theory assumes that common values exist within society. According to Hirschi, the person whose behavior deviates, does not have a different set of norms or values but the same (Hirschi 1969, 23). So how come certain individuals violate the norms they believe in? Concisely formulated, Hirschi's answer to this question is that the people who commit illicit acts just have a more weakened belief in the norms and values of society. In other words, there is a "variation in belief in the moral validity of social rules" (Hirschi 1969, 26). The less a person believes he should obey the rules, the more likely it is that he will violate them.

In conclusion, there are four elements that explain the bond people have to society: attachment, involvement, commitment and belief. The first element, attachment, means that our attachment to others keeps us from engaging in criminal activity. The second element, commitment, relates to the fact that people do not want to jeopardize the investments they have made in conventional activities, such as education and careers. The third element, involvement, boils down to the fact that it is impossible for people to invest time into deviant behavior when they simply do not have the time due to other conventional activities. Finally, the fourth element, belief, entails that people with a weaker belief in societies norms will be more likely to engage in illicit activities.

### 2.4.2 Strengthening the Bond

While the previous section showed what it is that causes people to deviate, this section will show how Hirschi believes deviant behavior can be discouraged. How can the individual´s bond to society be strengthened? Again, this will be done for each of the four elements.

*Attachment*

For the first element, attachment, it is primarily important to note to whom the individual should feel attached. According to Hirschi, there are three main actors for whom the individual can feel attachment: parents, teachers and peers (Hirschi 1969, 85). As these examples would suggest, Hirschi has looked mostly at male adolescents, because that is the group which relatively sees the most instances of deviant behavior (Hirschi 1969, 27). This corresponds with the profile of the average hacker, since the vast majority is male and most are in their late teens or early twenties (Bachmann 2010, 644).

Parents play an important role in producing conformity (Hirschi 1969, 85). Hirschi notes that the fact that delinquents are less closely tied to their parents compared to non-delinquents is one of the best documented findings of criminological research (Hirschi 1969, 85). The reason why, according to Hirschi, is that the "emotional bond between the parent and the child presumably provides the bridge across which pass parental ideals and expectations" (Hirschi 1969, 86). If the child is alienated from the parents, he will not learn and adopt their moral rules (Hirschi 1969, 86). In other words, if the bond to the parent is weakened the probability of delinquent behavior increases, and if the bond to the parent is strengthened the probability decreases. How does this translate into something more tangible? How does the adolescent´s attachment to his parents translate in a diminished occurrence of deviant behavior? According to Hirschi, children are less likely to commit deviant acts if they ask themselves the question: "What will my parents think?" (Hirschi 1969, 88). His empirical research shows, that the children that ask themselves this question are the ones whose parents know where they are and what they are doing (Hirschi 1969, 88). This means that the more the parents of children are aware of what their children are up to, the less likely it is the children will commit deviant acts. Another

factor is the level of intimacy of communication between the adolescent and his parents (Hirschi 1969, 90). The more intimate their level of communication – i.e. the more they share – the less likely they are to commit deviant acts.

Another actor towards whom adolescents feel some form of attachment is school. That is to say, Hirschi notes that there is a link between the performance of students and the likelihood they commit a crime (Hirschi 1969, 115). The better a student does in school, the less likely it is that he has committed a deviant act (Hirschi 1969, 115). According to Hirschi, this does not necessarily have to do with the student´s intellect but with the question of whether a student is academically competent (Hirschi 1969, 115). The academically competent student is more likely to do well in school and therefore more likely to enjoy school (Hirschi 1969, 115). The more the student likes school the less likely it is he shows delinquent behavior (Hirschi 1969, 115). Hirschi confirms this with empirical data, by showing that students who said they dislike school are more likely to have committed delinquent acts (Hirschi 1969, 121). Also, the attachment students feel towards their teacher is relevant (Hirschi 1969, 123). When asked whether they care what their teachers think about them, those who said they cared the least were those that were the most likely to engage in delinquent behavior (Hirschi 1969, 123). For their bond to be strengthened, students must be academically challenged and be made to care about what their teacher thinks about them.

The final actors Hirschi identifies to whom adolescents feel attachment are their peers. Hirschi notes that delinquents are very likely to have delinquent friends, while non-delinquents are very unlikely to have delinquent friends (Hirschi 1969, 136). Companionship is one of the most telling forces in male delinquency and crime (Hirschi 1969, 136). However, the question is whether delinquent tendencies are imposed on the individual by the group or whether the individual tends to seek out friends “whose activities are congruent with their own attitudes” (Hirschi 1969, 159). Hirschi’s empirical data seems to suggest the latter. Therefore, Hirschi concludes that the individual´s conformity or non-conformity affects his choice of friends rather than the other way around (Hirschi 1969, 159).

In conclusion, there are three types of actors to whom adolescents feel attachment, the parent, the school or teacher and their peers. Parents can decidedly influence the behavior of

their children. Hirschi´s data suggests that the more the parent is involved in his or her child´s life and adequately communicates, the less likely it is the child will show deviating or delinquent behavior. Regarding the school and teacher, academic competence seems to directly influence the likelihood the adolescent will engage in deviating behavior. Because those students who are challenged at school are more likely to enjoy school and subsequently show less likelihood to delinquent activity, academically challenging students is quite important to avoid deviant behavior. Regarding the teacher, if students do not care what the teacher thinks about them, they are more likely to engage in delinquent behavior. Finally, students can feel attachment to their peers. However, Hirschi´s data shows that there is no evidence that peers influence deviant behavior. Rather, students select their friends on the basis of pre-existing levels of conformity or non-conformity.

*Commitment*

Commitment, the second element, refers to the conformity of rules by individuals simply out of fear of the consequences that result from deviant behavior. If a person invests time and energy in a certain conventional activity, for example in education or in a career, he would consider the negative consequences that deviating behavior will have for this activity (Hirschi 1969, 21).

Hirschi found that regarding education, there is clearly a link between aspirations and delinquent behavior. The higher the individual´s aspirations for education, the less likely it is he will commit delinquent acts (Hirschi 1969, 171). The same goes for the aspirations of a high-status occupation. Again, the higher the aspirations, the less likely it is the student engages in delinquent activity (Hirschi 1969, 182). The same is true for the expectations others have for the students. The higher their expected occupational level, the less likely it is they commit delinquent acts (Hirschi 1969, 183). In conclusion, Hirschi finds that there can be little doubt that “the educational and occupational expectations of delinquents tend to be low” (Hirschi 1969, 185). How does this translate into a possibility to strengthen the bond of the individual with society? Stimulating the aspirations for either educational or occupational careers can lessen the

likelihood of delinquent behavior. Hence, the prospect of either admittance to a higher form of education or a higher occupational status can discourage deviant behavior.

*Involvement*

Of all of Hirschi´s elements of the bond, involvement is the most obvious. Simply put, when someone is mowing the lawn or playing sports, he is not committing delinquent acts (Hirschi 1969, 187). Therefore, the translation of this idea into actual strengthening of the bond is quite simple: offer recreational programs or other activities to keep individuals engaged (Hirschi 1969, 188). However, it is important to note that Hirschi himself highly doubts whether involvement actually stimulates conformity. His empirical research has not been able to validate the link between involvement and lessened likelihood of delinquent behavior. As a reason, he offers the suggestion that actual time spent performing delinquent acts is very limited (Hirschi 1969, 188). It does not take many days, not even hours, to commit delinquent behavior. However, he suggests that further research is needed to be able to say so decisively, which is why the notion of involvement is still included.

*Belief*

According to Hirschi, almost everyone in society has the same set of norms (Hirschi 1969, 26). People who commit illicit acts just have a more weakened belief in the norms and values of society. Hence, the less a person believes he should obey the rules, the more likely it is that he will violate them.

There are various ways in which the belief in norms and values can be translated into more tangible indicators. The first is respect for the law. It might not be surprising, but Hirschi found that those who engage in delinquent activity have significantly less respect for the law than those that do not (Hirschi 1969, 202). They have less respect for law enforcement agents and other conventional authority figures, and are more likely to believe that it is alright to circumvent the law if you can do so without getting caught (Hirschi 1969, 202). The second, is due to the fact

that individuals that commit delinquent acts often find ways to justify their behavior. Hirschi calls these justifications "techniques of neutralization" (Hirschi 1969, 205). Although most respondents in Hirschi´s research agree that most criminals should be blamed for the things they have done, they seem to think that this not applies to themselves (Hirschi 1969, 206). Hirschi found that most individuals that commit delinquent acts seem to believe they themselves are not to blame for delinquent acts. There are various other techniques of neutralization. Denial of injury, which entails the individual believes that when they commit delinquent acts they do not cause any serious harm (Hirschi 1969, 208). Denial of victim, which crudely put boils down to: "suckers deserve to be taken advantage of" (Hirschi 1969, 209).

Although now it is clear what indicates a weakened belief in norms and values, that still does not explain how the bond to society can be strengthened. How can the belief in norms and values by individuals be increased? For one, a stronger belief in norms and values can be obtained through respect for conventional authority figures.

## 2.5 Analytical Framework

The obvious question is how these elements can help answer the main research question.

In order to be able to answer the main research question, we must understand what the three parties involved in hacking in the Netherlands – i.e. government, hackers and companies – believe can discourage illicit hacking activity on the one hand and encourage ethical behavior on the other. In other words, along which of the elemental lines of Hirschi do the various actors believe action should be taken. According to Hirschi, it is the weakening of the bond with society that causes deviant behavior, in this case, criminal activity in the form of hacking. Hence, social control theory means that strengthening the hacker's bond with society will decrease the likelihood of illicit behavior. In this sense, ethical hacking in the form of responsible disclosure, whether by white or grey hats, should be considered as 'normal' behavior, because it corresponds with the values and ethics of society. Deviating behavior would be 'black hat hacking', any form of hacking that is done with malicious intent and actually does harm to society. Following Hirschi's logic, we can assume that ethical hacking can be stimulated as a form of cyber

security if the hacker's bond to society is strengthened. From this statement the question that logically follows is: which actions do the parties involved believe should be taken to either discourage illicit activity or encourage ethical activity? Does the action imply the strengthening of the hacker´s bond with society? For this, we need to look at Hirschi's four elements and the way these elements can be stimulated to strengthen the bond.

# 3. Research Design

This chapter serves to explain the methods I will use to perform my research. Moreover, it will explain why I made certain choices in the way I conducted my research. This chapter is structured as follows. Firstly, I will present the methodology used in this research. Secondly, I will discuss how and why certain data was collected. Finally, I will present the semi-structured interview methodology used to conduct said interviews.

## 3.1 Methodology

To successfully offer an answer to the main research question, research will have to be done. This section will offer clarification on the methodology used to conduct this research. It will answer the question on why I chose the selected methodology.

For various reasons, a qualitative research method has been selected for this research. Foremost, this type of method allows for an in-depth analysis of a situation, which will lead to a better understanding of a certain case (Flyvberg 2006, 227). Qualitative research has a few traits that make it a more fitting method for this particular research than quantitative. First of all, as indicated, qualitative methods are especially suitable when examining one case, which in this research is the Netherlands (Newman and Benz 1998, 9). The Netherlands has been chosen as a case study for two reasons. The first one, quite obviously, is accessibility to data. Especially for the conduction of interviews, the Netherlands has a huge practical advantage over other countries. The second, is that the Dutch government is known to actively engage in topics regarding cyber security, including ethical hacking. Furthermore, as opposed to many other countries including several in the European Union, the Netherlands is one of the few countries to allow at least some form of ethical hacking. Researching and comparing multiple cases – i.e. countries – would have been very interesting and would have undoubtedly increased the validity of eventual conclusions, but given the time period this would have been unfeasible. Second, there is little readily available data to allow for a more quantitative approach. There are no large troves of data reflecting held beliefs of the parties involved in hacking in the Netherlands.

Therefore, a statistical analysis would not be a suitable way to approach this subject. Rather, data will be collected through three distinct qualitative methods, to enable triangulation. The next section will elaborate on these three methods.

## 3.2 Data Collection

This section will discuss the way in which data was collected. Also, it will offer argumentation for the selection of the actors chosen to be interviewed.

The three methods used to enable triangulation are desk top research, document analysis and interviews. The desk top research was predominantly used in the first phase. It served as a means to study the available literature, both on Hirschi and hacking. Hereafter, documents were analyzed to discern a 'paper reality´. What does the available documentation on or by the NCSC, companies and hackers tell us about the situation in the Netherlands? Does it suggest anything about the way in which the various actors regard hackers and ethical hacking? Subsequently, interviews were conducted to supplement and juxtapose this paper reality.

The interviews were conducted according to a semi-structured approach. This means that questions were prepared in advance, but the participants were encouraged to discuss topics they themselves thought were relevant. As Galletta puts it, the benefit of a semi-structured interview is that information can be gleaned from the interviewees´ narrative as it unfolds (Galletta 2012, 77). However, a proper preparation allows for further inquiry into topics touched upon in the participants´ narrative. It is the task of the interviewer to make sure that what is discussed is still relevant to his research (Galletta 2012, 77).

Representatives of the three parties involved have been interviewed. Interviews would follow a semi-structured approach. For the government, the first and most obvious actor to be interviewed is the NCSC. The NCSC is the organization within the Dutch Ministry of Safety and Justice that creates and executes policy regarding cyber security in the Netherlands. For example, they published a document in which they present the Dutch responsible disclosure policy (NCSC 2015). The person I interviewed is a security researcher for the NCSC who specializes in ethics in cyber security. Additionally, someone from SURF, an ICT-cooperation organization for education

and research has been interviewed. The reason is three-fold. First, as an institution responsible for innovation in ICT, they might have a strong opinion on the hacking community and whether they see a future for ethical hacking as a cyber security measure. Second, it is useful to determine the opinions of those within a government institution apart from that of the NCSC. Finally, due to the fact that SURF has a responsible disclosure policy, they are on the receiving end of the responsible disclosure policy.

Deciding which companies to approach with an interview request was more challenging. Ideally, interviewees would be representatives of a diverse group of companies, covering different sectors and sizes. In reality, this proved too time consuming. However, I did want to include companies from more 'experienced' sectors, such as banking or telecom, and sectors with less obvious experience, such as retail. Furthermore, companies were only selected if they had a responsible disclosure policy, because this indicates a probable prior experience with hackers, whether black, grey or white hats. The companies from which representatives were interviewed are Intergamma B.V. and Moneybird. The former is mostly known for its retail company Gamma. Important to note, is that the person that was interviewed was responsible for online security. They therefore were well aware of cyber security related issues, the relevance of which will be touched upon later. The second company, Moneybird, is a relatively new company which specializes in providing online business services for thousands of companies. According to the company itself, they qualify as a semi-financial organization. Because they store a lot of personal data, online security is of great importance. The person I interviewed was one of the co-founders/directors. Due to a background in engineering and web development he did possess a lot of knowledge on cyber security.

The final group that would be interviewed were hackers. For various reasons, I only interviewed ethical hackers. First of all, establishing contact with black hat hackers would be very hard as I did not have any contacts in that group. As several researchers have noted, black hat hackers are very reluctant to share information with researchers (Leeson and Coyne 2005, 515). Secondly, researchers note that even if you manage to talk to black hats, there is little guarantee that they will tell the truth (Leeson and Coyne 2005, 515). According to some, black hat hackers get a kick out of deceiving researchers (Leeson and Coyne 2005, 515-516). Hence, attempting to

establish contact with black hat hackers without knowing any seemed like a too daunting and time consuming process with little chance of success. Instead, I decided to focus on talking to ethical hackers. Establishing contact with them proved to be much easier. Moreover, I presumed some ethical hackers might have a background as a black hat, or at least know sufficiently about them. The hackers I spoke to, could technically be categorized as grey hats. They work for cyber security companies and make a living out of their work. However, as will be discussed later in more detail, some disagreed with the term grey hat hacker. The first person that was interviewed, was not actually an ethical hacker but will nonetheless be placed in this category. His name is Jan Martijn Broekhof, the director of a company called Guardian360, which specializes in cyber security. Although not an ethical hacker himself, he employs many and has a good understanding of the hacking scene in the Netherlands. His company mainly has semi-governments, municipalities and medium sized businesses as customers. The second person is Daniel Niggebrugge, an ethical hacker who works for Fox-IT. Fox-IT is a very well-known cyber security company in the Netherlands. It has recently been bought by a British firm for a sum of 133 million euros (Hijink 2016). Daniel Niggebrugge spoke on personal title, not on behalf of the company. The third in this category is Edwin van Andel. A well-known figure in the hacking community, he started hacking in the early eighties. Since then, he has worked for various companies. Currently he works for Zerocopter, a company that specializes in the development of bug bounty programs.

## 3.3 Data Analysis

There are several remarks to be made on the analysis of the data that has been collected. First of all, before the gathered data was analyzed, it had been divided into three distinct categories: government, private sector and hackers. This categorization does not concern the topic or subject of the collected data, but the source. This has been done to discern the beliefs of the three parties involved regarding ethical hacking in the Netherlands and to subsequently place them along the elemental lines of Hirschi. Although this may seem obvious, one of the organizations that has been interviewed is a bit harder to categorize. This concerns the organization SURF, an 'ICT-cooperation organization for education and research' in the Netherlands. In this organization,

Dutch universities, colleges, university medical centers and research institutions cooperate to stimulate innovation in ICT. Because it represents mostly public sector institutions, it has been categorized as a governmental organization.

When analyzing the collected data, I tried to look for thematic patterns emerging. Within the category groups, I tried to discern coinciding and overlapping beliefs amongst the participants. Because quality is more important than quantity when using a qualitative research approach, every piece of data was carefully scrutinized (Galletta 2012, 124). Hirschi´s social control theory was used as a lens through which the data was observed.

This chapter offered an insight in the way this research has been executed. It showed why certain choices were made regarding research method, data collection technique, selection of participants for interviews and data analysis. The next chapter will offer the main analysis of this research.

# 4. Analysis

This chapter will offer the main analysis of this research. Hirschi's social control theory will be used to examine the collected data. However, before going into the chapter's overall structure, it is important to note that not all of Hirschi's theory was discernable in the data. Certain features simply did not appear, so they will not be discussed. First of all, concerning the element attachment, the level of intimacy in communication between parents and children did not appear to be relevant. Second of all, regarding the element belief, techniques of neutralization did not seem to be relevant. Although, as will be seen, the element involvement played a very marginal role to say the least, because it is one of the four core elements, it will be discussed for each of the parties involved.

That being said, the structure of this chapter is as follows. The chapter has been divided into three main parts. Each part will discuss one of the main parties involved in hacking in the Netherlands. First, the group hackers will be discussed. What are this group´s considerations regarding the discouragement of illicit hacking on the one hand and the encouragement on ethical hacking on the other? Along which elemental lines of Hirschi do they believe action should be undertaken? After the hackers, the same questions will be asked for companies. Finally, the same will be done for the government. Subsequently, each section will be divided into two subsections: the first will discuss the paper reality for each group whilst the second will draw upon the data collected through interviews.

## 4.1 Considerations of Hackers

This chapter will offer insight into the considerations of hackers regarding the discouragement of illicit activity and the encouragement of ethical behavior of hackers. The first section will offer an overview of the paper reality, for which various documents have been scrutinized. The second section will discuss the data gathered through interviews with ethical hackers.

### 4.1.1 Paper Reality

This section will discuss the paper reality of the considerations of hackers. First, it will offer a description of the hacking community in the Netherlands. Briefly, it will discuss its history and determine its size. Hereafter, an attempt will be made to discern whether information gleaned from documents offers insights into the considerations of the hacking community, focusing on those of ethical hackers. Along the lines of which of Hirschi´s elements can these considerations be placed?

*A Brief History*

In the second chapter, a short overview of the historical trajectory of hackers has been given. The vast majority of this history has taken place in the United States, where the prevalence of supercomputers as well as personal computers predated that of Europe and thus the Netherlands (Pike 2013, 67). However, the Netherlands does have its own history regarding hackers. Supposedly, the first big hack in the Netherlands occurred in 1985 when two hackers managed to hack PTT, the Dutch state telephone company (Dasselaar 2008, 29). There were not many hackers in those early days, and although some of them received minor jail sentences and fines, their actions are better described as mild hacktivism rather than serious criminal activity (Dasselaar 2008, 30-31). The Dutch ´hacking´ magazine *Hack-Tic*, run by two prominent members of the hacking community, is mostly filled with anti-establishment rhetoric (Dasselaar 2008, 30). It is hard to categorize individuals in the early hacking community as either black, grey or white hat, as they regularly show traits of either or all types. An example hereof is the fact that the two hackers in charge of the magazine end up starting the internet company XS4ALL, which they ran in cooperation with their former ´enemy´ PTT, to which they end up selling their company in 1998 (Dasselaar 2008, 32). In about that same period, a new generation of hackers emerges in the Netherlands (Dasselaar 2008, 32). This generation of hackers more resembles the ‘scriptkiddies´ and cyberpunks also described in chapter two. After a few years of less serious cyber vandalism, in 2004, a group of hackers sabotages various government websites through Distributed Denial of Service (DDoS) attacks, which prompts the police to take action (Dasselaar 2008, 32). This

period sees a dramatic increase of more serious damage done by hacking, definitively introducing hacking to the general public and placing it on the political agenda.

*Hackers in the Netherlands*

What does the available documentation on hackers in the Netherlands tell about their community and the way they view themselves? First of all, determining the exact size of the hacking community in the Netherlands has proven to be difficult. One source suggests there are approximately 200 skilled ethical hackers currently operating in the Netherlands (Broekhof 2015, 122). Pinpointing the total amount of hackers in the hacking community is harder, because it is unclear how many black hat hackers are active in the Netherlands. Most indications suggest that the number of skilled black hat hackers operating in the Netherlands is quite small (Van 't Hof 2014, 35). Reports indicate that there are a lot of people involved in cybercrime, but a hacker is not the same as a cybercriminal. Hackers can be cybercriminals, but cybercriminals do not necessarily have to be hackers. Also worth mentioning here is that hacking is an international phenomenon. The lawlessness and cross-border nature of the internet, means hackers can operate from virtually any place, making it even harder to determine exactly how many operate in the Netherlands.

*Considerations*

When determining the considerations of hackers regarding the discouragement of illicit or encouragement of ethical behavior only the beliefs of ethical hackers will be taken into account, since public accounts of black hat hackers are notoriously difficult to encounter. However, reliable data on the beliefs of ethical hackers is also quite hard to come by. Most information available is anecdotal rather than systematic. It is therefore questionable whether there is sufficient reliable documentation. It is unquestionable however, that ethical hackers see their own profession as beneficial to cyber security and society as a whole (Van 't Hof 2015, 28). There are examples of ethical hackers voicing their opinion on the matter. Often, they argue that there

are not enough ethical hackers operating in the Netherlands. They believe having more ethical hackers in the Netherlands would be quite desirable (Van 't Hof 2015, 29). For example, one hacker told a news agency he believes that children should be taught coding in school, to resolve the shortage of professional ethical hackers in the Netherlands, which he claims there is (Security 2015).

### 4.1.2 The Hacking Community

This section will discuss the findings of the analysis of data collected through the interviews with ethical hackers. It is structured as follows. First, a brief introduction will be given, describing how the interviewees view the hacking community in the Netherlands. Hereafter, the considerations of the interviewees will be examined and regarded through the lens of Hirschi´s theory. Along which of the elemental lines do the ethical hackers believe action should be taken to encourage ethical behavior or discourage criminal activity?

The account of the three respondents regarding the hacking community to a significant extent corresponds with the account gleaned from the literature and documents. All three respondents describe a small, tightly-knit community, where most people know each other (Broekhof). None of the interviewees could name an exact number of the total amount of hackers in the Netherlands, but Broekhof believed there were about 200 skilled ethical hackers (Broekhof). Regarding the amount of black hats, the respondents were less sure of the numbers active in the Netherlands, but they believed their numbers to be much smaller than that of ethical hackers. According to Broekhof, the black hat community in the Netherlands is a subculture of the general hacking population (Broekhoef). Important to note here is that they do discern between black hat hackers and cybercriminals, whom they do not see as the same. As indicated previously, black hat hackers are cybercriminals but cybercriminals are not necessarily hackers. Moreover, they describe the hacking community as very diffuse.

As said, the community is tightly-knit and the behavior of individuals does not necessarily have to be restricted to either black or white hat behavior. Illustrative of this notion is that Niggebrugge says that the distinction between white, grey and black hats is pointless, because

“in this world most things are grey” (Niggebrugge, 8). Niggebrugge remarks that he has done things when he was younger which he regrets and would now never do, although he did not do anything specifically illegal. Additionally, when asked whether he has always been an ethical hacker, Van Andel admits that he has done things that in retrospect might not have been ethical (Van Andel). He agrees that it is a very diffuse world, where things are quite exciting and mistakes are easily made, but he believes that as long as you do not intend to do harm your actions should not be seen as unethical (Van Andel). Niggebrugge´s account confirms the sometimes grey line between ethical and unethical behavior, saying that especially individuals in their teens and early twenties have a different take on ethics than older people (Niggebrugge). But what then should be considered as ethical hacking?

The answer the respondents give to this question shows the difficulty of formulating a clear cut definition. Each interviewee has a slightly different take on ethical hacking, but there are some similarities. As Van Andel noted, he believes that as long as hackers do not intend to do harm with their actions their behavior is ethical. He believes the intention of the hacker is key in determining whether their behavior is ethical. This is also what Niggebrugge believes. He thinks that hackers can have good or bad intentions and that this is what sets apart the ethical hacker from the black hats. Van Andel adds that when hackers show criminal behavior, that is when their actions are unethical (Van Andel, 11). Broekhof, after being asked about the term ethical hacker, says that maybe the term hacker should be gotten rid of completely (Broekhof, 3). He thinks the term is too vague (Broekhof, 3). Black hat hackers should just be called cyber or computer criminals, nothing more nothing less. Furthermore, their accounts underscore the contested notion of several of the concepts used. Niggebrugge for example said that he had given up on the whole discussion on the differences between the terms ´hacker´ and ´cracker´ (Niggebrugge, 10). Although he did not say so explicitly, this suggests that he is bothered by the negative connotation the term hacker has gotten.

Summarizing, there are several conclusions to be drawn from the previous. First of all, ethical hackers view their own community as small and tightly-knit. There are more ethical hackers than black hats and the black hat community is a subculture of the general hacking population. Second, having said that there are more ethical hackers than black hats, categorizing

them as either white, grey or black is problematic. As Van Andel and Niggebrugge note, ethical hackers make mistakes they later regret, suggesting that ethical hackers do not always behave ethically. Finally, even for ethical hackers themselves it is hard to pinpoint what exactly sets apart ethical hackers from black hats. However, they believe ethical behavior closely corresponds with the individual´s intention. As long as the hacker intends to do well, his actions are deemed ethical.

### 4.1.3 Thinking along Elemental Lines

Now that we know how ethical hackers view the hacking community, we will look at the way they think ethical behavior can be encouraged and criminal activity discouraged among hackers. To do so, we will use Hirschi´s four elements to discern whether their held beliefs corroborate with any of the elements of Hirschi´s social control theory. First, this will be done for attachment, followed by commitment, involvement and finally belief.

*Attachment*

As was explained in the second chapter, the first element, attachment, relates to the fact that it is our attachment to others that keeps us from resorting to deviant behavior (Hirschi 1969, 18). Should a person not care about the opinions of others, he is not bound by their norms and deviates from them more easily (Hirschi 1969, 18). Following Hirschi´s theory and findings, this category should be subdivided into three groups of actors: parents, school and teachers, and peers. Do the respondents indicate anything that would suggest they think along the lines of this element? This section is divided into three parts, one for each group of actors.

The first actors to which a hacker might feel attachment are his parents. According to Hirschi, if parents are more involved in the activities of their children, the less likely it is they will resort to deviating behavior. Do the respondents show any indication that they think this could work? Although quite implicit, Broekhof seems to believe so. He references being “raised decently” as a factor that leads to ethical behavior amongst hackers (Jan Martijn Broekhof, interview with author, April 28, 2016). When asked what it is that causes some hackers to behave

ethically while others turn to illicit behavior, Broekhof suggests it has to do with “common decency” and the “way they are raised” (Broekhof). Although he appears to imply that it is the hacker´s environment as a child to which he is referring when he says ethical behavior results from the way hackers are raised, he does not say so explicitly. It does suggest however, that he thinks the attachment of the hacker as a juvenile to those that raise him – one would assume mostly his parents – affects his behavior. Broekhof more explicitly suggests this when asked whether young hackers should be given lessons in ethics. He agrees, but also adds that parents should be assisted in teaching their children ethical behavior online (Broekhof). Broekhof says that most often parents have no clue about what it is that their child is doing online. However, as Hirschi´s research has shown, the more a child is aware of the fact that his parents know what he is up to, the less likely it is he will show delinquent or deviant behavior. Broekhof´s suggestion corroborates with Hirschi´s theory, as it signals he believes parents´ involvement should be stimulated and that this in turn has a positive effect on ethical behavior by hackers.

The second actor is the teacher or school. Although not quite the conventional type of teacher, Niggebrugge proposes the role of a teacher-like confidant. Niggebrugge calls this type of confidant “internet parents” (Daniel Niggebrugge, interview with author, May 2, 2016). Somewhere in between a parent and a teacher, Niggebrugge suggests that the role of the internet parent could be a great potential tool to encourage young hackers to engage in ethical behavior. Internet parents would serve as confidants. Importantly, internet parents would need to have a thorough understanding of what teenagers are up to on the internet. Combined with sufficient technical knowledge to understand what hackers do, they should be able to engage them in discussions about the ethics of hacking. This notion corresponds with Hirschi´s suggestion that there is a link between the likelihood of deviance and the way a child believes their teacher regards them. The role of a confidant like the ´internet parent´ Niggebrugge suggests, would offer more understanding for young hackers. The respondents also signal that school can be troublesome for many young hackers. Broekhof notes that most hackers have trouble at school because their minds are focused on hacking (Broekhof). As a result, he says the really talented hackers often drop out of school and definitely do not enroll in higher education after high school (Broekhof). When asked whether hackers should be given lessons in ethical hackers, he responds

by saying that lessons in the technical side of hacking would not be a good idea, since they are already very skilled and any teaching program you would develop would be terribly outdated by the time it was finished. He does think teaching them ethics would be a good idea, as do Niggebrugge and Van Andel. Niggebrugge believes programs in which children are taught about hacking, social media and the general ethics involved in online activity would be a great idea. However, this is not what Hirschi means with attachment to school. Hirschi´s theory suggests academically challenging children, so that kids enjoy school, because a child that enjoys school is less likely to show illicit behavior.

The final actors are the hacker´s peers. Although Hirschi found that it is not the juvenile´s peers that lead him to commit deviant acts or to refrain from doing so, but that he chooses his peers on the basis of coinciding behavior or beliefs, it is interesting to verify whether this is also the case for hackers. Although it is hard to verify the extent, there are some indications that hackers' peers do actually influence their behavior. As was mentioned earlier, the hacking community in the Netherlands is very small and tightly-knit. As a result, there is quite some social control and peer pressure. Hackers often share things and help one another, but also tend to make sure others in their community do not do illegal things (Broekhof). Especially nowadays, young hackers are often pushed towards the ethical side by their peers. Van Andel says that an increasing amount of young hackers now start on the "ethical side rather than the negative side" (Edwin van Andel, interview with author, May 2, 2016). This correctional behavior is mainly done online. Illustrative of this fact is the example Van Andel gives. He describes how Ricky Gevers, a well-known ethical hacker who has done time in jail for when he was a black hat, calls out and "virtually berates" hackers for boasting about their illegal hacking skills (Van Andel). As soon as the hacking community recognizes individuals or groups edging toward deviating behavior, they "push them back" towards normal behavior (Van Andel). So contrary to what Hirschi found, the hacker´s peers do seem to influence the likelihood he will show deviant behavior, in a positive sense.

In conclusion, there are definitive signs the respondents think along the elemental line of attachment. Corroborating with Hirschi´s findings, they recognize the importance of parent involvement in the lives of young hackers. They believe that parents should be encouraged and

assisted in better understanding what it is their children are up to, something that Hirschi has found will decrease the likelihood of deviant behavior. Moreover, although not the conventional type of parent, one respondent sees a potential role for a teacher-like confidant. Again, trust and understanding are key, which is in line with Hirschi´s theory. Regarding the school, respondents believe it should have a role in promoting ethics, but they do not mention academically challenging young hackers to make them enjoy school more and subsequently decreasing the likelihood of deviant behavior. Finally, the respondents also mention the important role peers play in promoting ethical behavior. They suggest that the community plays a significant part in prohibiting young hackers from engaging in deviant or delinquent behavior. This is contrary to what Hirschi found, but that does not make it less significant. Rather, it shows that Hirschi´s conclusion regarding the influence of peers is not applicable in this case.

*Commitment*

As has been explained, commitment, the second element, relates to the conformity of rules by individuals simply out of fear of the consequences that result from deviant behavior. If a person invests time and energy in a certain conventional activity, such as education and a career, he would consider the negative consequences that deviating behavior will have for this activity (Hirschi 1969, 21). According to Hirschi, the higher the aspirations of an individual for his educational and occupational career, the less likely it is he will commit delinquent acts.

As the previous section showed, according to the respondents, the average hacker has a troublesome educational future. Many skilled hackers struggle to finish high school, even though most hackers are highly intelligent (Niggebrugge). Those that do manage to finish high school and continue into either college or university, are supposedly not the most skilled hackers (Broekhof). Broekhof proposes that hackers should receive help to at least finish their high school. Although quite possibly beneficial for the hacker´s future, this does not relate to his aspiration or desire for a better educational career, nor does it attempt to encourage said aspiration or desire. Hirschi suggests that their aspirations should be stimulated. It is questionable whether ´receiving help to at least finish high school´ is the same as stimulating them to aspire higher. Then again, aspiring

to finish high school is an improvement compared to not aspiring to finish at all. Interestingly, Niggebrugge indicates that his company and many others only hire hackers that have either a college or university degree. This would suggest that hackers – and society – would be more likely to land a job as ethical hacker should they aspire and succeed in completing a higher level of education. However, Niggebrugge does not offer suggestions for how this should be achieved.

Regarding their occupational aspirations, Broekhof notes that most hackers are weary of a typical nine to five job. Hackers are more interested in what they are able to do on an operational level, than the prospect of a successful career as an ethical hacker (Broekhof). Broekhof says a big reason why hackers opt to work as an ethical hacker, is the type of work they get to do. As an ethical hacker, they get to break into the security systems of places such as hospitals and critical infrastructure, something that would be highly illegal should they do it on their own accord. Besides, hackers do not become ethical hackers out of aspirations for wealth. If they want to make the most amount of money, criminals will always pay them more, or so indicate all respondents. However, none of this indicates that the respondents believe the aspirations of hackers regarding occupational careers should be stimulated. Hackers do not want a typical career, or so it appears.

In conclusion, there is little that indicates the respondents think along the elemental lines of commitment. The only thing that might be considered as thinking along these lines, is the notion that one of the respondents believes hackers should receive assistance in order to be able to finish their high school. However, this is not convincing enough to be able to conclude they think along this elemental line.

*Involvement*

The most straightforward element of Hirschi´s social control theory, involvement, refers to the fact that an individual cannot commit a deviating act if he is spending time on another non-deviating act. An obvious way to bolster involvement would thus be to offer recreational programs to hackers. Do the respondents suggest anything of the like?

Only one respondent, Broekhof, mentions the use of recreational programs. He mentions a group called 'Jonge Onderzoekers (Young Investigators)', which he describes as a "scouting for nerds", that convene once a week to teach young hackers and likeminded students about "technical stuff" (Broekhof). However, the context in which he says this does not indicate he believes the recreational program should stimulate involvement. Broekhof sees the group as a means to encourage children´s interest in technical stuff. Especially kids who are already showing signs of being involved in hacking. Therefore, there is nothing that indicates the respondents believe ´keeping children busy´ will decrease delinquent behavior. This corresponds with what Hirschi found in his research. As Hirschi noted, increasing involvement is not an effective measure to counter delinquency because the amount of time needed to commit deviant acts is very little. The respondents do, implicitly, offer an explanation for why Hirschi´s assumptions about time available is even more applicable to the case of hacking. As a hacker, the time needed to commit deviant acts is even less. Admittedly, it takes a lot of time to invest in the level of skill required to do some of the more advanced hacks, but very much is possible with little experience. Even if hackers are kept busy during the day with recreational programs, they can easily commit any score of delinquent acts from inside their bedrooms at night.

*Belief*

The final element, belief, has to do with the norms and values of society. More precisely, it has to do with the degree to which a person believes in these norms and values. The less a person believes he should obey the rules, the more likely it is that he will violate them. To strengthen the bond with society, individuals must be made to more firmly believe in the norms and values of society. The question is, whether the respondents indicate that a firmer belief should be stimulated, and if so, how.

That the respondents believe a firmer belief in society´s norms and values should be stimulated is without question. All respondents seem to indicate that the primary reasons for hackers to act ethically or not, are their values and norms. Broekhof notes that it is the hacker´s "outlook to the world" that primarily determines whether he behaves ethically or not (Broekhof).

Niggebrugge says that the main reason why young hackers are more prone to delinquent tendencies compared to older hackers, is their lesser developed ethical views (Niggebrugge). Van Andel also notes that hackers can have a warped perspective of what is right and wrong when they are young (Van Andel). So how should the belief in the values and norms of society be stimulated? Again, all respondents seem to be on the same page. They all agree that lessons in ethics could be a valid way of increasing the beliefs of hackers, thus stimulating ethical behavior. Broekhof does question how this can be done effectively (Broekhof). As stated before, he indicates young hackers are the type of kids that are already struggling to keep up with regular school, because all they can think about is hacking (Broekhof). That is precisely why Niggebrugge doubts that such an approach will work (Niggebrugge). He believes it is hard to teach ethics at that age. That is why Niggebrugge opts for a more integrated approach, where all students receive lessons in ethics in computer use, including hacking, social media, etc. Furthermore, Van Andel also sees a role for the NCSC. He believes outreach by representatives of law enforcement agencies or government officials, such as NCSC officials and members of the High Tec Crime Unit, can create dialogue about proper conduct and ethical behavior (Van Andel). This corroborates with what Hirschi suggests can stimulate belief in rules. Increased respect for the law and government officials will make it less likely individuals commit delinquent act. This is also what Van Andel suggests. He says that by visiting hacking events, government officials of the NCSC can command the respect of hackers, which in turn leads them to sooner "head the right way" i.e. behave ethically (Van Andel).

In conclusion, it is quite clear that the respondents think along the lines of the element belief. They seem to believe that stimulating the beliefs of hackers in the norms and values of society will cause them to sooner act ethically. This can be done while they are young, through schools and parents, but also while they are older, by having government officials earn their respect.

*Conclusion*

With respect to Hirschi´s four elements, it is clear that the respondents think more along the lines of some than others. The interviewees seem to suggest that the elements attachment and belief are the most promising for encouraging ethical behavior. For attachment, the respondents see a possible role for each of the actors recognized by Hirschi. They even see a role for the group peers, which Hirschi´s empirical research found was not an influence on wider delinquent behavior. It is clear that they believe the direct social environment of the hacker can have a huge positive impact on their behavior. Regarding belief, they are convinced that stimulating the beliefs of hackers in the norms and values of society will increase the likelihood of ethical behavior. For the elements commitment and involvement, the respondents do not seem to see considerable possibilities to encourage ethical behavior or discourage delinquent activity. Regarding commitment, the conventional desires for educational and occupational careers do not seem to apply to hackers. Hackers would seem to benefit from increased assistance at schools, but this is not what the element commitment refers to. Involvement is the element that the respondents least see as beneficial. Hackers can easily commit delinquent acts from within the confines of their house, whether it be during the day or at night, so this element is irrelevant.

## 4.2 Considerations of Companies

After the hackers, the second of the primary actors involved in hacking are the companies. This part of the analysis will offer insight into the considerations of companies regarding the discouragement of illicit activity and the encouragement of ethical behavior of hackers. Again, the first section will offer an overview of the paper reality. The second section will discuss the data gathered through interviews with representatives of various companies.

### 4.2.1 Paper Reality

This section will discuss the available documentation on the relationship between companies and hackers. What are the considerations of companies in the Netherlands regarding hacking? Do they mainly see hacking as a threat or do they also see opportunities? Important to note is that this does not concern the ethical hacking companies, whose accounts were taken into

consideration in the part on ethical hackers. Instead, it concerns companies who may become victims of hackers, or who have experienced interactions with an ethical hacker.

*A Brief Introduction*

As was quoted as an example in the previous part of this chapter, the first victim of a serious illicit hack in the Netherlands was the Dutch telephone company PTT, in 1985. In 2012, KPN, the successor of PTT, was hacked again. This time, a seventeen year old hacker used a vulnerability to gain access to multiple servers and obtained client information of thousands of people (Koenis 2014). This example serves to illustrate that companies were among the first to be victimized by hackers and they have taken the brunt of the force ever since. As FBI Director Robert Mueller famously said: “There are only two types of companies, those that have been hacked and those that will be hacked” (Marsh 2014, 2). Hence, companies have every reason to be involved in the debate about hacking. In the Netherlands, there are countless examples of companies being attacked by hackers. According to research by TNO, a Dutch research institute, cybercrime cost the Netherlands an approximate ten billion euros in 2014 (Marsh 2014, 2). Companies in the Netherlands are a popular target: in 2012, more than 2.2% of all global hacking incidents that led to data loss took place in the Netherlands (KPMG 2014). That made the Netherlands the fourth most popular target in the world (KPMG 2014). Again, although hackers are definitely not responsible for all of the damage done, black hat hackers do cause damage, steal money or personal data, and sell information and zero-days – a valuable type of vulnerability – to cybercriminals.

*Considerations*

With so much damage being done to companies, one might expect a certain feeling of hostility towards hackers. And although this is almost decidedly the case for black hats, there are also signs that companies are increasingly embracing ethical hackers. This conclusion can be drawn from two trends among companies. The first is that companies increasingly publish responsible

disclosure policies on their websites (CIO Platform Nederland 2016, 7). As has been explained in the first two chapters, responsible disclosure is a way for hackers to indicate vulnerabilities in websites and information systems without risking prosecution. In 2013, when the NCSC published its best practice guide for responsible disclosure, only a handful of companies had responsible disclosure policies. Now, three years later, more and more companies are publishing responsible disclosure policies, especially in the telecom and banking sector (CIO Platform Nederland, 7). This is partly due to the marked growth of cyber security companies like HackerOne and Zerocopter, who, through bug bounty programs, facilitate ethical hacking. Although it is hard to pinpoint the exact percentage of an increase between 2013 and now, it is unquestionable that there has been a significant one. The second trend is an even more recent one, and although it may not be a voluntary, it is a trend nonetheless. On January the 1st, 2016, the Dutch ´Authority on Personal Data' (Autoriteit Persoonsgegevens) – a government institution responsible for creating and implementing policy regarding the safeguarding of personal data – started to enforce the so-called ´compulsory reporting of data leakage´ (Autoriteits Persoonsgegevens 2015, 4). This compulsory reporting entails that organizations are required to report immediately any occurrence of data leakage (Autoriteit Persoonsgegevens 2015, 4). Should companies fail to report data leaks, especially if they are serious, they will have to pay significant fines (Autoriteit Persoonsgegevens 2015, 49. As a consequence, companies have a financial trigger to improve the security of their information systems. Ethical hacking companies have seen a huge surge in the demand for their services as a direct result (Broekhof).

To summarize, companies would seem to have a double feeling towards hacking. On the one hand, companies in the Netherlands are among the most attacked in the world. The annual damage done by black hat hackers and cybercriminals is in the billions. On the other hand, several trends indicate companies are starting to embrace ethical hacking. An increasing amount of companies have responsible disclosure policy and due to the law on data leaks, there is a demand for higher cyber security standards.

### 4.2.2 Company View on the Hacking Community

So on paper, it seems companies are starting to use ethical hackers much more often. But how does this compare to the feelings of hostility they have towards black hat hackers? Do they see the benefits of using ethical hackers to increase cyber security, or are the possible advantages incomparable to the damage done by black hats? In this section, the views of the representatives of companies on the hacking community will be discussed. How do they view the community as a whole?

When asked about their general feelings towards the hacking community, just as happened when ethical hackers were asked, the respondents responded to the question with: ´which hackers do you mean?´ This response is telling, because most people would associate the word hacker with criminals. As their question implies, the respondents are well aware that there are different types of hackers. For Wim Daalhuizen, this might have been expected, since he is responsible for cyber security at Intergamma. Illustrative of the general response to hacking, is that he gets a very different reaction when he talks about hackers to his management (Daalhuizen). According to Daalhuizen, his management still only associates the term with black hat hackers (Daalhuizen). He himself however, decidedly discerns between ethical hackers and black hat hackers. What is more, he even doubts whether you should use the word hacker at all to describe those committing crimes. He attests there is a big difference between hackers and cybercriminals. Cybercriminals can use hacking, but they should not be called hackers. This is interesting, because it is exactly what the hackers said about their community. Daalhuizen also references the ´hacker versus cracker´ debate that Niggebrugge referred to, also indicating that he has given up on it (Daalhuizen). Diepenmaat appears to have a likeminded mentality considering the hacking community. He says that his feelings towards the hacking community are mostly positive, since his only contact with hackers is with ethical hackers through the responsible disclosure policy of his company (Diepenmaat). He speaks very highly of ethical hackers and thinks that they will play an increasingly bigger role in cyber security.

Regarding black hat hackers, both respondents believe they are a quite marginalized group within the hacking community. The overall picture that the respondents have of the community is remarkably positive and they speak highly respectfully of them. But is this how

most companies feel about hackers? Without responsible disclosure policies, companies are less likely to come into contact with ethical hackers. Nonetheless, there are a lot of indications that this is changing in the Netherlands.

### 4.2.3 Thinking Along Elemental Lines

The previous section showed that the companies interviewed for this research have a remarkably positive attitude towards the hacking community. They see hacking as an opportunity rather than a threat. The question now is, how they believe this opportunity can be seized. How should hackers´ ethical behavior be encouraged and illicit behavior be discouraged? Along which of Hirschi´s elements do they believe action should be taken? This section will discuss each of Hirschi´s elements.

*Attachment*

The first element is attachment, which relates to the fact that it is our attachment to others that keeps us from resorting to deviant behavior (Hirschi 1969, 18). As indicated before, the three main groups of actors are parents, teacher and school, and peers. This section is divided into three parts, one for each group of actors.

The first actors to which a hacker might feel attachment are his parents. There is absolutely nothing however, that indicates that the representatives of the companies believe that the parents should play a role in encouraging ethical behavior. Important to note is that the respondents were never directly asked about what the role of the parents should be. However the contrast with what the ethical hackers suggested is quite apparent.

The second group of actors, teachers and school, is something that one of the representatives does mention. He argues that ethical hacking should be taught at school (Diepenmaat). However, Diepenmaat does not mention school or teachers in the sense that Hirschi refers to when he talks about the element attachment. Diepenmaat thinks ethical values should be taught, which is more in line with the element belief. He does not mention the role of

the teacher, nor does he refer to challenging young hackers academically or making them enjoy school more. So once again, quite contrary to the opinions of hackers, there is no reason to assume the respondents think attachment should be stimulated.

The same goes for the last group. Once again, the respondents do not seem to believe stimulating attachment is a way to encourage ethical behavior or discourage illicit behavior. They do seem to hold the hacking community in high regard, but do not signal they think it can stimulate the behavior of their members. However, this is also what Hirschi believes.

Summarizing, it is abundantly clear that the respondents for the companies, one of the actors involved in hacking, do not think along the lines of the element attachment. They do not mention the role of parents or peers, nor do they refer to the school or teacher in the context of attachment.

*Commitment and Involvement*

As has been explained, commitment, the second element, relates to the conformity of rules by individuals simply out of fear of the consequences that result from deviant behavior. According to Hirschi, the higher the aspirations of an individual for his educational and occupational career, the less likely it is he will commit delinquent acts. Involvement, refers to the fact that an individual cannot perform delinquent act while being occupied with non-delinquent acts.

Perhaps even more so than for the previous element, there is nothing in the conversations held with the respondents that indicates they think along these lines. Not once do they indicate they believe the aspirations of hackers for an educational or occupational career should be stimulated, nor do they suggest occupying hackers with recreational activities. Already, it appears that the elements in Hirschi´s social control theory are not appealing or relevant for companies. The relevance of the element involvement for black hat hacking as a form of delinquent behavior, was already cast in doubt in the previous part. After involvement, commitment was the element that least reflected the line of thinking of the respondents. Although even less so, the same appears to be the case for this party involved in ethical hacking in the Netherlands.

*Belief*

The final element, belief entails the degree in which individuals believe in the norms and values of society. Hirschi´s theory holds that everyone ascribes to the same norms and values, it is just that some believe in them more than others. To think along this line, is to think that the belief in the norms and values of society should be stimulated.

As indicated for the element attachment, Diepenmaat does believe that ethics should be taught in school. He says that ethics are an important part of the education of any young person getting seriously involved in computers, whether it be software developers or hackers, and that they should be taught ethics extensively (Diepenmaat). Whether it should be done in high school is something that he doubts, but he thinks it should at the very least be done in colleges and universities. This corresponds with what Daalhuizen believes. He too thinks that ethics should be taught when hackers are younger (Daalhuizen). According to Daalhuizen, once hackers have become black hats, there is "no possible way to get them back" (Daalhuizen). He states that there is simply too much money to be made as a black hat hacker, that once you start doing it, there is no way back.

It is clear that respondents think that the beliefs of hackers in norms and values should be stimulated, but what about the role of law enforcement agencies and government officials? They do not offer anything that suggests respect for the law should be induced in hackers to stimulate their beliefs in values and norms. However, Diepenmaat does see a bigger role for the NCSC as an executive agency. He thinks that the responsible disclosure policy is not being enforced well enough. In this regard, he does not mean that hackers should be dealt with more strictly, but that companies should be incentivized through laws to commit to responsible disclosure policies.

Summarizing, there are enough indications that the respondents think along the lines of the element belief. They think it would be a good idea to stimulate hackers to learn about ethics in school. However, they do not seem to think that law enforcement agencies should play a bigger role in stimulating this.

In conclusion, there are very few instances in which the respondents think along the lines of any of Hirschi´s elements. The only element for which it is clear that the representatives of companies do so, is belief. This is in stark contrast with the ethical hackers. There were indications they thought along the lines, at least to some extent, of attachment, belief and commitment. Especially attachment, which was the element for which ethical hackers showed the most inclination, is completely non-existent for companies. It would appear that Hirschi´s social control theory is not able to explain or account for the considerations of companies. So what did the representatives of companies suggest? Their suggestions were almost all policy and demand oriented. Rather than believe the solution lays with hackers themselves, they thought that either the government or companies themselves could encourage or discourage ethical hacking. For the government, Diepenmaat for example believed their role should be to stimulate or even force companies to adopt responsible disclosure policies. He was adamant in his belief that ethical hacking was an extremely viable cyber security measure and that responsible disclosure policies were the future.

## 4.3 Considerations of the Government

In this section, the considerations of the government regarding the discouragement of illicit and encouragement of ethical behavior of hackers will be examined. First, this will be done for the paper reality. What does the available documentation tell us about the way the Dutch government regards hackers? Hereafter, the same will be done using the data collected through interviews. First, this data will be used to understand what government representatives´ view of the hacking population is. Second, the data will be analyzed using Hirschi´s four elements to determine along the lines of which of the elements they think.

### 4.3.1 Paper Reality

This section will analyze the available documentation on the government´s view on hacking. First, an introduction will be given, describing the historical trajectory of the Dutch government´s

relationship with the hacking community. Second, the available documentation will be analyzed in an attempt to discern the general attitude towards hacking and ethical hacking.

*A Brief Introduction*

The Dutch government first became involved with hackers in the 1990s (Dasselaar 2008, 31). Several hackers had received fines or mild prison sentences, but there appeared to be no serious reason for concern, since most hacks were relatively harmless. This began to change after a series of high profile hacks at the start of the new millennium. Where previously companies had been the target of hacks, in 2004, several government websites were targeted by a DDoS attack (Dasselaar 2008, 32). Alarmed, the Dutch government began to take more serious actions against hackers (Dasselaar 2008, 32). Although more awareness of potential threats existed, attacks would only increase in both number and severity. One of the most infamous and damaging hack attacks was the Diginotar case. In 2011, a private company that performed services for the Dutch government, was successfully attacked, compromising personal data of Dutch citizens (NU 2012). However, apart from damaging hack attacks, there was also an increasing number of hacks that resembled what is now considered responsible disclosure in the Netherlands. Because all forms of hacking were strictly considered illegal, there were multiple cases in which serious vulnerabilities were discovered. The way in which the Dutch government responded to each of the cases is telling of how its considerations regarding hacking and ethical hacking have altered significantly the past decade.

*Considerations*

So how does the Dutch government appear to view the hacking community if we base our assumptions on the available documentation? As said, the reaction of government institutions to hacks reveals how they regard hacking and hackers. In his book 'Helping Hackers' (Helpende Hackers), researcher Chris van ´t Hof has chronicled the most important hacks and disclosures (Van ´t Hof 2015). It convincingly shows a shift in state of mind within government institutions.

During the time of the first big cases of responsible disclosure, reactions are more hostile. There is less understanding for the plight of ethical hackers, the signaling of vulnerabilities is seen as damaging to the overall security of information systems (Van 't Hof 2015, 27). That being said, several ethical hackers that have been sued and called before court are being acquitted if their intentions were to improve security or serve the greater good, and no harm was done in the process (Van 't Hof 2015). Notable cases include the hack of the OV-chipcard, in which researchers of the Radboud University of Maastricht manage to hack the card and subsequently use it to travel for free, the hack of online identity verifier DigiD and the discovery of vulnerabilities in the information system of hospital 'Het Groene Hart'. Moreover, in 2012, as the number of hacks that are intended to showcase vulnerabilities increases, so does the call in Dutch parliament for a way to deal with these hacks (Van ´t Hof 2015, 148). Ivo Opstelten, Minister of Safety and Justice at the time, promises parliament to create a guideline for companies and hackers on how to deal with responsible disclosure (Van 't Hof, 148). This leads to the publication of the Best Practice Guide for Responsible Disclosure in 2013 (Van 't Hof, 148). In the document, the NCSC, on behalf of the Dutch central government, outlines its take on responsible disclosure. According to the Dutch government, the term 'disclosure' deals with the way that vulnerabilities in software and information systems are disclosed (National Cyber Security Centre 2015, 7). In this sense, responsible disclosure, is "when someone who learns of a vulnerability tries to contact the owner or supplier of the system" and "gives them the time to fix the vulnerability before the details of the vulnerability are published" (National Cyber Security Centre 2015, 7). Moreover, "the discloser and the affected organization coordinate in publishing the vulnerability" (National Cyber Security Centre 2015, 7). The Dutch government's definition of responsible disclosure coincides to a great extent with the general academic interpretation of the phenomenon. However, important to note is that the government sees only a minor role for itself considering responsible disclosure (Van ´t Hof 2015, 148). Only where the discovery of vulnerabilities concerns information systems of the Dutch central government or 'critical sectors' will the NSCS be actively involved (Van 't Hof 2015, 148). In other cases, companies and hackers are encouraged to sort out issues themselves, using the policy as a guideline. Only when the parties involved cannot work out their issues will the NCSC intervene or offer assistance.

The above clearly shows a change over time in the way the Dutch government regards hacking. After several highly mediatized disclosures in the period 2008-2012, a shift begins to take place. At first, hackers are mainly seen as a nuisance and a threat to cyber security. That changes when discoveries of major security flaws receive widespread media attention and judges rule in favor of the disclosers in separate occasions. Ethical hacking becomes a more accepted way of disclosing security vulnerabilities and the Dutch government responds by publishing a guideline that should acquit ethical hackers if they adhere to it. However, strictly speaking, ethical hacking is still illegal in the Netherlands. If a company were to sue an ethical hacker, the Public Prosecution will still mark the ethical hacker as a suspect and start an investigation (NCSC 2013). Even if a company does not sue, the Public Prosecution can decide to prosecute ethical hackers (NCSC 2013). Even so, these measures will only be taken if there is reason to believe foul play on part of the hackers was involved. Clearly, the Dutch government has a much more positive view of the hacking population than a few years ago.

### 4.3.2 Government Views on the Hacking Community

In the previous section, the available documentation was used to show how the Dutch government appears to regard ethical hacking. In this section, the interviews with government representatives will be used to discern how the Dutch government views the hacking community. Do they mainly see them as helpful ethical hackers or damage inflicting criminals?

Jeroen van der Ham from the NCSC admits that it is hard to view the hacking community in the Netherlands as a whole (Jeroen van der Ham, interview with author, May 20, 2016). He says that to him the community is divided into two parts, a visible and an invisible part. The visible part consists of the hackers he has contact with, whether in person at hacker events or online through twitter. These are all ethical hackers and are very actively involved in the hacking community. The other part, he considers the invisible side of the hacking community (Van der Ham). He says he knows practically nothing about this group of hackers; the number of black hats, the number of white hats, or how these two groups interact. He does believe, as did others, that there is a large grey area. He notes the story of a seventeen year old Dutch hacker as an

example, who had been arrested and jailed in the United States for criminal hacking activity (Van der Ham). This hacker described how at first he did not commit any illegal acts, but how he slowly but gradually got involved in more serious and illegal activity. Van der Ham suggests that this is what it is like for most black hat hackers (Van der Ham). The status quo is white hat hacking, those that are black hats 'gradually descend' into being a black hat.

Alf Moens from SURF also suggests to split the hacking community in two, but he does so in the more traditional sense by discerning between white hat hackers and black hats (Alf Moens, interview with author, April 27, 2016). He speaks very highly of ethical hackers, for whom he has a lot of respect. However, he does stress that he believes they should keep strictly to the rules (Moens). Hackers should only report flaws they stumble upon incidentally and refrain from actively scouring the internet for vulnerabilities. In this sense, Moens clearly favors white hats over grey hats. This notion is further confirmed when asked about the commercialization of ethical hacking. He is weary of commercialization, because he believes it will lead to ethical hackers being more aggressive, approaching companies that did not explicitly ask for help (Moens). Regarding black hat hackers, his opinion is straightforward. He believes them to be a nuisance and a huge threat (Moens).

Summarizing, there are several conclusions that can be drawn from the account of the two respondents. First of all, they do not seem to have a clear view of the size of the hacking community. The NCSC representative offers distinction between a visible and non-visible part of the community. He is only aware of hackers in the visible community, who are all ethical hackers. Second, Van der Ham regards ethical behavior as the norm amongst hackers, with black hat hacking being something into which white hats 'descend'. Both are very positive about the white hack population. The big difference between the two accounts is that the SURF representative is quite weary of grey hats. He regards the commercialization of ethical hacking as a negative development, which Van der Ham does not seem to agree on. He argues that companies such as Zerocopter and HackerOne, who commercialize responsible disclosure, can be a useful addition.

### 4.3.3 Thinking Along Elemental Lines

In this section, the considerations of the respondents regarding the encouragement of ethical and discouragement of deviant behavior will be examined. Again, this will be done by using Hirschi's four elements. Along the lines of which of the four elements do the respondents believe action should be taken? As previous, this will first be done for attachment, followed by commitment, involvement and lastly belief.

*Attachment*

As has been explained before, attachment relates to the fact that it is our attachment to others that keeps us from resorting to deviant behavior (Hirschi 1969, 18). According to Hirschi, there are three categories of actors that influence whether or not a person shows deviating behavior: parents, school/teachers, and peers. Because the respondents did not indicate the teachers or school should be involved, this category will not be discussed. Therefore, first the category parents will be assessed and then peers, before concluding whether the respondents think along this elemental line. Moreover, because Alf Moens did not indicate he believes any of the actors play an important role in influencing the likelihood of hackers showing deviant behavior, this section only discusses remarks made by Jeroen van der Ham.

Regarding the first category, parents, the respondents do not think they should play a big part in the encouragement of ethical behavior. Jeroen van der Ham notes that parents are currently in no position at all to get young hackers to behave ethically online (Van der Ham). When asked whether that should change, Van der Ham suggests that parents should receive support for helping them deal with children active in the hacking community. He says young hackers should be sent to 'hackerspaces' – events where hackers meet and engage in various activities – as a means of support for their parents (Van der Ham). Although helpful for the parents, it is debatable whether this is what Hirschi refers to when he says parents should be more involved in their children's activities. It does imply some involvement on behalf of the parents, but Van der Ham does not seem to suggest involvement should be actively stimulated as a means to encourage ethical behavior. He further adds that it is unlikely that parents can be

convincingly explained what it is their children do, should their children by hackers (Van der Ham).

Since there are no indications that the respondents believe teachers and school should be more involved in strengthening the bond with society via attachment, the next group of actors that will be discussed is the hacker's peers. Of the three actors, Van der Ham believes peers to be the most important in influencing hackers' behavior (Van der Ham). As ethical hacker Edwin van Andel had already indicated, Van der Ham also recognizes the important role of the hacking community in encouraging ethical behavior. He acknowledges that they call out and verbally reprimand hackers online if they brag about criminal achievements, which he thinks is a good thing (Van der Ham). He does however, believe it is largely up to the hacking community itself to assume this task. He does not think the government should get too involved, other than trying to steer the conversation so as to include viable discussions on ethics (Van der Ham). However, he clearly does see an important role for the hacker's peers to influence their behavior.

In conclusion, there are no very strong indications that the respondents think along the lines of the element belief. One of the respondents, Alf Moens, did not offer any indications whatsoever whether the actors should be involved more to influence the behavior of hackers. Jeroen van der Ham, the representative of the NCSC, did seem to suggest the involvement of at least one of the actors; peers. He acknowledged the important role they play in influencing the behavior of other hackers, suggesting that they should keep doing so. However, he did not specify how this behavior should be encouraged and did not think the government should play a role in it.

*Commitment and Involvement*

The second and third elements are commitment and involvement. Commitment relates to the conformity of rules by individuals out of fear of the consequences of deviant behavior. By encouraging the aspirations of hackers, whether they be educational or occupational aspirations, the likelihood of them showing delinquent or deviating behavior should diminish (Hirschi 1969, 182). Involvement is the most straightforward element, as it relates to the fact that an individual

cannot commit deviating acts if he or she is involved in other conventional non-deviating activities. Encouraging adolescents to join in recreational programs is a way to increase involvement.

As was the case for the companies, there is very little that hints that the government representatives think along the lines of these elements. Regarding commitment, there is nothing at all that the respondents offer as an indication of their thinking along its lines. Concerning involvement, Van der Ham does seem to encourage hackers to partake in events, such as hackerspaces (Van der Ham). One could classify these events as recreational programs. However, their involvement in these events is not intended to serve as a way to 'keep them busy', which is what involvement in social control theory entails. Therefore, the conclusion can be made that the respondents do not think along the lines of these elements.

*Belief*

To what degree hackers believe in the norms and values of society, is what the element belief refers to. To strengthen the individual's bond with society, he or she must be encouraged to more strongly believe in its norms and values. Do the respondents indicate that a firmer belief should be stimulated?

Van der Ham is a strong supporter of stimulating ethical behavior by teaching ethics (Van der Ham). As a lecturer in ethics in information science himself, he is very much aware of its importance. He stresses that those who work in information and computer sciences too often do not take ethics into consideration (Van der Ham). Subsequently, he strongly advocates teaching potential hackers ethics. As a starting point, he thinks college and university students dealing with information and computer sciences should receive lessons (Van der Ham). Whether high school students should also be actively taught ethics is something he is not sure about. He does see the added value, but simply doubts whether it is realistic to start such a program for children of that age (Van der Ham). Rather, he thinks that by starting with teaching ethics to students at colleges and universities, this will create a ripple effect, resulting in a shift in the state of mind of the entire information and computer sciences community (Van der Ham). As a result, new

individuals joining in will automatically be taught more about ethics. This would also affect the behavior of grey or white hats, leading them to be more aware of what constitutes ethical behavior.

Another way Hirschi claims the belief in the norms and values of society can be stimulated, is through increasing the respect for the law and government officials. Ethical hacker Edwin van Andel already suggested that he believed outreach by members of the NCSC proved very valuable. How does NCSC representative Jeroen van der Ham regard this suggestion? On the one hand, he does believe it to be important for the NCSC to advocate responsible disclosure and ethical behavior amongst hackers. He deems it crucial that hackers are fully aware of the boundaries in which he operates, which is why the NCSC organizes events and gives presentations (Van der Ham). On the other hand, he does not seem to think the NCSC or any other governmental organization should get too involved in the more traditional sense of authoritative figure (Van der Ham). Instead, he signals that that should be a task of the community itself. His conviction is that the government should stay at the sidelines as much as possible, letting companies and hackers figure things out amongst themselves (Van der Ham). Only when they fail to see eye to eye, does Van der Ham believe the government should step in. Obviously, this does not corroborate with Hirschi's theory, which foresees an active role for authoritative figures, in order to ensure respect for the law and consequentially a more firm belief in the norms and values of society.

Summarizing, there are no strong signs that the representatives for the government think along Hirschi´s elemental lines. There was also a big difference in the way both respondents seemed to think. Alf Moens, the SURF representative did not seem to think ethical behavior could be encouraged and deviating behavior discouraged by taking actions along the lines of Hirschi´s element. Jeroen van der Ham did think along the lines of two of the elements, albeit with significant restraint in comparison with the representatives of the other two parties involved in hacking in the Netherlands.

Regarding the first element, attachment, Van der Ham indicated that there was only a serious part to play for the hacker's peers. He indicated that they do a good job keeping hackers

in check, something that should be encouraged. In respect to the second and third elements, commitment and involvement, the respondents did not seem to think along those lines at all. The element which is represented strongest is the element belief. Van der Ham clearly seemed to think the beliefs in the values and norms of society should be stimulated, by teaching ethics to information and computer science students at college and university. However, he did not think the NCSC should be actively engaged with hackers in order to command respect for the law. Instead, he believes government agencies and agents should keep a lower profile and let companies and hackers sort things out amongst each other.

## 4.4 Aligning the Considerations

Now that the considerations of hackers, companies and government have been discussed, it is time to assess and compare these considerations. This section will do just that, discussing the similarities and differences in order to align the considerations of the three parties involved. In turn, aligning the considerations will allow for an answer on what the considerations of the parties involved are concerning the encouragement of ethical and the discouragement of illicit behavior of hackers.

First of all, all parties involved seem to have a mostly positive view of the hacking community as a whole. They concur that black hat hacking is a subculture of the hacking community, agreeing that most hackers are predominantly involved in various forms of ethical hacking, whether being white or grey hats. Additionally, all parties have made it clear that they see a difference between hackers on the one hand and cybercriminals on the other. However, there are indications that there is a significant difference in the way that individuals in companies think. Those involved in cyber security are much more aware of the various types of hackers compared to management. Companies without security experts and responsible disclosure policies quite likely feel different about hackers.

While the three parties involved in hacking are mostly in agreement regarding the way they view the hacking community, there are telling differences in their considerations about the discouragement of illicit and the encouragement of ethical behavior of hackers. The hacking

community itself, seems to think ethical behavior should be encouraged predominantly along the lines of attachment and belief. They signal that the period when hackers are young, is the time when they should be encouraged to behave ethically. In doing this, they see an important role to be played for the parents, teachers and peers. Moreover, they think that stimulating the beliefs of hackers in the norms and values of society can have a sized influence on their behavior. Here, they also see a role for government officials, who can steer hackers in the right direction by earning and commanding their respect.

The previous is not in line with what the representatives of companies seem to believe. Hirschi´s elements offer no convincing way to explain their considerations. They offer solutions that demand changes on behalf of companies themselves, rather than change the behavior of hackers. According to them, it is companies who should be encouraged to adopt responsible disclosure policies. They believe further regulation by the Dutch government can positively influence the role of hackers, because companies will sooner need the services of ethical hackers. A good example of this is the law on the required reporting of data leaks, which means companies will be more eager to find possible vulnerabilities before they are exploited and data is leaked.

The representatives of the government, the final party involved in hacking in the Netherlands, also show little inclination of thinking along the lines of Hirschi's elements. As was similar for the other two parties, the elements involvement and commitment are not considered as a means to encourage ethical behavior. Regarding the element attachment, the representative for the NCSC does think the hacker's peers are an important factor in increasing ethical behavior, but does not believe in a role for the parents and teachers. Lastly, stimulating a firmer belief in the values and norms of society is something that the NSCS representative believes to be of crucial importance. However, he does not think the government should try to stimulate a firmer belief by commanding respect, contrary to what ethical hackers suggested.

Having compared the considerations of the three parties, aligning those leads to the following conclusion. To encourage ethical and discourage illicit behavior of hackers, the parties involved in hacking in the Netherlands believe action should be taken along the lines of the elements attachment and belief. Given the fact that hardly any inclination was given that the parties concerned think action should be taken along the lines of the elements commitment and

involvement, it is safe to say that these do not have to be considered. Instead, focus should be on attachment and belief. Regarding the element attachment, the hacker's peers are the most important actors to influence his behavior. Because the community is tightly-knit, there is a lot of social control online. Hackers should encourage each other to behave ethically and refrain from engaging in illicit behavior. Whether parents and teachers should be involved is something the three parties are not in agreement about. Finally, concerning the element belief, hackers should be stimulated to more firmly believe in the values and norms of society. This should predominantly be done by teaching them ethics, at the very least in college and university, and ideally also in high school.

# 5. Discussion and Reflection

The final chapter will serve as a means to discuss the findings and conclusions of this research. Moreover, it will serve as a way to reflect on the research process. First, it will reflect on the general conclusion that was drawn from the findings of the research, using Hirschi's theory. Second, based on the conclusion and reflection, a recommendation will be made for the Dutch government and companies. Third, it will discuss any of the difficulties encountered while doing this research and discuss its limitations. Finally, it will offer suggestions for further research.

## 5.1 Reflection

The previous chapter ended with the alignment of the considerations of the parties involved in hacking in the Netherlands, which answered the main research question of this thesis. This section however, will take a closer look at the answer and place it into perspective. In other words, what does it mean?

According to Hirschi, the stronger the individual's bond to society, the less likely it is he or she will resort to deviating behavior. In the context of hacking, black hat hacking is considered deviating behavior, ethical hacking being the normal desired behavior. Hirschi believes that the individual's bond to society can be strengthened through four different elements: attachment, commitment, involvement and belief. The more these elements are ascribable to the individual, the stronger the bond and the less likely he or she will resort to deviating behavior. As was explained in the conclusion, the parties involved in hacking in the Netherlands do not seem to believe each of the elements Hirschi recognizes are important in discouraging deviant behavior. What could explain this disparity? Why do the parties think, at least to some degree, along the lines of the elements attachment and belief, and not those of commitment and involvement? It seems that there are various explanations.

The first possible explanation has to do with the act of hacking. The nature of the activity makes it quite unique from a criminological perspective, and very likely far beyond the scope of what Hirschi had in mind as a possible criminal activity when he composed his theory. The fact

that hacking can be used both for good and for bad, even though the activity in itself is illegal, makes it quite different from more conventional criminal activities. This assumption might explain why the parties involved do not think stimulating commitment is a viable means of encouraging ethical behavior. As was said by one of the respondents, hackers do not strive for a conventional career. Rather, hackers look for opportunities where they can do the most interesting work. Offering hackers interesting and challenging opportunities, within the legal confinements offered by responsible disclosure, is probably a much more effective way of producing conformity. The nature of the activity also explains why the element involvement is not relevant in this case. As was explained earlier, hacking as an activity is not limited by physical constraints or time constraints. It can be done from virtually any place and any time, given that the hacker has access to a computer and internet. Therefore, occupying hackers through recreational activity will very likely do nothing to stop them from engaging in criminal activity when they get home, assuming that is what they intend to do. It seems that the heavy dependency on technology for hacking as a form of deviating behavior renders the element involvement useless. Hirschi already struggled to find evidence this element was a factor, and this research further attests to that notion.

The second explanation has to do with the nature of Hirschi's social control theory. There were significant differences between the groups, and especially for the companies, there seemed to be no thinking along the lines of Hirschi´s elements. This might have to do with Hirschi's social control theory. Because he believes it is the individual's bond to society that influences whether or not the individual commits deviating act, measures taken to encourage ethical behavior logically revolve around the individual. The fact that the hackers showed the strongest signs of thinking along the lines of attachment and belief, might have to do with the fact that they have the most insight into how hackers think. As the accounts show, the ethical hackers had detailed assumptions on what encourages hackers on a personal level. This is unsurprising of course, given that they themselves are hackers. On the other hand, companies seemed to offer solutions that involved either the government or companies themselves. They thought more in structurally or environmentally oriented solutions. Hirschi clearly believes the individual is key, something that

the hackers agreed with to a large extent, but which companies and the government seemed less convinced of.

In summary, there are two main explanations that place the conclusion reached in the previous chapter in perspective. First of all, the nature of hacking as an activity explains part of the disparity between Hirschi's theory and the findings. Secondly, Hirschi's individualistic focus explains why companies and the government thought less along the lines of these elements. However, that does not mean that valuable lessons were not learned, which is what will be discussed in the next section.

## 5.2 Recommendations

With the ever increasing importance of information systems, securing and protecting these systems becomes an ever increasing priority. In the Netherlands, it is beyond doubt that the hacking community will play a significant part in this continuing process. The question is however, how this part will play out. On the one hand, black hat hackers and cybercriminals pose a serious threat to cyber security. Ethical hackers on the other hand, have a significant role in improving said cyber security. In the Netherlands, the hacking community as a whole seems inclined towards improving cyber security.

The conclusions of this research allow for a few recommendations to improve ethical behavior of hackers in the Netherlands. First of all, the role of the direct environment of hackers should be enhanced. Parents, teachers and peers should be encouraged to be more involved in the activities of young hackers. Research has shown that more involvement of these actors will decrease deviating behavior, whit which the ethical hackers consulted seemed to agree. Especially the group peers, which in this case is the hacking community, should be encouraged to more actively advocate ethical behavior. Secondly, hackers should be stimulated to more firmly believe in the norms and values of society. One of the foremost ways in which this should be done is through teaching ethics. This should be done at colleges and universities, but also at high schools. Although lessons in online ethical behavior will be hard to accomplish, the eventual benefits would be significant. Also, authoritative figures, such as NCSC officials, should be more

engaged in outreach programs. Developing relationships with hackers is a good way to command their respect and gain respect for the law, which in turn leads to less deviating behavior.

## 5.3 Limitations

During the course of this research, several limitations have presented themselves. The first and foremost limitation was already hinted at in the previous section; Hirschi´s social control theory. The social control theory, though possessing several qualities that make it a great tool with which to research delinquent and deviating behavior, poses several limitations. The main concern that surfaced when using Hirschi´s theory to answer the main research question, was the fact that his theory is decidedly individualistically oriented. This is to say that Hirschi focuses on causes of delinquency at a personal and individual level. It is the individual, or the individual´s interaction with his surroundings, that influences his behavior. Because Hirschi sees the weakened bond of society as the reason why delinquent behavior occurs, actions undertaken to discourage deviant behavior should be focused on strengthening the bond. While ethical hackers propose actions that suggest this bond should be strengthened, thus making Hirschi´s theory a useful tool for explaining their considerations, companies are more focused on what it is their own group can do to stimulate ethical behavior. Their proposals for the encouragement of ethical behavior are not aimed at the deviant individual, but at a more structural level, focusing on the behavior of companies. Hirschi´s theory and elements do not offer sufficient explanation for the considerations of the companies regarding the encouragement of ethical or discouragement of illicit behavior of hacking.

Another limitation is the selection of interviewees. Due to the practical constraints imposed on this research, only a limited amount of people could be interviewed. This is troublesome for a number of reasons, one in particular. Especially for the group of companies, the choice of respondents has undoubtedly influenced the account given by that group. Although I did try to select cross-sectoral companies, the fact that only two were interviewed obviously diminishes the representativeness. Moreover, I decided to only contact companies with a

responsible disclosure policy, because I assumed companies with such a policy would know more about ethical hacking and thus make for more interesting interviews. Although this is probably a correct assumption, it does not make selected respondents representative for the group as a whole. Those companies without a responsible disclosure policy, are more likely to be less knowledgeable regarding ethical hackers and thus be more hostile towards the hacking community as a whole. Also, the fact that I spoke to people involved one way or another in cyber security, means that they are not representative for the company as a whole. As was noted by one respondent, the views of management on the topic were markedly different from his own.

The third limitation was the availability of documentation and numbers. For one thing, it is quite hard to decisively determine the size of the hacking community in the Netherlands. Though the amount of ethical hackers is probably around 200, the number of active black hat hackers is unknown. Experts believe it to be smaller than the amount of ethical hackers, but there is no way to know for sure. Second, there is not a lot of documentation available on the behavior of ethical hackers. Because responsible disclosure is a relatively new phenomenon, obtaining an exact figure has proven impossible.

## 5.3 Suggested Further Research

Hacking, and ethical hacking in particular, is a subject that has not yet received much attention in research, especially from a governance perspective. Hence, there is still much ground to be covered. In conducting this research, I came across several findings or notions that offered suggestions for further research. First of all, a closer examination of the hacking community in the Netherlands would be very interesting. From a criminological or sociological perspective, what is it that makes hackers decide to either behave ethically or to deviate from this behavior? Research should focus on hackers when they are in their teens or early twenties, because the findings in this research suggest this is the age at which they are most likely to show deviating behavior, which also corroborates with traditional criminological views on delinquency. Through in-depth interviews with these young hackers and their environment, especially parents, more can be learnt about their motivation and behavior. Another area into which more research is

needed, is the considerations of companies. Research should include a much broader scope of respondents, including a wide array of companies differing in size, sector, and experience with hackers. Sending a large swath of these surveys, asking them about their considerations regarding hacking, would allow for a more inclusive and encompassing view of the opinion of that party. Moreover, because the Netherlands is one of the few countries with a developed responsible disclosure policy, comparison studies between the Netherlands and others would interesting. What are the effects of a more lenient policy towards ethical hackers, does this have a positive effect on cyber security? Although the effect would admittedly be difficult to verify, it would make for a very interesting research.

# Bibliography


Bachmann, Michael. 2010. "The Risk Propensity and Rationality of Computer Hackers." *International Journal of Cyber Criminology* 4 (1): 643-656.

Broekhof, Jan Martijn. 2015. *Een Verkenning van de Informatiebeveiligingsmarkt voor Intramax.* MBA Dissertation, Intermax.

Burningham, Grant. 2016. "The Rise of White Hat Hackers and the Bug Bounty Ecosystem." *Newsweek* 166 (6).

Center for Strategic and International Studies. 2014. *Net Losses: Estimating the Global Cost of Cybercrime.* Santa Clara: McAfee.

CIO Platform Nederland. 2016. *Responsible Disclosure: Implementatiehandleiding.* Den Haag: CIO Experience Group Information Security.

Computer Fraud and Security. 2013. "UK Launches Cyber-Security Reserves." *Computer Fraud and Security* 2013 (10): 2-3.

Conrad, James. 2012. "Seeking Help: The Important Role of Ethical Hackers." *Network Security* 8 (1): 5-8.

Fitch, Cynthia. 2004. *Crime and Punishment: The Psychology of Hacking in the New Milennium.* Paper, Boston: SANS Institute.

Flyvberg, B. 2006. "Five Misunderstandings About Case-Study Research." *Qualitative Inquiry* 12 (2): 219-245.

Green, D, and I Shapiro. 1994. *Pathologies of Rational Choice Theory: A Critique of Applications in Political Science.* New Haven: Yale University Press.

Hijink, Marc. 2015. *Nederland Werd te Klein voor Fox-IT.* November 24. Accessed May 1, 2016. http://www.nrc.nl/nieuws/2015/11/24/nederland-werd-te-klein-voor-fox-it.

Hirschi, Travis. 1969. *Causes of Delinquency.* Los Angeles: University of California Pess.

Hirschi, Travis, and Michael Gottfredson. 1990. *A General Theory of Delinquency.* Stanford: Stanford University Press.

Hof, Chris van 't. 2015. *Helpende Hackers.* Amsterdam: Tek Tok Uitgeverij.

Jardine, Eric. 2015. *Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime.* Waterloo, Ontario: Centre for International Governance Innovation and Chatham House.

Jordan, T, and P Taylor. 1998. "Sociology of Hackers." *The Sociological Review* 46 (4): 757-780.

Knight, William. 2009. "License to Hack." *Infosecurity* 6 (6): 38-41.

Koenis, Chris. 2014. *Securitybaas: KPN-hack een Wake-up-Call.* May 23. Accessed May 3, 2016. http://webwereld.nl/security/82653-securitybaas-kpn-hack-een-wake-up-call.

Leeson, Peter T, and Christopher J Coyne. 2005. "The Economics of Computer Hacking." *Journal of Law, Economics and Policy* 1 (2): 511-532.

Marsh. 2014. *Tien Vragen over Cyber Risk.* Amsterdam: Marsh Nederland.

Mehan, Julie E. 2014. *Cyberwar, Cyberterror, Cybercrime and Cyberactivism: An In-depth Guide to the Role of Standards in Cybersecurity Environment.* Cambridge: IT Governance Publishing.

Nationaal Cyber Security Centrum. 2013. *Leidraad om te Komen tot een Praktijk van Responsible Disclosure.* The Hague: Ministerie van Veiligheid en Justitie.

National Cyber Security Centre. 2015. *Introducing Responsible Disclosure: Experiences in the Netherlands, A Best Practice Guide.* The Hague: National Cyber Security Centre.

Nava, Eduardo Vela. 2016. *Google Security Blog.* January 28. Accessed March 17, 2016. https://security.googleblog.com/2016/01/google-security-rewards-2015-year-in.html.
Newman, Isadore, and Carolyn Benz. 1998. *Qualitative-Quantitative Research Methodology: Exploring the Interactive Continuum.* Carbondale: Southern Illinois University Press.
Ozment, Andy. 2005. "The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting." Cambridge, USA, June 2.
Pike, Ronald E. 2013. "The 'Ethics' of Teaching Ethical Hacking." *Journal of International Technology and Information Management* 22 (4): 67-76.
Rogers, Marcus. 2005. *The Development of a Meaningful Hacker Taxonomy: A Two Dimensional Approach.* Cerias Tech Report, West Lafayette: Center for Education and Research in Information Assurance and Security.
2015. *Security.* June 20. Accessed May 25, 2016. https://www.security.nl/posting/432924.
Sharma, Raghav, and A. S. Dalal. 2007. "Peeping into a Hacker's Mind: Can Criminological Theories Explain Hacking?" *ICFAI Journal of Cyber Law* 6 (4): 24-47.
Skinner, William, and Anne Fream. 1997. "A Social Learning Theory Analysis of Computer Crime Among College Students." *Journal of Research in Crime and Delinquency* 34 (4): 495-518.
Weerman, Frank M. 1998. *Het Belang van Bindingen: De Bindingstheorie als Verklaring van Verschillen en Veranderingen in Delinquent Gedrag.* Groningen: Rijksuniversiteit Groningen.
Xu, Zhengchuan, Qing Hu, and Chengong Zhang. 2013. "Why Computer Talents Become Computer Hackers." *Communications of the ACM* 56 (4): 64-74.

# Appendix A

**Questionair and Response of Ethical Hackers**

*Questions*

What do you believe the hacking community looks like?

How big a part of the hacking community constitutes black hats?

What do you think of the concept ethical hacking and the difference between white and black hats?

Should the NCSC, or a different government institution, more clearly define what ethical behavior is?

Did you yourself ever do anything that you would now consider unethical?

What do you think the government can do to stimulate ethical behavior?

Could you 'convert' black hats to being white hats?

Should (possible) hackers be taught lessons in ethics?

Do you think programs should be developed in which parents or school are more involved in hacking?

Do you think peers should play an important part in stimulating ethical behavior?

What do you think the role of the hacking community should be?

Do you believe the NCSC or other government institutions should do more regarding outreach?

In general, what do you think the role of authoritative figures should be?

Do you think policy countering black hat hacking should be focused on hackers specifically?

Do you think punishing young hackers is an effective measure?

Should young hackers be encouraged to finish their education?

Jan Martijn Broekhof

“Je merkt dat bedrijven steeds meer bewust worden van de risico’s van gebrekkige cyber security. Hierdoor is er steeds meer vraag. Aanleiding is wel jammer, want het komt vooral door de aangepaste wet meldplicht data lekken. Drijfveer is vooral financieel, het is niet zo zeer dat bedrijven hun veiligheid op orde brengen voor zichzelf. Ethical hacking wordt wel steeds meer geaccepteerd. Maar bedrijven vinden het nog steeds niet prettig om ongevraagd benaderd te worden. Het blijft een schrikreactie. Guardian360 doet dit dan ook zelf niet. Hebben we ook veel met juristen over gehad. Als ondernemer is het natuurlijk een ontzettend fijne tool om zo binnen te komen zetten. Je kan meteen het één en ander laten zien. Wel kun je al een eind komen zonder computervredebreuk te plegen, maar het echt interessante begint daarna pas. Je moet ook niet die negatieve reactie willen oproepen. Daarnaast blijkt het vandaag de dag ook niet nodig, meer dan genoeg klanten dienen zich vanzelf aan.”

“Ja, je merkt echt dat steeds meer hackers naar de legale kant trekken. De hackerswereld is wel nog steeds een beetje een subcultuur die onder de oppervlakte blijft. Daarentegen groeit de hackersscene ontzettend, zeker aan de kant van ethische hackers. Ik heb alleen weinig zicht op de illegale kant, misschien neemt dat wel evenredig toe. Lastig om te zien. Echt goede hackers lastig om te vinden.”

“Ja, er is steeds meer vraag naar ethical hackers. Plus dat de echt goede hackers een soort artiesten zijn. Die willen helemaal geen 9 tot 5 baan. Dat is een uitdaging waar veel bedrijven mee kampen. Bedrijven die echt penetration testing doen hebben moeite met het vinden van genoeg goede gasten.”

“Ja. Het heeft met meerdere dingen te maken. Deels krijgen ze bij ons uitdagingen die ze normaal niet zo snel tegenkomen omdat het dan echt volstrekt illegaal is, bijvoorbeeld bij ziekenhuizen etc rondkijken. Anderzijds is het ook ergens gewoon een kwestie van goed fatsoen. Zijn ze fatsoenlijk opgevoed, hoe staan ze in het leven, wat is je wereldbeeld.”

“Ja absoluut. Ik ben bezig met een initiatief om een tegenhanger op te richten voor file day (site waar je leaks en vulnerabilities kan posten). Bedrijven die het goed doen wil ik hier bij belonen. Dus vanuit positiviteit aandacht geven aan hacken, als je mensen beloont, dat dat ook een aanzuigend effect heeft op andere mensen. En als je kijkt naar de mindset van een hacker, die begint zich eigenlijk al rond zen twaalfde te vormen. Dus van die jongens die op die leeftijd al hun vaders computer aan het hacken zijn, eigenlijk zou je ze dan moeten leren kennen en dan heel langzaam het goede pad op leiden. Dat is wel de uitdaging. Je moet ze dus vroegtijdig herkennen en als bedrijven wil je dat wel, maja, om nou acht of negen jaar te investeren in zo´n jochie dat kost een boel geld. Dus daar ligt denk ik wel een rol voor de overheid. En het andere is dat die echt goede hackers ook niet sociaal vaardig zijn. Dat is misschien chargerend, maar dat is in zekere zin wel zo.”

“Nou ja, Anonymous noemt zichzelf ook ethisch hacker, maar is dat nou echt ethisch. Ik denk dat er een hele gradatie is binnen het begrip. Wat is nou een ethical hacker, welke gedragingen horen daar bij etc. Maar misschien moeten we ook gewoon af van het begrip hacker, het is te onduidelijk.
Misschien moet je black hats wel gewoon anders noemen, gewoon internet criminelen.”

“Ik zou dan opzoomen op ethiek. Hacken dat leren ze zelf wel en eer je een lespakket hebt is het al weer achterhaald. Wat ethiek betreft is dat wel weer de vraag hoe je ze dat leert. Vaak zijn dit juist de jongens die moeite hebben op school omdat ze alleen maar met hun hoofd bij hacken zitten.”

“Ja je zult er toch wel echt iets met ethiek moeten doen. Of dat echt les moet zijn of dat je ouders helpt ofzo. Het gaat erom dat heel veel bedrijven die ethical hackers zoeken, die zoeken toch HBO of informatica studenten. Maar de jongens die zo ver gekomen zijn zijn waarschijnlijk niet heel goed meer in hacken, die haken veel eerder af. Je moet dus veel eerder talent gaan kweken. Bijvoorbeeld door ze te begeleiden wel de havo af te maken. De Jonge Onderzoekers bijvoorbeeld doen goede dingen. Zijn een soort ‘scouting voor nerds’. Zij leren kinderen van alles over

technische dingen. Die komen elke week samen om een beetje met ledjes te klooien enzo, dat is dus naast het schoolprogramma."

"Ik heb ook onderzoek gedaan naar de grootte van de white hat community en ik kwam op een getal van 200 goede hackers. Maar dat blijft lastig in te schatten. Het blijft een klein wereldje, de meeste mensen kennen elkaar allemaal."

"Nee, als je de hackingcommunity als geheel pakt, heeft het overgrote deel het idee van we moeten dingen met elkaar delen. Die helpen elkaar ook veel. Ik denk daardoor dat je eerder kan zeggen dat hackers elkaar helpen op het rechte pad te blijven. Dat hele black hat gebeuren, dat is echt een subcultuur van het hacken als groter geheel."

Daniel Niggebrugge

"Snel willen weten hoe iets werkt en er snel kunnen achter komen hoe iets werkt. Het zijn ook wel gewoon echt slimme jongens. Ik dacht altijd dat security een niche van de IT sector was, maar dit klopt eigenlijk niet. Security is met alles vervlochten. Het is juist een enorm breed specialisme. Dit is de algemene hackers mindset. Als je bij een bedrijf als Fox wilt werken komen daar nog extra componenten bij kijken, zo is integriteit ontzettend belangrijk."

"Sowieso de discussie over de definitie van wie is white hat en wie is black hat is erg onzinnig. Er is nou eenmaal een hoop grijs in de wereld. Als ik in mijn vrije tijd op het internet en ik moet ergens gevoelige gegevens achterlaten terwijl ik het vermoeden heb dat de website kwetsbaar is, dan kan het zijn dat ik een aantal testjes doe om dit te verifiëren. Hierbij zorg ik er wel voor dat ik geen schade aan de website kan berokken, maar toch kan je je hierbij afvragen of dit nou wel ethisch is. Want ik had geen toestemming van de eigenaar van die website."

"Ja je ziet dat er een shift is in hoe mensen over ethical hacking nadenken. Dit is elk jaar aan het veranderen. De aanvragen worden elk jaar meer. Er zijn nog steeds genoeg organisaties die niet

weten waar ze het over hebben, maar er zijn veel meer bedrijven die steeds volwassener worden. Bedrijven vragen vaak of we veel verder willen gaan dan alleen een pen test, ze willen dat we de volledige veiligheid van ze testen. Je kan ook veel verder gaan dan met alleen een RD beleid, want wanneer je een inbraak hebt, zie je dat dan ook en hoe reageer je daar dan op."
"Ik denk dat er steeds meer mensen komen die het vak van ethical hacking beoefenen. Je kunt je wel afvragen of die het allemaal even goed doen, maar het worden er steeds meer. Je ziet daardoor wel steeds groter verschil in dekking in de markt, wat voor soort partijen zich aanbieden bijvoorbeeld. Er gaan wel steeds meer jongens in dat gat zitten, want de markt is er ook gewoon naar. Er zijn commerciële kansen die ook wel benut worden. Dit was dan ook wel hard nodig."

"Ja ik denk dat ethiek les geven zeker zin zou hebben. De vraag is wel of je ze dan ook de techniek moet leren. Ik denk dat het op die leeftijd lastig is om ethiek met techniek te combineren. Het ligt ook gewoon echt anders op die leeftijd. Zelfs als je begin twintiger jaren bent dan kan je ethisch besef toch ook gewoon net wat anders zijn dan later, dan zit het toch gewoon anders in elkaar. Maar ik denk wel dat het leren van hacken zeker op de HBO en uni zin heeft. Als ze het echt willen leren, leren ze het anders wel op het internet. Nu kan je ze in ieder geval beter alles bijbrengen, en daar hoort zeker ook een stukje ethiek bij. De vraag is dus of je dat op 12 jarige leeftijd al zou moeten doen. Anderzijds, als je niet over hacken leert op de middelbare school zou les over ethiek bij computer gebruik, social media en de gevaren daarvan zeker niet misstaan. Ik denk wel dat daar een grote behoefte aan is."

"Veel belangrijker dan de term is eigenlijk of je goed of kwaad in de zin hebt. Ethical hackers zijn gewoon mensen die netjes handelen als ze een lek vinden, dan mag je ze best ethical hacker noemen. De hele hacker vs cracker discussie, die heb ik opgegeven. Wat dat betreft gaat het wel gewoon echt om de goedwillende tegen de kwaadwillende mensen. De mensen die gewoon uit zijn op financieel gewin, dat is duidelijk, dat zijn geen goede mensen."

" Ik denk dat wat het NCSC heeft gedaan met het RD beleid dat dat een hele goede stap is. Maar ik denk niet dat je daar op nationaal niveau heel veel verder in moet gaan. Misschien ben ik te

beperkt in mijn denken, maar ik zie daar zelf niet heel veel meer kans. Ik zie daar zelf niet heel veel meer kans. Het blijft een grijs gebied, zeker omdat je toch mensen aanmoedigt het te doen door een RD beleid. Ze kunnen daardoor toch ongevraagd hetzelfde bij andere bedrijven gaan doen. Dus dat maakt het lastig. Het zou dan wel misschien helpen dat bedrijven standaard iets publiceren, dat dat wanneer je het niet wil je een soort van nee sticker krijgt. Verder kan je daar qua beleid weinig aan doen. Ik vond wat je over zei qua scholing, dat kinderen meer les krijgen over computergebruik en ethiek etc, geen slecht idee. Daar zou de overheid wel een rol in kunnen gaan spelen."

" Ik heb in mijn jongere jaren ook zeker dingen gedaan waarvan ik nu denk, dat was niet heel handig en dat had ik nu nooit meer gedaan. Je ethisch besef verandert dus zeker naarmate je ouder wordt. Het kan dus zeker helpen als je op jongere leeftijd hier over kan praten, als hier open over gesproken wordt en je je kan spiegelen aan anderen."

"Je zou een soort internet ouders moeten hebben, die weten waar kinderen mee bezig zijn en die actief kunnen inspringen op maatschappelijke discussies. Niet op een belerende manier, maar het gesprek met jongeren aangaan, als een soort vertrouwenspersoon. Deze ouders moeten dan wel over veel technische kennis beschikken, want je hebt ook best veel technisch begrip nodig wil je mee kunnen praten."

"Als je wil dat ethical hackers met elkaar praten moet je wel het fysieke missen, want de jongens die hier veel mee bezig zijn die zitten alleen online. Daarom zou je een soort van online community moeten hebben. Dit maakt het wel weer moeilijk omdat mensen daar dus niet per se aanwezig zijn en niet iedereen daarin zo maar vertrouwen. Er zijn vast al online communities die hier geschikt voor zouden zijn, allerlei fora etc. Blijft lastig omdat de anonimiteit makkelijk gezocht is. Je hebt ook gewoon veel einzelgängers, die wel op die fora rondkijken en al heel ver zijn in hun kunnen, maar gewoon helemaal hun eigen pad kiezen. Dan kunnen ze ook gewoon goede dingen doen, maar contact krijg je niet met ze."

Edwin van Andel

“Ja, het hackerswereldje was vroeger echt heel erg klein. Dat was de tijd van jongens als Gongrijp en het blad Hack-Tic. Het was ook amper hacken te noemen, dingen waren echt heel slecht beveiligd. Nu zou je dat wel echt hacken noemen, maar toen zagen we dat niet zo. Er werd toen heel veel met evenementen gedaan.”

“Het is ook een heel diffuse wereld. Want in het begin is alles spannend. Je doet dan ook dingen die achteraf misschien niet kunnen. Ben je dan onethisch bezig? Ik vind zolang je geen criminele doelen hebt, dus zolang je niet echt dingen gaat hacken om weer te kunnen verkopen, dan ben je niet onethisch bezig. We hadden op den duur een poster hangen waarop stond: alles wat ik deed was voor de jaren negentig dus het was niet strafbaar. Hacken was toen nog helemaal niet bekend, er waren ook nog helemaal geen wetten voor. Dus is het ook heel lastig om te zeggen dit is wel of niet ethisch. En dat is nu nog steeds heel lastig, alleen is de Nederlandse overheid met de NCSC voorop nu wel serieus goed bezig om daar wat mee te doen.”

“ Aan de ene kant merk je wel dat de houding tegenover hackers positief veranderd is, maar aan de nadere kant zijn mensen nog steeds wel heel bang voor hackers. Ik doe heel veel talks, heel veel presentaties, ook over RD en dat soort zaken. Dan merk je nog steeds dat mensen zeggen oké, als ik RD ga doen, wie garandeert mij nou dat die hacker niet mijn database kopieert. Hij kan wel melden dat hij iets gevonden heeft, dat kan hij allemaal keurig doen, maar wie zegt dat hij niet stiekem alsnog die database heeft. En dat punt, dat is waar het in Nederland nog het meest op moet. Dat is niet zozeer iets van het NCSC of wie dan ook, maar dat is gewoon iets wat echt langzaam moet greoien. En wij proberen wel echt te pushen dat hackers gewoon goed zijn. Tuurlijk heb je altijd slechte, die heb je overal wel. Maar over het algemeen zijn hackers gewoon bereid om te delen wat ze hebben, ze zijn zelfs trots om wat ze vinden, ze willen daar gewoon erkenning voor. En op dat moment willen ze juist meehelpen om het internet veiliger te maken.”

“Ik denk aan de ene kant, ik kan dat niet vastleggen, maar wat ik denk is dat er wel absoluut een shifting is en mensen die jong zijn en beginnen, die worden op dit moment steeds meer naar de ethische kant dan naar de negatieve kant.”

“Nou met name door twitter en dat soort communicatie. Je hebt op twitter wel eens mensen die melden waar ze mee bezig zijn en dan heb je in Nederland mensen als Ricky Gevers die daar dan heel fel op zitten. Als iemand aan het ouwehoeren is, dan pakt Ricky ze virtueel in het nekvel en zegt, gast waar ben jij nou mee bezig. Ricky is zelf ook gearresteerd geweest, dus die weet precies hoe het allemaal werkt. En er zijn in Nederland wel meer, een groepje, jongere hackers die een beetje afwijken om die weer een beetje terug te duwen naar het normale. Een soort van sociale controle.”

“Opzicht denk ik dat, wat het NCSC bijvoorbeeld goed doet, is ook naar hacking events gaan. Jeroen loopt bijvoorbeeld op heel veel van dat soort dingen rond. Nou dat was voor die tijd heel lastig en nou kan dat gewoon. En daardoor krijg je wel in die hackerskringen wel gewoon respect en eerder de neiging om te melden en de goede kant op te gaan. Tuurlijk blijven er altijd negatieve jongens maar wat je ziet is wel de criminele markt verschuift zich heel erg naar Rusland en dat soort landen. Die worden wel steeds professioneler.”

“Mensen gaan ook kijken, want tot hiervoor was security iets daar moest je geld in stoppen maar je zag niks. In Nederland is dat dan ja, zonde geld, kan je beter wat anders voor doen. Nu ligt er een boete en heel veel druk op en moeten ze wel, en nou komen ze er achter oké dan kunnen we beter.. daarom zie je dat cyber security, security in het algemeen, in Nederland echt aan het groeien is. Bedrijven schieten aan alle kanten de grond uit, Fox is flink goed verkocht, dat loopt als een dolle.”

“Volgens mij is er in Nederland nog nooit iemand streng gestraft voor een inbraak. Denk dus ook niet dat het bij Nederland pas om daar streng voor te gaan straffen. Aan de andere kant denk ik dat het ook gewoon heel lastig wordt, want de jongens die je dan pakt zijn inderdaad de jongens

die gewoon gepakt worden. En dat klinkt een beetje raar, maar de criminelen die het echte geld verdienen zitten in het buitenland, in Rusland. Die doen dat via zulke ingewikkelde wegen dat je ze niet kan pakken. De jongens die je wel pakt zijn de genen die iets nadoen, dat zijn juist de jongens die je nog wel de goede kant op kunt krijgen. Als je die dan hard gaat straffen, wegzet voor vijf jaar, komen ze nooit meer aan het werk."

"Nou bijvoorbeeld door hackers veel meer te laten spreken op evenementen. Daarom is het ook zo goed dat we zijn gevraagd om mee te gaan naar dat hoogambtelijk EU overleg. Dan kan je de mensen die daar aanwezig zijn kennis laten maken met een hacker. Dat een hacker niet eng is, dat ie gewoon normaal praat enzo. En als je daar steeds meer bewustwording voor creert dat RD werkt, dat bug bounty´s werken en hoe ze werken, dat je dan langzaam wel een shift krijgt die daar naar toe gaat."

# Appendix B

**Questionnaire and Response of Companies**

*Questions*

What do you believe the hacking community looks like?

How big a part of the hacking community constitutes black hats?

What do you think of the concept ethical hacking and the difference between white and black hats?

How do you generally view hackers; as a threat or as an opportunity?

Should the NCSC, or a different government institution, more clearly define what ethical behavior is?

What do you think the government can do to stimulate ethical behavior?

What do you believe the role of companies should be?

Could you 'convert' black hats to being white hats?

Should (possible) hackers be taught lessons in ethics?

Do you think programs should be developed in which parents or school are more involved in hacking?

Do you think peers should play an important part in stimulating ethical behavior?

What do you think the role of the hacking community should be?

Do you believe the NCSC or other government institutions should do more regarding outreach?

Do you think policy should be focused on hackers specifically?

Do you think punishing young hackers is an effective measure?

Should young hackers be encouraged to finish their education?

<u>Wim Daalhuizen - Intergamma</u>

“Maar daarentegen denk ik niet dat je er het aantal hack aanvallen mee kunt verminderen. Ik denk dat je de impact kan verminderen. Mensen zullen het altijd blijven proberen en op het moment dat ik de gaatjes dicht heb, is het veel lastiger. Een echt gerichte aanval doe je echt bijna niks tegen. Het enige wat je dan kan doen is het zo snel mogelijk detecteren en dan proberen op te lossen. Maar de gewone huis tuin en keuken hacker heeft het best lastig. Daar is RD heel nuttig voor. Ik zie het dus als een mechanisme, als een laag.”

“Ethical hackers: hoe meer hoe beter. Maar dan wel echt ethical. Misschien is dat dan in mijn hoofd, maar ik vind een hacker die ergens op een site probeert iets te vinden in een omgeving zonder RD en dat vervolgens gaat melden, die is voor mij al een grens te ver. Volgens mij mag je ethical alleen zijn op het moment dat je toestemming hebt. Hoe je die toestemming hebt verkregen, via contract of wat dan ook, zonder die toestemming ben je niet ethisch bezig. Dus ja, hoe meer ethical hackers hoe beter.”

“Nee, black hat hackers terugkrijgen naar de ethische kant, dat lukt je met geen mogelijkheid. Er is veel te veel geld in te verdienen. De echte black hats kunnen vanuit een vrij beperkte investering zo ontzettend veel geld verdienen. Als je jongens ethiek wilt leren, dan moet dat als ze jong zijn. Sowieso, hoe breed ga je met hacking. Mensen die denken vaak, oeh hackers, hackers zijn eng. Bij onze directie schrikken ze nog steeds van de term hacker, dan moet ik ze uitleggen dat hacken niets meer is dan het verzinnen van creatieve oplossingen voor problemen. Maar als je.. Ik heb ooit een keer een presentatie gezien van McAfee van een bank in Rusland, daar hadden criminelen een bank gehackt en spoot het geld letterlijk de ATM´s uit. Kijk je hebt hackers en cybercriminelen. Dat een cybercrimineel gebruikt maak van hacking.. Ik heb niet het idee dat je zo veel full time black hat hackers hebt. Die zijn er misschien wel, maar is Gamma dan interessant. Is ook een afweging die je maakt. Komen die bij ons langs, of gaan die naar een ander? Overheden, defensies, dat soort dingen gaan die heen. Ik zie het concept hacker en cybercrimineel echt als twee verschillende dingen. Dat zou net zoals zijn als dat ik een slotenmaker en een inbreker hetzelfde noem. Hacken is opzicht een positief iets. En hoe vaak we dat ook zeggen, toch komt het iedere keer weer terug. Nee, op het moment dat je probeert

duidelijk te maken wat een hacker is, dat wordt gewoon slecht begrepen. Cybercriminelen maken gebruik gewoon gebruik van hacken."

"Tja, dan kom je weer in die hele cracker vs hacker discussie terecht. In feite is een hacker zoals wij die gebruiken ook bij RD, iets voor bij een seuciryt test, punt. En die vindt dingen of die vindt geen dingen. Als ik een pen tester gebruik, is dat dan een hacker of is dat geen hacker? Ik denk alleen niet dat je die termen positief krijgt."

Jeroen Diepenmaat – Moneybird

"Wij waren sowieso één van de eersten die een RD beleid online hadden gezet. Het is een goed onderwerp, laat ik dat voorop stellen. Een van de belangrijkste dingen in onze sector, we zijn een financiele dienst, nog geen bank, maar we slaan wel ontzettend veel belangrijke data op. Misschien wel meer kritische data dan banken. Wat je ook doet, als je gegevens opslaat, moet je daar als bedrijf bewust van zijn en moet je daar naar handelen. RD is een continu proces waar je als organisatie gewoon bewust van moet zijn en mee bezig moet."

"Sinds we Moneybird opnieuw gereleaset hebben, toch wel een melding of 25. Daar zitten ook high priority dingen tussen, naast de minder dringende zaken. De jongens die die meldingen doen weten ook echt waar ze mee bezig zijn, dat zijn echt lastige dingen. We zijn nog nooit echt gehackt, maar ik denk ook dat dat te maken heeft met ons RD beleid."

"Ik denk absoluut dat er een causaal verband is tussen ons RD beleid en het feit dat wij nog nooit zijn gehackt."

"In principe heb ik vooral positieve gevoelens richting hackers. Het woord hacker is natuurlijk lastig. Ik heb eigenlijk alleen maar contact gehad met jongens die via RD contact met ons opnemen. Ik heb alleen maar respect voor die gasten. Misschien worden we ook wel gesympathiseerd door die groep omdat we als één van de eersten een RD hadden."

“Hacken moet in Nederland een veel luchtiger begrip worden. Als je politici af en toe hoort roepen over dat ze gehackt zijn, terwijl ze gewoon hun wachtwoord hebben opgeschreven, dan merk je dat er gewoon ontzettend veel onbegrip voor hacken is. Ik vraag me ook af: wat kan er nou nog beter zijn dan RD?”

“Ik pleit er ook voor dat ethical hacken een stukje in onderwijs moet gaan worden. Heel veel ontwikkelaars komen uiteindelijk op het web terecht. Er zouden ook lessen in ethiek gegeven moeten worden.”

“NCSC doet het echt best oké. Er zijn gewoon te weinig ondernemers die zich daar aan houden. Er valt vooral veel terrein te winnen op het uitvoerende terrein.”

# Appendix C

**Questionaire and Response of Government**

*Questions*

What do you believe the hacking community looks like?

How big a part of the hacking community constitutes black hats?

What do you think of the concept ethical hacking and the difference between white and black hats?

Should the NCSC, or a different government institution, more clearly define what ethical behavior is?

What do you think the government can do to stimulate ethical behavior?

Could you 'convert' black hats to being white hats?

Should (possible) hackers be taught lessons in ethics?

Do you think programs should be developed in which parents or school are more involved in hacking?

Do you think peers should play an important part in stimulating ethical behavior?

What do you think the role of the hacking community should be?

Do you believe the NCSC or other government institutions should do more regarding outreach?

Do you think policy should be focused on hackers specifically?

Do you think punishing young hackers is an effective measure?

Should young hackers be encouraged to finish their education?

<u>Jeroen van der Ham</u>

"Ja, het afgelopen jaar is er echt een shift aan het plaatsvinden. En dat is best wel snel gegaan eigenlijk. Het RD (Responsible Disclosure, MB) beleid is in 2014 ingevoerd en toen begonnen eigenlijk alleen de banken en ISP´s (Internet Service Providers, MB), maar vrij snel volgden ook

andere bedrijven en tegenwoordig zie je dat steeds meer bedrijven het doen. Of in ieder geval dat ze er van af weten. Er zijn een heleboel die er van gehoord hebben."

"Ja, het is een positieve ontwikkeling dat er een markt ontstaat en nee, daar hoeft de overheid niet scherper op te zitten. Kijk, hoe ik het zie, is dat je als overheid ruimte creëert voor het bedrijf en de melder om met elkaar in contact te komen, zonder dat de overheid zich daarmee hoeft te bemoeien. De overheid hoeft daar pas aan te pas te komen als het mis gaat. Dan pas moet de overheid bijsturen, dat is hoe ik het zie."

"Ik worstel inderdaad een beetje met hoe ethisch handelen beter gedefinieerd kan worden. Daar ben ik over na aan het denken om dat beter te kunnen omschrijven. Maar uiteindelijk gaat het om de regels, heb je regels nodig om het goed te kunnen beoordelen. Dat is ook waar het OM mee worstelt. In principe wil je de intentie kunnen vangen, de intentie waarmee je een bepaalde uitspraak doet, maar die intentie kun je alleen maar vangen in gedrag. Die kun je van te voren niet omschrijven of vangen in regels. Het vangen van intenties in regels is ontzettend lastig. Het OM probeert nu met de opgestelde regels dat wel te vangen. Dat lukt nog niet helemaal goed. Intenties kun je heel moeilijk vangen in regels, maar uiteindelijk kan je alleen objectief beoordeeld worden op hoe je je gedragen hebt."

"Ja ik denk dat je dat gedrag op school kunt stimuleren. Wat ik gedaan heb bij die opleiding, in de ethische commissie, ik denk dat dat al een heel besef heeft gebracht."

"Of je twaalfjarigen al les in ethiek moet geven is wel een probleem waar ik mee worstel en waarvan ik niet goed weet hoe we dat moeten oplossen. Ik denk in eerste instantie is het haalbaar om bij dit soort studenten, maar dan bij alle studenten in Nederland, om dat besef binnen informatica beter te krijgen. Ik denk dat je dan al een hele grote slag maakt, op het moment dat je daar kritische massa krijgt dan zal ook de hele informatica community daar anders tegenaan gaan kijken. Dat mensen die er later bijkomen er ook anders tegenaan kijken. Daarnaast, ik zit daar nu een beetje over na te denken, maar het is natuurlijk heel erg moeilijk om een twaalfjarige of zestienjarige ethiek bij te brengen. Als je kijkt naar het brein van een zestienjargie, dan is dat morele besef nog ontzettend in ontwikkeling. Juist bij pubers zie je dat ze acties ondernemen waarvan ze de gevolgen niet onderzien."

"Ik ben daar wel over aan het nadenken geweest. De belangrijkste is de derde partij, de peers, dat je die als eerste aanpakt. En dat doe je denk ik door het op de hogere opleidingen in te brengen. En van daar uit, misschien een tweede stroom, dat je via hackerspaces meer voorlichting probeert te doen. Dat je tegen ouders zegt, om ze te ondersteunen, stuur die jongen eens langs bij een hackerspace en laat hem eens praten met mensen."

“Ja, ik denk opzicht wel dat er een grotere rol voor de hacking community is. Het gebeurt inderdaad wel dat de hacking community hackers die onethisch gedrag vertonen en daarover opscheppen op hun plek worden gezet. Ik probeer daar af en toe wel als ik dingen zie om daarin bij te sturen, maar ik zie het niet echt als mijn taak om die jongens bij te sturen. Ik denk dat dat door de community zelf gedaan moet worden. Maar de manier waarop dat gebeurt dat probeer ik wel zelf te beïnvloeden. Dus meer na te denken over de ethiek daar van en er over na te denken over wat voor acties je onderneemt ipv alleen maar te kijken naar de gevolgen.”

“We proberen natuurlijk steeds meer RD uit te dragen, dus we proberen aan de ene kant de community te steunen door RD uit te dragen en dat ook duidelijk te maken, want één van de veelgehoorde klachten vanuit de community is nog steeds, maar ja mijn positie is onduidelijk. En ik denk dat we nu juist door de twee rechtszaken die zijn geweest dat het wel al iets duidelijker is geworden, dat er wel al een soort van bescherming bestaat, dat je niet zomaar gepakt kan worden.”

“Ik ben redelijk actief in de hacking community. Maar, dat is wel eigenlijk alleen in de zichtbare hacking community. De mensen die naar bijeenkomsten komen, de mensen die naar hackerspaces gaan, dat soort mensen. Dat zijn de wat meer actievere en zichtbare mensen, die onzichtbare groep die zie ik niet. Daar weet ik ook niet zo veel van.”

“Nee, de zichtbare niet zo. Het zijn meer de onzichtbare en bijvoorbeeld die types die laatst bij DWDD was. Die jongen die was in de VS veroordeeld en heeft daar opgesloten gezeten. Die was een beetje afgegleden en als stoere puber een beetje begonnen en is langzaam aan afgegleden. Daaraan zie je ook dat het niet per se een black of white het te noemen is, maar een beetje grijs en toen op een gegeven moment afgezakt.”

“Ik weet niet hoe je het afzakken zou kunnen voorkomen. Dat weet ik niet. Dan kom je weer terug op die drie groepen, ouders, school en peer. Die ouders wisten helemaal niet wat hij aan het doen was, de school ook niet. Het punt is ook gewoon, dit gaan we ouders niet zomaar leren. Scholen hebben nu ook niet de capaciteit om hier iets mee te gaan doen, dus dan kom je weer terug op die peers.”

“Lesgeven op school in ethiek zou ideaal zijn, maar tegelijkertijd moet je ook wel realistisch zijn over hoe lang dat dat duurt, voordat dat daadwerkelijk er is. Dat is een hele lange tijdsspan. Inhoudelijk is de lesstof best goed te doen, maar het vinden van de juiste mensen om de les te geven en het onderwijs op gang brengen dat is gewoon moeilijk.”

Alf Moens

“Nou dan moeten we die community in twee splitsen. Er zijn heel veel jonge, maar ook ouderen die enorm veel verstand hebben van hoe IT in elkaar zit, van hoe applicaties in elkaar zitten en die daar voor hun eigen plezier gewoon ook mee bezig blijven om zich daarin te verdiepen en ook rondkijken overal. Vanuit dat oogpunt, mensen die daar mee bezig zijn, dat waardeer ik heel erg, ik vind het knap dat ze zich daar zo in verdiepen en er zo veel van af weten, maar ook dat ze ook even tippen van hier is iets aan de hand of daar moet je eens naar kijken. Of wel direct naar ons of in zijn algemeenheid van goh, met dit en dat systeem is iets aan de hand en daar moet iets mee gebeuren. Dat deel, als je dat de hacker community noemt, daar heb ik zeer veel respect voor, als zij gewoon signalen afgeven. Als dat binnen zijn limiet blijft. Ze weten vaak ook wel wat ze moeten doen om binnen limiet te blijven.”

“Je ziet dat hackers die dat initieel vanuit hobby doen, dat die zich langzaam aan ook beginnen te organiseren omdat het in sommige landen wat moeilijker is om je bevindingen onder de aandacht te brengen dat ze zich gaan organiseren om dat via een bedrijf aan de aandacht te brengen. Dat traject en de professionalisering vind ik geen probleem, behalve als dat de kant op gaat, dat wanneer je een belletje krijgt van goh, er is wat aan de hand, hoeveel heb je er voor over. Ik ben geen google die een bounty programma heeft, dus vertel me wat er aan de hand is en dan kan ik misschien een aardigheidje voor aanbieden. Dat is niet iets waar iemand van kan leven. Daarom waardeer ik dat ook, omdat het iets is dat je in je hobby tijd doet. Maar als dat professionaliseren commercialiseren betekent, dan denk ik van ja, dan gaan we niet de goede kant op. Het andere aspect van hackers, dat zijn de kwaadwillende. Die willen inbreken, data verzamelen of wat dan ook, die moet je hard aan pakken. Dat is gewoon criminaliteit, het lijken fietsendieven omdat de pakkans klein is, maar het zijn bankrovers. Dus dat moet gewoon echt veel meer via opsporing en repressie aangepakt worden.”

“Tuurlijk moet je de boel goed beveiligen, maar repressie is een belangrijke manier om de boel aan te pakken. Ik denk dat, hoe goed je ook beveiligt, als iemand echt wil komt ie er wel in. Combinatie van social engineering en technische vaardigheden die komt er doorheen vroeg of laat. Die aanvallers, die willens en wetens gewoon bij je binnen willen komen en schade berokkenen, of dat nou gericht is of ongericht, dat is criminaliteit.”

“Lesgeven op twaalfjarige leeftijd. Waar moet je dan die les gaan geven? Dat moet je niet op elke middelbare school gaan geven, want dat slaat gewoon niet aan. Afgezien van algemene ethiek les, van wat doe je wel en wat doe je niet, maar dat wordt al wel veel gedaan in het onderwijs. In de tijd waarop ik op middelbare school zat, daar kwam ook gewoon aan de orde

wat je wel en niet moest doen. Maar je moet ook net maar openstaan als tiener voor dat soort boodschappen. Goed, je moet het niet achterwege laten, maar het effect ervan is natuurlijk beperkt. Kijk, je hebt wel mogelijkheden als je zegt, ik ga dat organiseren. Dat ik organiseer dat een groep ethische hackers, dat die zich als ethische hacker inzetten en ik zeg, kom maar testen. Daar is een aantal jaar geleden na Lektober is vooral die roep geweest, laten we hackers inhuren die onze systemen komen testen. Dat de methode waarop je dat moet doen, want dat is gewoon commercieel of semi-commerciele activiteit. Er zijn wel bedrijven die dat doen en die bedrijven hebben ook een aantal van dat soort jongen in dienst. Of hebben daar een relatie mee, afhankelijk van welke structuur ze daarin hebben gekozen. Om dat verder te organiseren denk ik van ja, wat organiseren we dan eigenlijk. Waar ik wel in geloof is dat je, als ik zeg ik organiseer iets van een hackaton ofzo. Dat je zegt, ik heb hier een systeem en ik ben wel benieuwd of daar wat mee aan de hand is. Is natuurlijk vragen om problemen als je dat doet, want vaak wordt het hartstikke onderuit geschoffeld, maar dat is natuurlijk een mogelijkheid. Maar ja, ik denk niet dat je veel verder moet gaan. Dat je dit moet institutionaliseren. Het blijft gewoon eigen verantwoordelijkheid van jou als leverancier en van jou als organisatie. Je ziet wel bij grote leveranciers en software ontwikkelaars dat die dat op een andere manier oppakken met hun bounty programma´s. En eigenlijk is dat een, dat lijken heel grote bedragen, maar wat ze eigenlijk zeggen is ja, we hebben eigenlijk geen middelen om zelf uitgebreid onze software te testen, we gooien dat in de markt en laat ze maar kijken of iemand daar nog problemen mee heeft.”