Cyber safety considered

An introduction in two readings

Wouter Stol

Boom Juridische uitgevers
Den Haag
2010

Cyber safety considered

In memory of my father
Dr Ph.Th. Stol
(1924-2002)

Preface

On September 1 2004 I began my first term as lector, with the newly inaugurated Integral Security lectorate at the NHL University of Applied Sciences. One of the lectorate's main themes was 'safety and technology'. During the course of the first lectorate period (2004 to 2008) it became apparent that those working in the fields of policing, justice and social assistance had concerns about safety in cyberspace. To address these issues, the lectorate launched a Cyber Safety course at the end of the first term, on September 1 2008.

At the time, cyber safety was an unknown concept. We knew about cyber security (protection) and cybercrime (crime), but no attention was paid to safety in the broad sense of the word, as it is understood in the world of Integral Security. But today, through Google, 'cyber safety' produces about 580 search results on Dutch sites. Knowledge centres working on research and education in the field of cyber safety can be found on www.cybersafety.nl - the digital platform of the Cyber Safety Research and Education Network (CyREN), an organisation initiated by the lectorate.

In 2008, the NHL University of Applied Sciences and the Open University (OU) launched a strategic collaboration. This included the creation of an endowed chair, 'Police studies', one which pays particular attention to cyber safety. I was nominated for this chair on June 15 2009.

In 2010, the NHL University of Applied Sciences and the Police Academy agreed that Cyber Safety would be a combined lectorate for both institutions, a joint effort for a mutual goal: more safety in cyberspace. Three knowledge centres: the NHL University of Applied Sciences, the Open University and the Police Academy agreed to collaborate. Together they work on research and education in this new field of expertise, which is a good thing given the demands of this new and complex field.

In 2010 I held my public lecture (May 19) and my oration (September 2). This book contains both of these texts. Although we've kept repetition to a minimum, it was not possible to prevent a certain amount of overlap in the texts, an explanation of what cyberspace is, being a case in point. Hopefully the readers will forgive me for this.

This book is intended to be more than a documentation of two ceremonial occasions. It can be used as an introduction to the field of cyber safety. It is for students of Integral Security, Forensic sciences and Information Technology at college level for Police Academy students as well as for people who would like to become acquainted with this material in their professional capacity. This book can also serve as a background document for developing policies on cyber safety within the judicial system.

Developments in cyberspace move quickly. These two texts were written in 2010; their shelf life is limited in the sense that technical possibilities and trends in cyberspace are changing continuously. At the same time, research is producing new insights into the nature and scale of the issues at hand – or so we hope. Nevertheless, the fundamental principles of technology and safety under discussion will remain relevant for a long time to come.

Wouter Stol
10 September 2010

1 Cyber safety: an exploration

Lecture

For the Cyber Safety Lectorate of the NHL University

presented in an abridged version

on 19 May 2010

by Prof. dr W.Ph. Stol

Honourable members of the Board of the University, colleagues and other interested parties, dear family and friends – and among you especially my mother, because she shows us that it is perfectly possible to live without cyberspace, and especially too my sons, Ivar and Roald, because they make it clear to me that there is no longer a life without cyberspace,

I will start by telling you how cyberspace came about, or rather, what caused the rise of cyberspace. And it may not be as you think. This will be followed by a short personal intermezzo. After that, I will talk about cyberspace and abnormal behaviour; I will tell you about how the Cyber Safety Lectorate came about and I will share with you some of the lectorate's research findings. We summarised one of the most important findings with the words 'Cybercrime belongs to the people'. This is not a revolutionary call to arms, it is simply an observation. Cybercrime *does* belong to the people.

As Cyber Safety lector, I not only feel responsible for research, but I also feel that I should be contributing to education. I will therefore ensure that by the end of the afternoon you will all be able to hack a computer. You will all come away with that skill, at the very least. But first let's start with a brief social analysis of the origins of cyberspace.

1.1 Prologue: a brief social analysis

For about century now, we, the human race, thought that we had just about finished mapping our world. After we had reached the North Pole, and shortly afterwards the South Pole, in the first decades of the twentieth century, it seemed as though there was not much undiscovered space left, at most a few remote places in the vast jungles of the southern hemisphere and one or two deep troughs in the ocean. No Major Missions remained, no final frontiers of an unknown world that appealed to everyone's imagination. The Norwegian Roald Amundsen claimed the last great trophy when he reached the South Pole. Explorers, seeking new worlds with unknown horizons, had to rely on the space between the planets and the stars for new discoveries. To discover new worlds we had to travel further and search harder. This was the privilege of an extremely limited elite: a handful of astronauts and few mainly western scientists with exorbitantly expensive equipment. Humanity as a whole was trapped as it were, both physically and spiritually, within the boundaries of the world around it. But then, from a position of distress, through its yearning to expand and from a sense of creativity, *homo technologicus* created a new world within existing space: cyberspace. Once again there was air and space, space to see new possibilities, space to take new paths, space for hope and optimism, space for inspiration and discovery, space for creativity and freedom. Space not only for a few scientists, but for many. Here is a quote about new developments in Kenya as an example:

> *'As opposed to the older hippo generation, that still complains about colonialism and imperialism, the cheetahs are taking charge. They are connected to the web, are joining online networks and are urging others to join in. (…) The Internet has given them the key to drag Africa out of the gutter. Or, as Tonee Ndungu puts it: "We lived on a glimmer of hope. Finally, finally we can reach it and grasp it." Ndungu, too, is a real cheetah.' (de Volkskrant, March 25 2010)*

Tonee Ndungu is not the only one who shows us the relationship between the Internet and this new living space. The current president of the United States, Barack Obama, made intensive use of the

Internet to achieve his presidency. And after he became president he announced that he wanted to put an end to the programme for manned space travel.

With this brief social analysis I place myself in the tradition of optimistic social scientists, among whom I would like to mention the American Lewis Mumford as an important exponent of this movement. The optimism that he brings to the fore in his unparalleled study *Technics and civilization* – from 1934 – encompasses two points.

Mumford demonstrates convincingly that it is not so much technology that determines the path of history, but the spiritual development of man, in other words: culture. It is not the chance technological inventions of ingenious or disturbed engineers that decide the path of history, but the mental state in which society finds itself that determines which technology society produces. In the social analysis I have just sketched, it is no coincidence that the Internet arose at a time when, for decades, people no longer had the prospect of pioneering new territories The fact that the majority of people never roam the earth anyway does not detract from this. The issue here is the lack of prospects, the shortage of space to explore. Contrary to what we are told, worldwide cyberspace is not merely the result of a few boffins stringing together a bunch of computers. That explanation is too simple. Cyberspace is the result of the fact that humanity, because of a lack of room to explore in its everyday world, found itself in a state of mental imprisonment. Cyberspace is the answer to the shortage of opportunities to pioneer and explore.

Secondly, Mumford vehemently defends, and in my opinion successfully, the claim that people are not only capable of launching new technologies, but also of steering them, and even changing their direction. We are not doomed, like a sorcerer's apprentice, to be destroyed by the technological force that we unleash – provided we do not want to.

Mumford died in 1990 aged 94 and missed the breakthrough of the Internet. Yet his approach to technology is appropriate even when it comes to the Internet. After all, there is no point in making an effort to improve things unless you are convinced that man's intellectual force and his capacity to influence things is more powerful than 'technology' or some other invisible hand that determines the course of history for us. We, you and I, *do* live in the world of the Internet. It is therefore our responsibility to allow cyberspace to be an environment that inspires people and gives them the opportunity for progress and new, promising discoveries.

This is no paltry task; it is demanding of those who take it on. Roald Amundsen and his fellow explorers had to battle cold, exhaustion, malnutrition, polar bears, injury, sledge accidents and many other hazards. This is not hard for us to imagine. Yet these pioneers struggled within their teams with boredom and bad relationships, to the point of treachery, theft and murder. When people live together, not only must they defend themselves against the elements, but also – and I think especially – against each other. Security is a basic requirement for any human endeavour, be it the conquering of the North or South Pole or developing the *terra incognita* of cyberspace.

People are always the instigators behind the dangers of cyberspace. Security in cyberspace is not so much a technological problem or aspect of physical safety – as security experts call it. Instead it is first and foremost a question for the social sciences such as sociology, psychology, criminology and jurisprudence. The technological sciences play a supplementary role.

The concept that is central to safety in cyberspace is behaviour and ultimately the main issue is how to influence people's behaviour in such a way that it does not cause insecurity. Or better still: so that people can protect themselves and others effectively from risks. This practical 'how question'

('How can people's behaviour be influenced in such a way that it enhances safety?') is not a simple one to answer. The first thing is to find out what the safety issues are , what their background is and how they develop. Only then is it possible to consider properly how to tackle the problems, and decide what can be done to make cyberspace safer. But there's the rub: we know very little about insecurity in cyberspace. And we therefore know very little about how to effectively tackle it. This lack of knowledge is the reason I stand before you today. I will now allow myself to take a short intermezzo to give you a personal introduction. But after that we must get to work. There is much to be done.

1.2 Personal intermezzo

I believe it was more or less by chance that I ended up in the world of safety and technology. In 1983, 27 years ago already, Commissioner Wil van Ingen of the Amsterdam police force was looking for a young inspector for a project to renovate the central command and control room. Part of this project was the computerisation of the control room: the report cards were to be replaced by a computer system. I am not sure why he asked me to do this job. I can only remember that he was looking for someone who had recently joined the force so that that person would be around to finish the job. The more experienced inspectors and chief inspectors were often transferred. I knew nothing about computerisation, and at 25 was still new to the police force, but at the time this was apparently not an impediment to becoming a project manager to computerise the central reporting and information centre of the largest police corps in the Netherlands.

At the time I was studying sociology alongside my work. I am interested in people and how they live and work together. As part of my study, and to combine my work with my study, I researched the consequences of the control room computerisation on job quality (Stol, 1988, 1990). It was at a time when computerisation was associated with job losses and task erosion. Together with a fellow student and friend, Fons Panneman, I also gave courses to trade union managers about the consequences of computerisation to, for example, job quality and task load. These days these are themes that no one worries about anymore.

The exciting combination of work and an increasingly technological environment suited me well. In my curiosity I noticed the introduction of basic processing systems (BPS): typewriters were being replaced by computer systems that police officers used to do their paper work. Before I graduated, I studied this phenomenon as a type of office automation. Later, for my thesis research, I asked myself whether the police would use the information that they had been saving about addresses and citizens for their work on the streets, and if they did, what the consequences would be (Stol, 1996). I hung my police hat upon the willows and decided that in future I would be a researcher in the field of policing. In the years that followed I became engrossed in the use of the various police computer systems.

Once my thesis was finished, I allowed myself to get an Internet connection. I became an active user straight away. In 1996 I became part of the virtual police communities, particularly those in the US because there was very little going on in the Netherlands at the time. I learned how to design web pages and started The Dutch Police Pages, which I managed with my colleagues for a year after that. The management of this site was later taken on by politie.nl.

After a period in which I was only online as a user, the Ministry of Justice gave me the opportunity to do research into the nature, seriousness and combating of crime in cyberspace (Stol, Van Treeck & Van der Ven, 1999). Even though I have done research into various subjects in the interim, among others 'police and the youth' and 'violence in nightlife settings', safety in cyberspace remained a special theme in my work, a theme that continues to intrigue me. It is my old love of the combination of work and technology, the tension between being a human and machines, the tension between feelings and reason, between human emotions and calculation, and now, thanks to the Internet, all of this is more complex and therefore more interesting than all the other aspects that I have researched in the past.

What makes cyberspace so special from a security point of view? What *is* cyberspace in fact? Is cyberspace, alongside being virtual, not fictitious? Should we be concerned or is it simply a question of 'just don't switch on the computer and then you won't be bothered by it', which is what a police officer advised a woman who was being stalked in cyberspace?

1.3 Cyberspace and safety

Cyberspace

Internet belongs to the category of technology that has been of immense importance to social development. Other technologies in the same category include the art of writing (3,200 BCE), printing presses (1,000 CE), the telegraph (1833), the telephone (1876), the television (1927), the computer (1943) and the mobile phone (1973). Without doubt the invention of writing is the greatest innovation of all time. To be able to invent writing, people had to dare to believe that their thoughts could go their own way, separate from their bodies, that spirit and body were not an indivisible unit. That seems to me to be the biggest mental adjustment in the history of humanity. The Internet is an almost direct extension of this.

The Internet belongs to the category of innovations that I have just mentioned, but it is different to the rest. The Internet is not merely a method of communication; people also build social structures on the Internet. Social structure is the sum of all more or less fixed patterns of human interrelationships. Alongside communication between people, this includes the rules, the infrastructure and all the other aids that people use to maintain their relationships. People cannot pretend structures don't exist or even ignore them; they have to take them into account. Social structures arise through the comings and goings of people, and once structures have been formed, they in turn give direction to what people do. Giddens (1984) called this characteristic the duality of structure.

Even if no one were on the Internet, there would still be domains, websites, profile sites, search engines, chat rooms and all their interconnections. Whoever enters the Internet has to take its structure into account. The social structure within the Internet is what we call cyberspace.

The social structure on the Internet channels people's behaviour. In this sense, cyberspace has compulsory aspects. If you are looking for information, you use a search engine. If you are looking for contact with other people, you use social networking sites. You have to follow the beaten tracks that a handful of 'techno-anarchists' leave. A few innovators come up with new paths, which does not detract from this general principle. The structures are not only compulsory, they also offer opportunities. People with similar interests who would never have found each other in the past now meet thanks to these structures through search engines, websites and virtual communities.

Because the Internet has a social structure it resembles a real society. An important difference is its virtual character: the absence of a physical environment. This means that distance and time differences on the Internet play a minor role. In terms of safety, it is more important that people are physically absent. Summarised, the two most important characteristics of the Internet are:

1. It has a social structure that we call 'cyberspace' and that compels people's behaviour in certain respects but at the same time it offers new opportunities.
2. The social structures of the Internet do not have a physical environment: distance and time play a minor role and people are physically absent.

Cyber safety

The theme of my lectorate is cyber safety, or in other words: safety within the social structure of the Internet. I will briefly delineate the boundaries of my profession and will then look at the relationship between the Internet and safety.

Safety is the effective protection against personal suffering: protection against the infringement of physical or mental integrity. Safety is a broader concept than crime, a concept that only refers to the committing of crimes. Cyber safety therefore encompasses more than cyber crime. It is most obvious in the context of youth and cyber safety where Internet addiction, cyber bullying and communication with unwanted sexual connotations come to mind. While the boundaries of what is and what is not a crime are by no means always clear, insecurity begins are soon as someone is harmed or as soon as they *perceive* that they are being harmed.

I argue, by the way, for a somewhat flexible approach to physical or mental integrity of *individuals*. Were we to strictly adhere to integrity of individuals then the phenomena that were not directly threatening to individuals, but to social integrity instead, might be overlooked. Here I have in mind the so-called victimless offences (e.g., illegal trade) and the rise of criminal structures or links between the underworld and lawful society (e.g., laundering through business activities cyberspace).

It is also appropriate to emphasise what is not included in this field. I have two remarks in this respect. Firstly, information protection technology is not part of the field of cyber safety. Information protection is undeniably relevant to the field. The nature and extent of protection also determines, for example, whether cyber criminals are successful. But protection technology is not directly the object of research within the field of cyber safety – just as alarm systems are not directly linked to research into robberies.

Secondly, cyber safety concerns safety within the Internet's social structure. Using the Internet when working on safety in the offline world is therefore not relevant. While Internet sites such as www.depolitiezoekt.nl, where the police post photographs of people they are looking for in connection with robberies, are part of the Internet's social structure, they are not directly linked to cyber safety. They are linked to an offline problem, namely robberies. In cases like this the Internet is merely used as a means of communication. Studies into the effectiveness of www.depolitiezoekt.nl therefore do not belong to my field of expertise, but rather to communication science or research into how to combat robberies in the physical world.

What www.depolitiezoekt.nl does however demonstrate is how difficult it is for the police force and the Public Prosecution Service to find their way around the Internet. For this reason I would like to flash forward quickly; later I will be discussing the police force in more detail.

Www.depolitiezoekt.nl opens with the sentence 'The Police and the Public Prosecution Service request your help in finding the following people.' This, together with the house style employed on the site, suggests that the police and the Pubic Prosecution Service are the ones responsible for looking after this site, yet the makers of the site are not mentioned, and there is no sender information. Who manages this website? Who is responsible for it? Who can I contact if I have questions or remarks? On April 6, 2010 I asked these questions on your behalf through the guest book of the Amsterdam-Amstelland police department. On April 12, 2010 I got the following answer 'www.depolitiezoekt.nl is an initiative of the Amsterdam-Amstelland police department. Several other police departments have also started using this website. You can direct your question to 0900-8844. Ask for Amsterdam-Amstelland's team that is responsible for robberies.'

The absence of a clear sender on this site is no coincidence since the disclaimer reads as follows: 'While the greatest possible care is taken in the placing of information on this site, we cannot be held responsible for its contents. No rights can be derived from the information contained on these pages nor can we be held responsible for the consequences of using it.' To me, this is incorrect. Police officers draw up police reports under oath or affirmation of office and by doing so they personally vouch for the truth of what they write. The same principle applies to any other stages in the investigation: the police are always accountable, right through to the courts. Now, in cyberspace this principle is jettisoned: here the police can put photographs of people in the public domain along with the claim that these people are suspected of criminal activities. They then proceed to absolve themselves of any responsibility for the accuracy of the information. In my opinion the police are definitely responsible for the content of the information that they put on the Internet and they can also be called to account for it, if necessary before the courts.

In essence, the point I am making with this flash forward is that evidently the police quite easily stray onto shaky ground when they enter cyberspace. Suddenly they lose their way and forget how police work is supposed to be conducted. The Cyber Safety Lectorate therefore needs to not only provide insights into safety issues but also into what can be done, and how it should be done, to tackle the issues. The questions are twofold:

- What exactly is the case?
- What can be done about it?

In a similar fashion, the Internet relates to safety in two ways:

a. It offers people new opportunities to behave contrary to the norm (and this gives rise to new problems).
b. It presents new opportunities for regulating behaviour (new opportunities, therefore, to do something about abnormal behaviour).

A. Cyber safety: new opportunities for behaving contrary to the norm

To start with, the Internet significantly increases opportunities for people. In 1983, before the Internet era, in her research into communication technology, Ithiel De Sola Pool (1983: 226) concluded: 'Computers, telephones, radio and satellites are technologies of freedom, as much as was the printing press.' Through all of these technologies, people started to become part of a more extensive network and their opportunities to act increased accordingly. With their personal computers, laptops and mobile phones, they participate in the international network through the

Internet, for their hobbies or for work. They order goods through web shops, they download the latest hits and they visit sex sites. Through these communication channels, it has become possible for people, more so than in the past, to form and maintain relationships with others, without their environment being aware of them.

On the Internet people are able to take part in social traffic more anonymously than in the offline world. The average Internet user is not able to establish the true identity and address of their fellow users. Generally speaking, they cannot see each other and therefore cannot recognise each other or tackle each other about things afterwards. They also do not risk being accosted for things because they are not physically present. This means that behaviour on the Internet that contravenes the norms carries fewer risks than the same behaviour would do in the offline world. Because people all over the world who behave in the same aberrant fashion can find each other easily, deviant social networks form where previously it was not possible. According to Frissen and Van Lieshout (2003: 21), cyberspace enables citizens 'to search for, extend and even transgress' the boundaries of what is permissible. They speak of 'unrestricted behaviour'.

What I have just said is in line with the familiar thinking of both scientists and those in the field, in brief: the Internet facilitates crime. This claim is easy to defend and fairly popular but there is more to it.

One objection to this claim is that since the rise of the Internet, i.e., the mid 1990's, there has not been a noticeable increase in crime that can be attributed to the Internet. The counterargument is that crime facilitated by the Internet might not be reflected in police statistics. I will return to this later.

More important than this quantitative discussion, to my mind, is the question of how this assumed facilitating of crime works. After all, only once you know how things work, once you know why things are the way they are, is it possible to work towards putting measures in place to address them.

The rationale behind the claim that the Internet facilitates crime is generally as follows. Because people can act more anonymously on the Internet than they can in the physical world, and because less monitoring takes place on the Internet, people are more likely to behave differently to the norm than they would offline. The question of whether people are really more anonymous online than offline, and whether they are less subject to monitoring online than offline is not the main issue here. Here the Thomas theory applies, and that is: 'If men define situations as real, they are real in their consequences' (Merton, 1968). In other words: if people are of the opinion that they are anonymous, and that they are not being monitored, then they consequently behave as though that is the case.

B. Cyber safety: new opportunities to regulate behaviour

In many respects, cyberspace resembles the offline world. This is not strange because the same people make these worlds what they are. We are the ones. You and I. In cyberspace, too, there are norms, and people hold each other to account according to these norms. This is particularly so on the social networking sites that people are often part of. There cyberspace is similar to the offline world. Those searching for norms in cyberspace will soon find them. To start with: when you're on the Internet, you probably feel as though you have to behave yourself. You wouldn't start behaving like an animal the minute you enter cyberspace. What's to stop you? It is all the norms that you have internalised from your upbringing and schooling that you take with you to cyberspace. In part these norms are fixed in a general 'nettiquette', for instance, or in smaller communities on a list of frequently asked questions (FAQ). On Hyves (a Dutch social networking site) it is considered 'not ok' to bully, stalk, discriminate, spam, create a false profile or to post pornography. We can also consult other researchers to learn about norms in cyberspace. Svensson and Van Wijk (2004) concluded in their research into codes of conduct among student communities on the Internet:

> *'The copying of copyright protected works is judged positively, sharing pornography as neither positive nor negative and spreading child pornography is emphatically condemned. (…) whoever downloads should also share files; hacking and spam is out of the question, as is the spreading of computer viruses.' (2004: 79)*

De Pauw and colleagues (2008) report that it is not acceptable to cheat in the world of online gamers. Various studies point out that in hacking circles there are strict codes of conduct, such as safeguarding one another's anonymity and not committing acts of vandalism[1] (Jordan & Taylor, 1998, Stol et al., 1999, Turgeman-Goldschmidt, 2005). Norms apply everywhere, including in cyberspace. And in cyberspace, too, people can expect sanctions. In the student communities mentioned by Svennson and Van Wijk, Internet users call offenders to account for their behaviour; if this is not effective then a moderator – a discussion leader within the Internet community – takes measures, for example, by issuing a warning, removing a contribution or excluding the offender, either temporarily or permanently. In extreme cases, the service provider may disconnect the offender (Zouridis & Frissen, 2004).

In their research into gaming Internet communities, De Pauw and his colleagues detected sanction mechanisms. I quote: 'Online communities developed a monitoring and regulation system through a moderator to tackle inappropriate behaviour. The most efficient punishment is "shaming" whereby cheaters are stigmatised. This is more effective than a ban or a warning because it undermines the players' reputations' (2008:20-21). On Hyves, users can make 'not ok' reports. In the information it states: 'Items are automatically removed temporarily after a number of "not oks". We then assess the situation to see if they should be put back or permanently removed.'[2]

Partly on the basis of the studies I have mentioned, I have differentiated four types of reactions to behaviour in cyberspace that contravene social norms:

1. The first is 'non-action': no measures are taken against the offender. Their behaviour is tolerated or ignored, or those who are bothered by it retreat to some other part of the Internet.
2. The second is informal social control: other Internet users undertake actions against the offender. This may entail someone speaking to the offender, or that a large group of Internet users close ranks against the offender, or that the offender is nailed to the virtual cross.
3. The third reaction, which is really a differentiation of informal social control, is mediation. Internet users call in a mediator to resolve the conflict. This could be done through a mediator of a specific Internet community or, in extreme cases, the Internet service provider (ISP).

[1] These are examples not generalisations. There are various kinds of hacker groups with various norms (see for example Van der Hulst & Neve, 2008 and Leukfeldt et al., 2010).

[2] www.hyves.nl, May 6, 2008.

4. The fourth reaction to abnormal behaviour in cyberspace is formal social control. Internet users call upon the intervention of a formal body to take monitoring and corrective action. Incidentally, formal authorities also act on their own initiative.

While non-action may be a reaction to deviant behaviour in cyberspace, it does not regulate the offender's behaviour since they can carry on unhindered. In order to mediate and apply informal social control, other Internet users must be able to find offenders and approach them. This works well provided the offender regularly visits more or less open, visible and stable Internet communities, such as gaming sites, Internet communities or profile sites such as Facebook or LinkedIn. It is then possible to approach and hold the offender accountable. Technical measures are also possible in cyberspace, such as removing texts, barring someone's access to a community or organising an e-mail bombardment (dDos attack). Mediating and informal social control can be effective against crime but frequently formal social control is called for. The most important organisations for meting out formal social control are of course the police and the justice department. This is not only the case for tracing cybercrimes, but also for the prevention of crime, the timely apprehension of criminals, and the building an information base and monitoring – in short a complete arsenal of police methods.

Although the police normally only take action when other corrective mechanisms fail, and although the police cannot do much without the active input of others in society, they play an essential role. It is therefore of vital importance for safety in cyberspace that the police are able to take action effectively – obviously within the limits of the law and common decency.

What options are available to the police? In theory, a lot. When people use modern technology they invariably leave a digital trail in their wake. For instance, Internet service providers have records of who is online and when; computers and mobile phones record which sites have been visited; mobile phones automatically connect to transmission stations; those who pay electronically not only reveal their location but also their spending patterns; those who take part in social networks on the Internet show the outside world where their interests lie and in which circles they move, and so on. The movements and particulars of people are better registered than ever before. While it is true that a handful of whiz kids know how to stay off the radar, this does not change the principle. The comings and goings of citizens are registered more than before and this allows for stricter control. This counts not only retrospectively in the sense of tracing movements, but also in advance in the sense of 'knowing who you're dealing with'.

Although investigation is only part of the picture, I would like to make a remark about it at this point. I once heard a police detective say the following about police investigations at the scene of a crime: 'perpetrators always leave tracks, always: hair, skin, specks, an imprint, whatever. The problem is that we often don't find tracks because we are not in a position to discover them – often simply because we don't have enough manpower to search for them intensively enough.'

Perpetrators of cyberspace crime also leave tracks. And there too the police don't always find them; quite frankly: they mostly don't. The police detective's statement that I have just paraphrased applies here too: 'we often don't find tracks because we are not in a position to discover them – often simply because we don't have enough manpower to search for them intensively enough.' More specifically: why are the police not in a position to discover tracks in cyberspace?

The biggest problem that the police are faced with in their operations in cyberspace is a lack of knowledge, and not only in terms of investigations. This is nothing new; the police themselves have repeatedly pointed it out (Stol et al., 1999; Stol, 2003; PWC, 2001; LPDO, 2003; Griffith, 2005; Van der Hulst & Neve, 2008; Toutenhoofd et al., 2009). I hasten to add that the police are taking action to address this shortage of knowledge but it won't happen overnight. I will return shortly to this crucial problem that the police – and other authorities within the judicial system - are facing because the Cyber Safety Lectorate plays an essential role.

C. A balance?

I argued that cyberspace gives people new opportunities to behave against social norms, and that they use these opportunities. I went on to contend that behaviour regulating mechanisms operate in cyberspace and that the police make an essential contribution to this. Are the two in balance? Or are there insufficient mechanisms to regulate behaviour in cyberspace? Is deviant behaviour getting the upper hand? Are the police consigned to the side-lines and does crime in cyberspace have a free rein? Or is the opposite the case: do the authorities have a stranglehold thanks to new technology?

As it stands the police have a lot of catching up to do, this much is clear. But this is not cause for serious concern because the police are not the only barrier against deviant behaviour in cyberspace. Citizens and countless private organisations and enterprises also work towards safety in the digital world, from mediators on small websites to the security divisions of large banks. They are the first line of defence against insecurity. Society is resilient and it is certainly not totally dependent on the police. Only if citizens and businesses cannot prevail under their own steam does it become a matter for the police. Obviously the police need to be prepared for this. The lack of knowledge that I mentioned earlier as the biggest problem facing the police needs to be addressed.

1.4 Lack of knowledge and the Cyber Safety Lectorate

One of the events that led to the creation of the Cyber Safety Lectorate was the introduction of the new State Security Monitor (*Veiligheidsmonitor Rijk* (VMR)) in 2006 (CBS, 2006). This monitor had recently been developed and was intended to function as an instrument for the annual population study into the security situation in the Netherlands. It replaced three measurement instruments that had been in use up until then: the Permanent Research into Living Conditions (*Permanent Onderzoek Leefsituatie* (POLS)) of the Central Bureau for Statistics (CBS), the Police Population Monitor (*Politiemonitor Bevolking* (PMB)) and the Large Cities Policy Monitor (*Grote Steden Beleid* (GSB-monitor). From 2006 onwards, one measurement instrument was deemed sufficient for security. The project team that developed the new instrument paid a lot of attention to the continuity of the statistics: it was feared that there would be a disruption in trend tracking studies because the situation in the country would be measured using a different instrument. Perhaps the old data would no longer be usable as reference material. The new measurements would be left hanging due to the absence of a historical perspective. To investigate whether there would in fact be a disruption in the tracking studies, the newly developed monitor ran parallel to the POLS and the PMB on a limited scale. Statistical analysis led to the conclusion that the results of the new monitor were not entirely comparable to those of the other two studies. For this reason, the results of the new instrument apply 'as derived from a new study and as the starting point of a new series' (CBS, 2006:15).

When I opened the new Security Monitor, I naturally turned to the questions concerning safety in cyberspace. I found none. Those who developed it had clearly done their best to follow the old PMB and had paid no attention to current development. In 2004, the Social Cultural Planning Bureau (*Sociaal Cultureel Planbureau*) published research findings in which 82.1% of the population aged 16 years and above agreed with the statement: 'committing offences with the help of IT will increase' (SCP, 2004: 245). This had not filtered through to the new Security Monitor.

This was a distressing state of affairs. From my own field of expertise – police and technology – I was well aware that security issues in cyberspace would increase and become more complex in the years to come. In order to tackle security issues, one has to start by gathering information about the problem. This is a basic principle, known in policing circles as intelligence led policing. The very first question that needs an answer is: how often does the problem arise? This is then followed by more complex questions, such as: what exactly is the problem, who is causing the problem, who are the victims, what are the causes, and: what would be effective measures to combat it? When I saw that the new State Security Monitor would not be able to answer even the simplest question, I realised that it was time for a group of researchers to focus on the practical issues, and apply themselves to finding answers to these questions. In other words: it was time for the Cyber Safety Lectorate.

Another incident also played a role for me in these developments. During a talk with a few youth police officers, I heard that they had lost touch with the youth. Young people were no longer to be found in the places where they used to hang out. The officers were aware that the youth were often in cyberspace, but where exactly? And how could youth officers stay in touch with them? One of the officers said that they don't even speak the same language as the youth use in cyberspace. In this case, it had nothing to do with research carrying out a national survey: here someone in the everyday business of police work was stating that all was not well in their field work, that the police in a very real sense were losing the connection in societal developments. I can add several other examples to this incident with the youth agents, examples of police officers who are struggling to get to grips with cyberspace.

The Cyber Safety Lectorate was established and started on September 1, 2008. The goal of a lectorate is to:

- contribute to the quality of education;
- contribute to the work of professionals in practice;
- link education and professional practice.

Research is the means for this. The lectorate's research programme focuses on three themes:

- trends in cybercrime;
- youth and cyber safety;
- business and cyber safety.

Each research project takes place in the field, and lecturers and students take part in each project. Research findings benefit practical operations and are used to develop the educational programmes and material. For instance, one of the subsidiary subjects is now cyber safety and students from various disciplines participate. This subject is invariably fully subscribed. One of the reasons for this is the fantastic contribution that we get from guest speakers. Education and practice reinforce each other through this. Other study components include a cyber safety programme for part-time students; a post-college course in cyber safety for professionals; internships for students and recently Cyber Safety was established as a graduate course specialisation within Integral Security at the NHL University. Back to the main theme of the lectorate.

The research strategy is as follows. Because so little is known about insecurity in cyber space, the lectorate has started by conducting exploratory and overview research into the phenomenon. For this reason we chose themes from a wide subject spectrum. From this broad spectrum, subjects will emerge that require further exploration.

An example. The book *Verkenning cybercrime in the Netherlands 2009* [Investigation cybercrime in the Netherlands 2009] (Leukfeldt et al., 2010) comprises the report of an exploratory study based on police files. It investigated five cybercrimes in terms of penalisation, offenders, modi operandi, scale, victims, damage and connections with other cybercrimes. One of the research projects currently underway as a follow-on study from the broader exploration concerns the question of whether swindlers in cyberspace are a different kind of offender to the swindlers who commit fraud in the offline world. Broad reconnaissance is the basis on which we will build research into specific subjects.

In all our research projects we work closely with the cyber safety profession. We gladly do research commissioned by organisations in the field because we then know that there is a clear need for it and that the results will actually be used. An example of this is the study we did for the police force's national Programme for Combating Cybercrime (*Programme Aanpak Cybercrime*) for the National Police Services Agency (NPSA) (KLPD – *Korps Landelijke Politiediensten*), the Ministry of Justice, the Ministry of Education, Culture and Science and the Public Prosecution Service. The lectorate has been around now for eighteen months and during that time we have worked on various studies:

- screening for child pornography on the Internet;
- the scope for cybercrime related work for the police;
- the intake of cybercrime reports by the police;
- processing of cybercrime cases by the police, the Public Prosecution Services and judiciary (the flow of cases through the legal system);
- overview study into cybercrime based on police files;
- cybercrime victimisation among the Dutch population;
- youth and cyber safety focussing on bullying, addiction, unsolicited sexual contacts and youth crime;
- the illegal trade in art and cultural objects on the Internet.

As you can see, there is finally going to be a study done into cybercrime victimisation. The NPSA have commissioned this research in close collaboration with, among others, the Ministry of Justice and the Central Bureau for Statistics. I can't speak yet about the findings of this research, but I can mention the results of a few other studies.

1.5 Some findings

Cybercrime accounts for less than 1% of all reports registered by the police (Domenie, Leukfeldt, Toutenhoofd & Stol, 2009). This is one of our research findings. This could mean that cybercrime occurs infrequently, that citizens and businesses that are victims don't notice it, that they do notice it but don't report it to the police or that they do go to the police but that the police don't record it. That statistic is therefore not very meaningful. In a study among 1,246 Frisian Internet users, respondents were asked whether they had been victims of hacking or e-fraud during the previous two years. Of those, 2.7% said that they had been the victims of hacking and 1.2% of e-fraud, and this excludes 'attempts at'. Of these victims, 4.2% reported the crimes to the police. Obviously we need to be careful with these figures because they are based on a small sample among a limited target group. If this is an indication of the results we can expect from the national victimisation research into cybercrime, then we must conclude that willingness to report these kinds of offences is fairly limited.

The percentage of those who report for all offences is 26.7% according to the 2009 edition of the integral security monitor. This percentage is highest for vehicle theft (89.4%) and theft from vehicles (70.4%) and lowest for threats (11.1%) and sexual offences (2.7%) (CBS, 2010). The percentage who report is therefore only lower for sexual offences than it is for the 4.2% of victims of hacking and e-fraud cybercrimes. This arouses curiosity for the statistics about those who report sexual offences in cyberspace. For the interim my take on it will be that the percentage of those who report cybercrimes to the police is not low (<1%) because cybercrime is rare but because willingness to report crimes is limited.

I suspect that willingness to report crimes among businesses is much lower than this 4.2%. In the 317 e-fraud files that we studied, we only came across seventeen that involved a company as the victim. Either businesses are far less likely to be victims of e-fraud than citizens, or businesses are less likely to report the crime. The latter is not improbable. I know from people in the business world, particularly from the large organisations who generally have their own in-house experts, that they have their doubts about the police when it comes to cybercrime. Smaller organisations also prefer not to report things to the police because it costs too much time and doesn't produce results. Recently a group of Rotterdam shop owners were in the news when they announced that, out of protest, they would cease reporting shoplifting to the police (the newspaper *de Volkskrant*, May 6, 2010). A symbolic gesture, apparently, because shortly after that the shop owners organisation, Detailhandel Nederland [Retail Trade the Netherlands], reported that shop owners were only reporting 2% of all shoplifting incidents (*de Volkskrant*, May 8, 2010). On November 11, 2009, Wijnand Jongen, chairman of thuiswinkel.org, the umbrella organisation of web shops, sounded the alarm because web shops allegedly lost €90 million to e-fraud in 2009 and the police were doing far too little about it. While I hasten to add that those are the damages according to Mr Jongen, all the indications are that there is much more afoot than is obvious from the police statistics.

From our research into how the police register cybercrime reports, we know that police staff in the charge offices are often at a loss (Toutenhoofd et al., 2009), if they even entertain it. Sometimes the person reporting the incident is sent away having been told that it is not a matter for the police. Particularly in cases of e-fraud, the police use their classic invocation: 'this is not a civil case' which means that the informant would have to resolve the issue with the perpetrator themselves, if necessary through a lawyer or the courts. But fraud is still fraud.

Registering cybercrime reports is not going well, so much is clear. At the moment, staff noting cybercrime reports are learning as they go along, and from colleagues that have done it before. They are not told whether they are doing it correctly or not. This is a job for police training. It is not necessary to turn all officers into cybercrime experts, too few cases are reported for this, but it is important that the police develop a training strategy that matches what is going on in society. In this regard I would like to draw attention to the input of IT experts outside the police force. There are enough IT specialists that are willing to help register cybercrime reports or to work on cybercrime cases. The police can involve these people through the voluntary police force. These days this does not refer to people who help out at fairs and carnival parades. I often say this during presentations and last time someone came to me and said: 'Nice of you to say that, you're describing me!' He told me that he works as a security expert for a large telecommunications company in the Netherlands and that he is a member of the voluntary police force – and that he does get deployed to help out at parades but that the police never make use of his IT expertise.

Yet cybercrime is regularly reported and registered. The lectorate studied 655 of these files. We looked at cases involving hacking, e-fraud (some involving identity misuse), extortion, spreading of child pornography and hate speech. It is beyond the scope of this work to discuss all the interesting findings here. You can read about it at home. I will highlight a few points here.

Perhaps the most important finding is that cybercrime has been democratised and has become a more or less everyday occurrence. We should not imagine that suspects of cybercrime are whizzkids, no pimply youths with milk bottle glasses that work deep into the night with computer commands running past on the screen while he searched for leaks in the computer system. The police files reveal a completely different picture of the average Dutch cybercrime suspect (Leukfeldt et al., 2010):

- Suspects are generally born in the Netherlands: among the five types of crime investigated by us, the percentage of suspects born in the Netherlands ranged between 86 and 92%.
- Although the Internet has no borders, most of the suspects were operating within the Netherlands (between 77 and 100%, depending on the type of cybercrime).
- Suspects are most likely to be men (73 to 98%), as is generally the case with crime, although it was noticeable that many women were involved in e-fraud; a significant number of e-fraud suspects were unemployed, so presumably economic motives play a role for the suspects.
- Crime is often the work of men under the age of 45, and this is also the case with cybercrime; hacking and hate speech suspects are in many cases to be found in the age group 12 to 24 years.
- Those who download or disseminate child pornography are an exception: they are virtually always men from all age groups – what is striking is that there is a group of young suspects who commit this offence: of the 168 suspects that we found in the police files, almost a quarter (23.8%) are in the age group 12 to 24 years. These are young people that make clips of a sexual nature of other young people, with their mobile phones or webcams, and then put this material on the Internet. This is sometimes accompanied by extortion; we found 14 files concerning cyber extortion and in 9 of the 14 cases the suspects were between the ages of 12 to 24 years. The youth are making themselves felt in the world of cybercrime – although they are probably not fully aware that their behaviour is categorised as such a serious offence.

'And what about hacking?' I hear you ask. I will tell you more about it and at the same time show you that it is not as difficult as it may seem.

Hacking is a kind of basic offence. E-fraud, child pornography and hate speech are crimes in their own right. There are few links between them and other kinds of crime. E-fraudsters commit e-fraud and don’t get involved with downloading of child pornography or hate speech, and so on. I can’t say much about cyber extortion, there were too few files for this offence, but in a number of cases we saw a link between extortion and the dissemination of child pornography. Hacking is clearly linked to other kinds of crime; it can be seen as a means to commit other crimes.

Hacking is also child’s play. For those of you who can’t hack, here’s a short set of guidelines. But watch out: don’t try this at home, it’s a punishable offence. We’ll start at the very beginning. According to article 138a of the Criminal Code, hacking is the deliberate and unlawful entry into a computer system. Unlawful means that you do not have permission to use that computer. Deliberate means that you didn’t accidently end up on that computer, for example through a typo. Hacking is therefore the deliberate use of another person’s computer without permission. The law does not stipulate that this need be done by cracking codes, breaching firewalls or carrying out some other kind of technical feat. If a colleague leaves his desk to fetch a cup of coffee without logging off, you can hack his computer by sitting at his desk and using it. This is a punishable offence. It is slightly more difficult to find out what the password is, but even that is not beyond the realms of possibility. You can look over someone’s shoulder, search for a note containing the password, guess what the password is, ask someone else who may know what it is or winkle it out of the owner using an excuse. There are plenty of ways to do it – and they’re all punishable. You are punishable if you:

- get possession of a password with a view to using it to hack (art. 139d Criminal Code) – that looking over someone’s shoulder that I just mentioned, is in itself an offence;
- since it is a crime, you are already punishable as soon as you try to get hold of a password (art. 45 CC – attempting to);
- are in possession of software with a view to using it to hack (art. 139d Criminal Code)
- are in possession of a password with a view to using it to hack (art. 139d Criminal Code)

In the hacking cases that we found in the police files, the suspects were not hacking for the sake of hacking. They were intent on financial reward or to aggravate a personal conflict. Hackers hack computers with the intention of committing e-fraud; or they hack computers because of a personal conflict: for example in relation to a divorce, an argument with a classmate or dismissal from work. Hacking is not intended to disrupt society or cause general mayhem, but to further the interests of the individual. It is generally about everyday affairs in which everyday people are intent on making life difficult for each other. Often the suspects and the victims are known to each other.

The question is therefore whether we should regard hacking suspects as hackers. In my opinion, it would be better to consider them as fraudsters, sexual offenders, perpetrators of violence or vandalism that use hacking to operate. In the same way, a mugger using an illegal weapon is still a mugger and not that possession of an illegal weapon puts them in a special criminal category. This is more than academic deliberation. For the police it means that they can stop trying to create various typologies for hackers and their accompanying ‘offender profiles’. That is a road going nowhere. Hackers don’t exist! It’s not about the means that the offender uses (i.e., hacking), it ‘s about their intentions (fraud, theft, vandalism, violence, hate speech, and so on). Hacking may be a simple matter for the offenders. The hacking files that we studied pose a serious problem for the police because almost a quarter of the suspects of this kind of cybercrime (23.3%) operate from abroad. That is about a seventh of all e-fraud cases (14.5%). A journalist at the *NRC* newspaper thought it remarkable that, even though the Internet has no borders, the vast majority of the suspects operate within the Netherlands (*NRC*, April 12, 2010). This is cold comfort for the police; for them it is more important that in many of cases the suspects operate from abroad. At the moment, arbitrary officers in arbitrary police stations rarely if ever get confronted with cases involving suspects living abroad. But this is changing. These kinds of cases are on the increase because of cyberspace. The police are not ready for this and it is time they started to anticipate it. To my mind the solution lies in a combination of inland centralisation and at the same time a measure of decentralisation. Intensifying international collaboration will not succeed if every local police station in the Netherlands gets involved, so coordination needs to take place at a national level. On the other hand, combating of cybercrime would benefit if international cooperation was simpler and part of everyday routine, in other words: less a case for exclusively national authorities. These would otherwise become overwhelmed with the volume of relatively small cases (minor misdemeanours that never used to have an international component, but do now because of the Internet).

The aim of our study into police files was to get a better overview of the phenomenon. The study did move us forward, but the last word has not been said on the matter by any means. We know that certain areas of cybercrime are outside our field of vision:

- For starters we have no insight into the files of organised crime, such as files on international gangs that engage in skimming, for example, deposit fraud or the commercial exploitation of child pornography. Special teams, such as the NPSA's Team High Tech Crime, handle cases like these, and the files of these teams are not to be found in the general police register that we could access.
- Secondly, we had no insight into so-called victimless cybercrimes, such as the drug trade or illegal gambling, because if there is no victim, then no report will be made and there will be no police file.
- Thirdly, we only had insight into cases that were reported. The percentage of population that report these crimes is presumably low, so low that for this reason alone we missed 95% of all cybercrimes. We have even less insight into Cybercrimes involving businesses because willingness to report crimes among those in the business sector is even less prevalent by all accounts.

The final word has still not been said because several of the findings are eligible for further research. Here are some examples:

- In several areas, it came to light that there is a relationship between the youth, crime and sexuality. I don't want to trot out that old cliché about 'the youth of today' going to the dogs, but there are indications that follow-on research should be done into the youth and sexuality in cyberspace.
- Secondly, we noted in several areas that there is a difference between cybercrime suspects and 'the average suspect in the Netherlands', as we know them from the criminal profiling systems that the police use. The question of whether a cybercriminal is a different kind of delinquent then 'the classic criminal' needs closer attention. It is relevant to crime prevention, and perhaps a better picture of this new group of criminals will help the police in their investigations.
- Thirdly, the business sector is conspicuous in their absence in the files we studied. At the same time web shops are sounding the alarm because e-fraud is completely out of control. It is therefore high time that research was done into victimisation among business, particularly with

respect to the possibilities of a public-private sector collaboration working towards greater safety in cyberspace.

1.6 Word of thanks

As I mentioned at the start: much remains to be done. Fortunately I'm not alone in this task. I would not have achieved as much were it not for the input of numerous people at home and abroad, all of whom are working towards a safer cyberspace. I would like to extend my heartfelt thanks to them. I have in mind particularly those organisations that I mentioned as those who commissioned our research; the many enthusiastic students; all the people in the field that spontaneously contacted us and often travelled to Leeuwarden to hear more about the work of the Cyber Safety Lectorate; all the people that have welcomed me into their organisations and told me of their experiences; the management of NHL University, the Open University and the Police Academy; and all my colleagues in those organisations. I would like to extend a special vote of thanks to Joyce Kerstens for her comments on earlier versions of my reading.

Above all I count myself as fortunate that I may work with a group of extremely enthusiastic colleagues that are always ready to take on a new challenge, invariably think in terms of solutions and opportunities, while at the same time are critical, also of themselves. Joyce Kerstens, Marika Toutenhoofd, Miranda Domenie, Rutger Leukfeldt, Sander Veenstra, Jurgen Jansen, Marja Blok, Joyce Verhees and Ietje van der Maten: together you are a fantastic team!

I have spoken

References

CBS (2006). *Veiligheidsmonitor Rijk. Landelijke rapportage* [State Security Monitor. National Report]. Voorburg: CBS.

CBS (2010). *Integrale veiligheidsmonitor 2009. Tabellenrapport* [Integral Security Monitor 2009]. Den Haag/Heerlen: CBS.

Domenie, M.M.L., E.R. Leukfeldt, M.H. Toutenhoofd & W.Ph. Stol (2009). *Werkaanbod cybercrime bij de politie* [Workload cybercrime for the police]. Leeuwarden: NHL Hogeschool.

Frissen, V. & M. van Lieshout (2003). *Tussen dwang en drang. OOV, ICT en ontgrenzing van het gedrag* [Between coercion and persuasion. OOv, IT and liberating behaviour]. Delft: TNO.

Giddens, A. (1984). *The constitution of society.* Cambridge: Polity Press.

Griffith, R.E. (2005). How Criminal Justice Agencies Use The Internet. In A. -Pattavina (Ed.), *Information Technology and the Criminal Justice System* (pp. 59-77). Thousand Oaks: Sage.

Hulst, R.C. van der & R.J.M. Neve (2008). *High-tech crime, soorten criminaliteit en hun daders* [High-tech crime, types of crime and their perpectrators]. Den Haag: WODC.

Jordan, T. & P. Taylor (1998). A sociology of hackers. *The Sociological Review, 46*(4), 757-780.

Leukfeldt, E.R., M.M.L. Domenie & W.Ph. Stol (2010). *Verkenning cybercrime in Nederland 2009* [Investigating cybercrime in the Netherlands]. Den Haag: Boom Juridische uitgevers.

LPDO (Landelijk Project Digitaal Rechercheren) (2003). *Visie op digitaal opsporen* [A vision of digital investigating]. Zoetermeer: LPDO.

Merton, R.K. (1968). *Social Theory and Social Structure.* New York: The Free Press.

Mumford, L. (1963, 1934). *Technics and civilization.* New York: Harcourt Brace Jovanovich.

Pauw, E. de, S. Pleysier, J. Van Looy & R. Soetaert (2008). *Game on! We krijgen er niet genoeg van* [Game on! We can't get enough of it]. Brussel: viWTA.

PWC (Profit for the Worlds Children) (2001). *Kinderpornografie en internet in Nederland. Een overzicht van de huidige situatie, knelpunten in de bestrijding, suggesties voor verbeteringen* [Child pornography and the Internet in the Netherlands. An overview of the current state of affairs, bottlenecks in combating it, suggestions for improvement]. Haarlem: PWC.

SCP (Sociaal en Cultureel Planbureau) (2004). *In het zicht van de toekomst* [In sight of the future]. Meppel: Giethoorn ten Brink.

Sola Pool, I. de (1983). *Technologies of freedom.* Cambridge: The Belknap Press of -Harvard University Press.

Stol, W.Ph. (1988). *Automatisering bij de politie. Meldkamerwerk en kwaliteit van de arbeid* [Computerisation in the police force. Central control room operations and the quality of work]. Amsterdam: Huisdrukkerij Politie Amsterdam.

Stol, W.Ph. (1990). Automatisering bij de politie, voorspelbaarheid van sociale gevolgen van automatisering en het belang van de menselijke factor [Computerisation in the police force: predictability of the social consequences of computerisation and the importance of the human factor]. *M&O, tijdschrift voor organisatiekunde en sociaal beleid*, *44*(1), 30-45.

Stol, W.Ph. (1996). *Politie-optreden en informatietechnologie. Over sociale controle van politiemensen* [Police actions and information technology. On social control among police officers]. Lelystad: Koninklijke Vermande.

Stol, W.Ph. (2003). Sociale controle en technologie. De casus politie en kinderporno op het Internet [Social control and technology. Case study of police and child pornography on the Internet]. *Amsterdams Sociologisch Tijdschrift*, *30*(1/2), 162-182.

Stol, W.Ph., R.J. van Treeck & A.E.B.M. van der Ven (1999). *Criminaliteit in cyberspace. Een praktijkonderzoek naar aard, ernst en aanpak in Nederland* [Crime in cyberspace. Applied research into the nature, seriousness and approach in the Netherlands. Den Haag: Elsevier.

Svensson, J. & A.Ph. van Wijk (2004). Gratis zullen we alles delen [We'll share everything that's for free]. In J. Svensson & S. Zouridis, *Waarden en normen in de virtuele wereld* (pp. 15-81). Enschede: Universiteit Twente.

Toutenhoofd, M.H., S. Veenstra, M.M.L. Domenie, E.R. Leukfeldt & W.Ph. Stol (2009). *Politie en cybercrime. Een onderzoek naar de intake van het werkaanbod cybercrime door de politie* [Police and cybercrime. Research into the taking up the cybercrime workload by the police]. Leeuwarden: Noordelijke Hogeschool Leeuwarden.

Turgeman-Goldschmidt, O. (2005). Hacker's accounts: Hacking as a social entertainment. *Social Science Computer Review*, *23*(1), 8-23.

Zouridis, S. & P.H.A. Frissen (2004). Over virtuele vrijplaatsen en civilisatie in cyber-space [On virtual refuge and civilisation in cyberspace]. In J. Svensson & S. Zouridis, *Waarden en normen in de virtuele wereld* (pp. -85-140). Enschede: Universiteit Twente.

2 Police in cyberspace

Oration

Presented in an abridged version

on the occasion of the public acceptance of the office

of affiliate professor for the endowed chair for Police Studies

initiated by the NHL University of Applied Sciences at the Open University

on Friday, September 2, 2010

by Prof. Dr W.Ph. Stol

Rector, colleagues, former colleagues, family members and friends, ladies and gentlemen, welcome to this historic location. Doornenburg Castle was built in an age when people could defend themselves with thick walls and a moat. Much has changed. Hopefully a lot more will change in the coming years because there is plenty of room for improvement for the police in cyberspace.

2.1 Introduction: the police and cyberspace

The title of my speech could easily read 'the police in cyberspace', but that is not what it is. The title is 'police in cyberspace' because it involves more than just the police organisation, more than just men and women in blue. I am differentiating between the function of the police and the police organisation, just as former professor of police studies Heijder (1989) did in the past.

It is important to differentiate between the two concepts because it allows us to answer the question of whether the police actually do what their function or society asks of them, or whether they perhaps undertake activities that their function does not require of them, or even forbids them to undertake. Police studies as an academic discipline rest on a research tradition that is based on establishing empirically what the police do, for example through participatory observation to ascertain how the police function in practice. European pioneers in this tradition include Feest and Blankenburg from Germany (1972), and a more recent European study from Norway (2003) by Finstad[3]

The word 'police' derives from the Greek 'politeia' which means more or less 'running the city state' – the polis (Hoogenboom, 1994). It is a broad concept. In the Netherlands, the word 'policie' also had a broad meaning, in the sense of 'managing' (Cachet, 1990). These days the term 'police' or police function generally has a narrower connotation and is concentrated around law, order and security.

I understand policing to mean the maintenance of the prevailing law and order. Some may wish to read this as 'prevailing legal order'. The essence of policing is that it comprises the techniques and broader social agreements for regulating behaviour. By 'maintaining *prevailing* social order' I don't mean to imply that police operations are unfamiliar with social change but that, in principle, this is what they aim at.

My approach differs somewhat from the definition that Cachet, for example, formulated in 1990. Maintaining law and order in his definition also states that 'as a final resort the legal and legitimate option exists to use force or violence' (1990: 89). To my mind, this addendum points the definition of 'police' too much in the direction of 'the police' initially, since it is 'the police' who have the monopoly of force in times of peace. I prefer to approach social issues broadly in the first instance, so as not to disregard all sorts of other participants and processes. There are a considerable number of organisations involved in maintaining social order without having the right to use force as a last resort, as we can see from the work of Van Hoogenboom (1994) and Van Steden (2007). And here I am not even referring to the contribution that citizens make to maintaining social order, those outside the auspices of formal organisations. The cooperation of citizens, as Cachet and Versteegh note, is 'a key factor in solving problems and offences'? (2007: 1046).[4] Because the research affiliated to my chair concentrates on policing within an as yet unfamiliar social terrain, one that is developing

[3] For a more extensive overview of similar studies, see Stol, 1994; Stol et al., 2006.

[4] In the Netherlands, Van de Bunt and Rademaker (1992) and In 't Velt (1996, 1999) documented at length that the police did not so much solve crimes using classic detective work or data bases, but rather through information supplied by citizens – victims, perpetrators and witnesses.

rapidly and where social processes may work in ways that are strange to us – cyberspace – it is important to use a broad definition of the policing concept as a departure point. These considerations do not detract from the fact that *the* police are central to my research, but it is crucial to keep an open mind towards others who are active in the field of policing.

What is cyberspace? Why is it that since the breakthrough of the Internet in the mid 1990's we talk of cyberspace, whereas when other communication technology arose there was no talk of a newly formed social arena? There was never talk of radiospace, televisionspace or telephonespace, for instance. What sets the Internet apart from earlier communication technology, such as the television or telephone, is that when people use the Internet they are not only communicating, but laying down structures that are, to an extent, anchored in the technology. Sometimes these resemble worn paths in a tundra landscape, paths that people are inclined to use again for the sake of convenience, and sometimes they resemble vast highways that closely packed crowds of people routinely travel.

I understand social structure to be the more or less fixed patterns in human relationships, including the rules, infrastructure and all other means that people use to maintain their relationships. In other words, the paths they've used in the past. Social structures arise from the actions that people undertake. Once social structures are formed, they give direction to what people do (Giddens, 1984, 1989). People cannot pretend that the social structures they have formed don't exist, or ignore them. They have to take them into account, to a greater or lesser extent. Even if no one was to go on to the Internet, there would still be domains, websites, news groups, search engines, profile sites, forums and all their interconnections. Moreover, people are expected to use the language laid down by the technology. Those who enter the Internet have to take into account the structures they find there. The fact that the occasional 'techno-anarchist' does not always follow the beaten tracks does not detract from the principle. The Internet's social structure, the dynamic combination of people acting together and patterns laid down by technology, is what we call cyberspace.

Incidentally, social structures are not only forceful, they also open up opportunities. People sharing the same interests that in the past would never have found each other, now meet thanks to the structures of search engines, websites and profile sites. Social structures change. Old structures change or disappear and new ones arise. Cyberspace is certainly subject to continuous change.

We have now broadly explored the concepts of police and cyberspace, and have an idea of what I will more or less be engaged with in my capacity as Police Studies professor: maintaining legal order within the social structure of the Internet. This is the modern aspect of the theme that I have researched for 25 years, namely police in relation to information technology (e.g., Stol 1988, 1996, 2010).

Police work, and now I am talking about *the* police in particular, is essentially work to do with information, or knowledge if you will. Ultimately the core of police work is that police officers have to know – and prove – who did what when and where. Police and information are an inseparable twosome (compare Stol, 2007). The knowledge and power of the authorities are also an important theme in the work of French philosopher Michel Foucault. We all know that knowledge is power. Those who read Foucault's work quickly learn that the reverse is perhaps even more valid: power is knowledge. If you have power, you have access to information and opportunities to construe the truth. The police know this better than anyone else: if you have authority, you are the one who gathers the information and with that you describe reality. When you draft a police report, the truth is committed to paper according to police principles and from a police point of view.

My colleague Claartje In 't Velt (1957 to 2006) entered the field of policing in 1991 as a cultural anthropologist and described this process aptly as follows:

> *'A correct, formal handling of affairs strongly occupies minds in daily work. This is the case, for instance, when police reports are being drafted. The fact that it is not yet possible to enter police reports in PAPA (the former police computer system – WS) is a much-discussed topic. It means that they have to be "hand written", a process during which the required wording needs to be sought. Looking up the correct – fixed – phraseology and typing the texts is a time consuming chore. Using adopted forms and phraseology is generally very important in preventing procedural mistakes. I could see that, in these reports, official and formal language is used to exclude any chance of misunderstandings. I came across the following passage in a police report: "We saw that the air gun could be applied for actual use and was not packaged as such so that it could not be applied for actual use. We could see, namely, that this weapon in its entirety was not packaged." All kinds of regulations and rules are there to prevent any kind of misunderstanding from arising surrounding the incident.' (1991: 16)*

It is no coincidence that in 1972 Feest and Blankenburg described everyday police work with the title *Die Definitionsmacht der Polizei* and that Finstad (2003) did the same thirty years later with the title *Politiblikket* (the police point of view).

Foucault's work, with its focus on police, information and power, contains good leads for research in the field of law and order maintenance and information technology. He in fact provides a framework that can serve as a background and analysis outline for such research. For this reason, I will introduce him later. I will also put forward the most important criticism of his work. But first I will focus on practical work in cyberspace by way of a short intermezzo.

2.2 Intermezzo: a few impressions of cyberspace

To describe the everyday reality of cyberspace, we often resort to guess work and casuistry because a lot remains unknown, and more particularly, unmeasured. Below I give an impression, through a sketch and an introduction, of what follows in my speech – without claiming to reveal all the relevant characteristics of cyberspace.

Cyberspace is possible because people want to broaden their horizons and meet other people – and because they have linked computers together. It is not known how many computers are involved. They can, however, give an approximation of how many domains have been registered. According to the American domain management firm, VeriSign, about 183 million domain names were registered worldwide by mid-2009. Of those, 89% have at least one website linked to the domain name (*The Domain Name Industry Brief*, vol. *6*(2), June 2009). In answer to the question of how many websites there are as a consequence, various estimates are given, such as 232 million (www.moneyma.com) and 27.45 billion of 27,450 million (www.worldwidewebsize.com). The second estimate is about 120 times bigger than the first, so these figures aren't worth a lot in their own right.

What is more important is the report that the Internet service Facebook, one of the platforms or profile sites that people use to stay in touch with one another, now has 500 million registered participants (*de Volkskrant*, July 23, 2010), a population exceeded only by China and India. The third country, the US, has levelled at 300 million. Some Internet services have been able to tie huge volumes of people to their sites.

In by far the majority of cases, these people use these new opportunities positively. Some of them experience social network sites as a very important part of their lives. For example: in April 2009, when in preparation for a reading I studied a few social network sites, I saw that Number 1 in the popularity contest for youth site Sugababes (www.sugababes.nl) was online for 23.4% of her time during the 14 months that she was a member of the site. I mentioned in my reading that this was an example of what looked suspiciously like computer addiction. A youth worker that attended my reading thought that I had a somewhat sombre view of things because participating in these social networking sites teaches young people all kinds of social skills – i.e., they are good for their development. When preparing for this reading I returned to the site and saw to my surprise that the same girl was still battling away at the top. Since the previous time that I had mentioned her in a reading she was still logged in for about a quarter of her time, that is to say for about 40 hours a week – by then for about three years.[5] Most of my students would find that forty hours a week is more than enough time to complete their study. Perhaps it is time to invite this young lady, as an expert in the field of Internet use, to an in-depth interview in the scope of the ongoing research project into 'Youth and Cyber Safety'.

The Netherlands is in the forefront of Internet development. In 2009, 90% of all Dutch households had access to the Internet and 77% of these were connected via broadband (www.cbs.nl). In January 2009, 'a staff member of Hyves (a Dutch social networking site) mentioned that there are 7 million registered Dutch Hyves profiles of which about 5 million had been active in the previous month' (Govcert, 2009:10). That is a significant amount when we take into account that our country has around 16.5 million inhabitants (CBS).

People in the Netherlands regularly shop online. The Dutch Home Shopping Market Monitor (Nederlandse Thuiswinkel Markt Monitor) provides more information on this market. 'Online consumer spending passed the € 6 billion mark in 2009, and reached €6.4 billion, an increase of 17%.' 'In 2009, almost 53.5 million orders were placed, an increase of 25% in comparison to 2008.' 'The average amount spent increased in 2009 by 13% to €737.' The expectation is that online consumer spending will increase in 2010 by 15% to €7.3 billion' (Blauw Research, 2010). Where so much money is involved, criminals will be active. In 2008, Dutch banks suffered a loss of €31 million through skimming – clandestine copying of bank card details and then plundering the account (*NRC*, May 18, 2009; KLPD, 2010a). An example of such a case appeared in the newspapers: 'According to the justice department, the five men and one woman from Romania and Moldavia, who are suspects in an extensive skimming case, made off with €1.8. million Most of this, 1.2 million, was accessed through one supermarket in Badhoevedorp' (*de Volkskrant*, July 27, 2010).

Cyberspace is also the place for discussions about ethics, the place where jokes that may not be jokes anymore circulate, the place where news travels fast but may not always be reliable. On

[5] It is not clear whether this girl was at her computer all this time, or whether, on the contrary, that she is also active on other profile sites. Being logged on to one site for 40 hours a week indicates a certain degree of fixation, regardless. Moreover, she has to participate actively on sugababes.nl to score enough points to stay at the top.

Monday, August 23, 2010, the Anne Frank tree blew down. ‘Less than half an hour after the Anne Frank tree blew down, pieces of it were offered for sale on the Marktplaats website.’ ‘Straight away high prices were offered for a piece of the tree. One visitor offered nearly €10 million,’ according to news from AT5 Amsterdam (www.at5.nl) at 15:16 that same afternoon. As an unsuspecting reader, you may think that that’s pretty spectacular. But AT5 is bad at reporting news. The news refers to two adverts on Marktplaats and both do indeed offer €9,999,999.00. But offers on this site are without obligation: they don’t commit anyone to buying or selling anything because Marktplaats is an advertisement site and not an auction site. The high offers may well be a protest against the trade in bits of the tree. Those who look more closely will notice that the person making the offer, called Fred, has another advert on Marktplaats in which he offers a T-shirt with the slogan ‘Have you been fooled lately?’ He recommends his T-shirts with the statement: ‘Unique shirt: the slogan will appeal to you!’ Perhaps his advert about the tree is a joke, an attempt to get a discussion going, a protest, an attempt to ridicule those selling branches, a way to give these vultures what they deserve? In cyberspace things are not always what they seem.

On a more serious note, the Royal Library issued a statement on Thursday August 26, 2010 with an emotional overtone, unsurprisingly perhaps to do with the Second World War (*de Volkskrant*, August 26, 2010). The Royal Library intends to put online unabridged versions of 26 Nazi inclined magazines from the thirties and forties. Around 300 thousand pages will be made available. ‘The Royal Library is a neutral organisation that does not wish to select documents on the basis of their contents,’ is how the library defends its decision. ‘We wish to make as much information as possible available for scientific research, and it should be unfiltered.’ The Ministry of Justice, according to newspaper reports, points out that the magazines may contain illegal material, such as hate speech texts that are punishable in terms of article 137c (insulting to a section of the population), article 137d (inciting discrimination against a section of the population) and/or article 137e (publishing discriminatory statements).[6] The Centre for Information and Documentation Israel (CIDI) is against placing this material online because it will cause a lot of trouble. The Dutch Institute for War Documentation (*Nederlands Instituut voor Oorlogsdocumentatie* (NIOD)) says that it concerns information that is already public. The NIOD thinks it is patronising that people can access the information through the Royal Library and the NIOD but cannot look it up on the Internet. This opinion demonstrates that the NIOD is somewhat ignoring the peculiar nature of cyberspace. There is a difference between getting sensitive information from the Royal Library premises in The Hague and downloading it instantly and anonymously from a website. The latter means that all barriers will be removed. The laws mentioned above make the publishing of certain texts punishable – regardless of how they are published. In the eyes of the law there is no difference between making something public partially or completely. The difference between the two is a moral dilemma. Is the Royal Library permitted to distribute texts over the counter to researchers but not to extreme right wing youths through the Internet? Where do we draw the line? These are questions for which academics have no answers.

The biggest problem in cyberspace is the question of who’s who, which person or organisation is hiding behind which user name and which user name can you trust. Identity fraud is the central problem in this virtual world. Charles den Tex brought this to the attention of the general public in his novel *Cel* [Cell] (2008).

[6] On hate speech, see Tienstra, 2008; Leukfeldt et al., 2010, Chapter 6.

In this world in which 500 million people are members of one organisation, people can easily hide behind an identity other than their own. It is a world in which emotions flare up around ethnic issues, in which as unsuspecting user you can't always be sure what is meant seriously, in which sugababes battle doggedly year in and year out and in which skimmers net €1.2 million in one supermarket: this is the world in which my research takes place. For this, I have derived a few pointers from Michel Foucault.

2.3 Foucault's vision of modern law enforcement

In his critical social analysis, French philosopher Michel Foucault points to the basic principles of law enforcement in our modern society. He was writing at the beginning of the 1970's, so in the pre-cyberspace era, but in my view his observations appear to a large degree to be independent of technology.

According to Foucault (1975), people behave in a controlled way ('disciplined' is the word he uses) because the authorities have a controlling effect on them. In his view, there is disciplinary machinery at work that drills things into people, and that breaks their spirit and makes them docile. This is not a cheerful vision, but Foucault does put his finger on the fundamental principles of controlling behaviour by the authorities in our modern society.

He sees behaviour control as first and foremost a matter of information or knowledge. Authorities that want to exercise effective control must have insight into what their citizens do. For this, citizens must be labelled (named) and registered at a fixed location (address). Then the authorities must keep an eye on them, preferably continuously and inconspicuously.

Surveillance in the broadest sense of the word, constantly spying, observing and recording: these are central to Foucault's approach. In this sense, the panopticon is a familiar metaphor: a prison in the shape of a dome designed in such a way that the inmates can be constantly watched without them knowing when it is happening. The expression 'the panopticism of society' points to the fact that citizens are being observed by the authorities in more and more areas so that places where they are anonymous and not under observation are shrinking. But it doesn't stop at monitoring.

The authorities, according to Foucault, have to record the information that they have gathered while monitoring citizens in personal files. They must then be able to challenge citizens individually about their deviant behaviour so that they can be brought in line with a desired code of conduct. Ultimately physical force should be possible, although effective control by the authorities should not rest on the repeated application of violence but rather on subtle monitoring via surveillance. Subtle monitoring is when citizens conduct themselves in a disciplined manner because they never know when they are being observed.

This modern method of control leads ultimately to people reaching a kind of permanent and innate state of constraint. It is then no longer necessary to actually exercise control; people are inherently controlled. Control is now separate from monitoring by authorities and people feel controlled even when there is no detectable authority. It involves a kind of self-control that has been instilled under a great deal of pressure. In Foucault's words: those being controlled 'should be caught up in a power situation of which they themselves are the bearers' (1979:201). In summary, the main elements of Foucault's approach are:

- people must be provided with a name and address, they must be identifiable and it must be possible to locate them;
- the authorities must gather information about citizens through observation;
- subsequently personal files must be kept;
- the authorities must challenge people about their deviant behaviour;
- physical force must be applied if necessary.

It is to Foucault's credit that he listed the principles of modern monitoring by authorities and put them into a logical order. However, the following comment is called for. Foucault ascribes the authorities with an awful lot of power. The question is whether the authorities, and the police on their behalf, have as much power as is designated in all the parts of his model. The police are pre-eminently the authority for formal social control. Police officers have the means to influence the behaviour of citizens if they subscribe to the informal processes of social control (see for example Bittner, 1967; Cachet, 1990; Van der Torre & Stol, 2000). The police are likely to be successful if they respond to contraventions of norms that citizens themselves consider to be serious and which citizens themselves are willing to rise up against, such as robberies, muggings and child abuse. If citizens recognise themselves in what it is that the police are tackling then they are prepared to offer their cooperation and information (report crimes, give tips, act as witnesses, provide forensic material). The authorities are quite powerless without this kind of support from the informal circuit.

The British sociologist Anthony Giddens (1993) is one of Foucault's critics. According to him, Foucault describes reality in terms of abstract processes and fails to take into account sufficiently the everyday reality in which people act and give direction to society. People are more than a by-product in a history steered by an invisible hand. People *make* history. One could say that the critique of Foucault is that he pays too much attention to structures and not enough attention to the people creating these structures as they go along. In this he does not take sufficient cognisance of the empire of everyday life. Foucault wanted to bring 'the primacy of the subject' up for discussion. He wanted to counterbalance the trend that puts human actors at the centre of everything, the subjectivism of the 1960's, a trend that to his mind had gone too far (see for example Foucault, 1985). He wanted to show that there are social processes that transcend the individual. He succeeded in this but at the same time he lost sight of humans as actors, according to his critics. Yet Foucault demonstrates that he is also of the opinion that his work calls for further interpretation. On the last page of his book about the principles of law enforcement, he offers it up as a background against which further study can be done into controlling behaviour and the production of knowledge in our modern society. There he writes: 'At this point I end a book that must serve as a historical background to various studies of the power of normalisation and the formation of knowledge in modern society' (1979: 308).

Foucault died at the age of 57 in 1984 and could therefore never have contemplated behaviour control in cyberspace. In a first general confrontation between Foucault's elements of authority control and cyberspace, it is evident that people are more anonymous on the Internet than they are offline and that monitoring is less simple on the Internet than it is offline. In other words, in the first two steps of modern law enforcement as described by Foucault, authorities will encounter difficulties in cyberspace. People are not easy to identify in cyberspace and there is no real systematic monitoring and gathering of information (generating of knowledge) by the authorities.

Internet surveillance is a topic that occupies those in police circles at the moment, not because it has solutions to offer, but because police officers are not sure what to do about it. The Internet shows that the system for use by the authorities to control behaviour as described by Foucault will not suffice, at least for the time being. Foucault's model leads to the conclusion that policing cyberspace is not a simple task.

Now that I'm studying the material in light of theory, I would like to see what scientific theory has to say about the supply side of the issue. Cutting to the chase: if there is no criminal behaviour in certain sectors of society or if self-regulating processes redress it on time, then there should be no objections if control from the authorities does not function very well in that sphere. With Foucault, we looked at behaviour control by the authorities; in the next section I will focus briefly on theories about deviant behaviour. In the section after that, I will discuss the practice of deviant behaviour in cyberspace.

2.4 Theory and deviant behaviour in cyberspace

While criminologists study why people resort to deviant behaviour, sociologists are the ones who study how people manage to prevent their societies from succumbing to chaos. How do people preserve social order (e.g., Elias, 1939; Berger & Luckman, 1966; Giddens, 1984)? Why do the majority of people *not* resort to criminality? If we want to know why people behave abnormally in cyberspace, it is good to review why people follow the beaten track and make an effort to ensure that society is decent both off- and online. When researching cyber safety we should therefore use criminological and sociological methods, insights and theories. I will not be giving an exhaustive or even extensive overview of criminological and sociological theory; for this I gladly refer you to others (e.g., Calhoun et al., 2007; Akers & Sellers, 2009).

What concerns me here is to gain insight into what the theory predicts regarding deviant behaviour in cyberspace. Obviously we are well aware that criminals frequent cyberspace a lot; we don't need theories for this. I will return to this; my first question is whether there are grounds for assuming that cyberspace will lead to an increase in crime in our society or whether it is a case of criminality moving from offline to online.

From criminology, we can apply the rational choice theory (e.g., Holtackers, 2007; Ferwerda, 2008; Akers & Sellers, 2009). This theory holds that people are rational, calculating beings. They strive towards goals – having an expensive car and status for example – and consider how they can reach these goals. If these goals are reached using criminal means and the chance of getting discovered is or seems slim, then rational consideration between the risks and the benefits will lead to choosing crime as a means. Given that the Internet offers new opportunities for criminal practices, supplementing the opportunities that have existed for a long time, and given that people on the Internet are less susceptible to control, or think they are less susceptible, it is to be expected that they will be more likely to opt for criminal behaviour, according to the rational choice theory. This theory therefore predicts that cyberspace will lead to more crime in our society.

Whether people are actually more anonymous when online, and whether they have less to fear from monitoring when they are online, is not of paramount importance here. If people *believe* that they are anonymous and if they *believe* that they are not being watched, then that will suffice. The Thomas theory applies here and it says: 'if men define situations as real, they are real in their consequences' (Merton, 1968: 475). In other words, if people believe that they are anonymous and if they believe that they are not being monitored, then they will act as if this is the case.

Leukfeldt (2010) takes the rational choice theory as the basis for his research into e-fraudsters. On the basis of this theory, he predicts that there is a new group of perpetrators to be observed: people who previously considered the risks to be too great but now with the Internet do dare to swindle other people. His analysis of over 170 police files to do with e-fraud and 226 police files to do with offline fraud shows that e-fraud perpetrators are younger on average than offline fraudsters. Using background characteristics of perpetrators, which includes information about antecedents, his analysis leads to the conclusion that perpetrators progress from theft to fraud sooner in their criminal careers. According to Leukfeldt, cyberspace is not producing an entirely new group of criminals:

> *'E-fraudsters are significantly younger than classic fraudsters ($p<0.05$). They commit crimes through the Internet earlier in their lives. Furthermore, e-fraudsters move significantly earlier from financial crimes without violence into fraud crimes than classical fraudsters. This indicates that the threshold to commit fraud crimes through the Internet is lower than the threshold in the physical world.' (2010: 63)*

He explains this acceleration in the criminal careers of property fraudsters by pointing out that fraud on the Internet requires fewer social skills – and is therefore less risky for those starting a career in fraud – than fraud in the physical world. The rational choice theory therefore offers a partial explanation at best: the theory can explain why property criminals move from theft to fraud sooner. But contrary to what can be derived from the theory, Leukfeldt does not identify a completely new group of perpetrators.

Felson and Cohen's routine activity theory is a criminological theory based not only on offenders but on victims (Akers & Sellers, 2009). This is a theory that predicts criminality by studying those everyday routine activities that increase a person's chance of becoming a victim. According to this theory, criminality arises in situations that combine a motivated perpetrator and an attractive target in combination with a low degree of monitoring: 'the likelihood of crime increases when there are one or more persons present who are motivated to commit a crime, a suitable target or potential victim that is available, and the absence of formal or informal guardians who could deter the potential offender' (Akers & Sellers, 2009: 35). For instance, those who go out a lot have a greater chance of ending up in this kind of situation, and thus of becoming a victim, than those who habitually stay at home in the evenings. Cyberspace extends people's range of activities, as well as the number of places that people can frequent (web forums, auction sites, online games, web shops, profile sites and so on) and where they can meet motivated offenders. After all, it is through the Internet that offenders and victims can easily come in contact with each other, even if the potential victims don't frequent risky places. According to this theory, the fact that social control in cyberspace is not as simple as it is offline works to the advantage of criminals.. The routine activity theory resembles the rational choice theory in as much as it predicts an increase in crime as a result of cyberspace.

Van Wilsem (2010a) uses the routine activity theory as a framework for analysis in his research into daily online and offline activities and online and offline victimization through threats. His conclusion, on the basis of a quantitative analysis of victimization (N = 6,896), is that certain routine activities in cyberspace increase the risk of victimhood both on- and offline, and the same applies to certain routine activities in the traditional world. There is evidently a multidimensional interconnection between the online and offline worlds. It does not follow from his research what exactly we are to make of these influences, how the processes work precisely, and what leads to what. These aspects, according to Van Wilsem, 'should be the subject of further research, for example through a smaller scale qualitative study' (2010a: 86). While his research did not focus on the question of whether there is more or less crime because of cyberspace, his findings indicate that cyberspace leads to an increase in opportunities and combinations that result in criminal activity.

From sociology we can apply the control or commitments theory of which the American Travis Hirshi (1969) in particular was a proponent (Wilterdink & Van Heerikhuizen, 1993; Veenstra et al., 2009). The essence of this theory is that people are less likely to commit crimes if they are more tied to, and also feel more tied to, the community in which they are active. Here it is not only rational considerations that play a role, as they do in the rational choice theory, but also moral and emotional factors. Those who follow their intuition will easily arrive at the conclusion that people feel less committed to one another in cyberspace than they do in the offline world. It is much more fleeting, you never look each other straight in the eyes. People often have hundreds of 'friends' on social networking sites but the depth of these friendships is questionable. Old ties through family, friends, school, church, sports clubs and work don't disappear overnight, but because people are now spending a part of their social time in transitory cyberspace, their social ties are becoming more spread out, and with this, weaker. If we follow this reasoning, we will arrive at the conclusion via the commitments theory, too, that the rise of cyberspace will lead to more crime.

In this respect, the labelling theory must not go unmentioned. The core of this theory is that deviant behaviour is not a characteristic of how criminals behave in its own right, but that it arises because the dominant group in society determines certain behaviour to be deviant and attach the label 'criminal' to it. The best summary is still the one given it by Howard S. Becker in his *Outsiders*: 'deviant behavior is behavior that people so label' (1963: 9). In other words: 'crime is what you call it'. Since the rise of the Internet, several kinds of actions that were not initially punishable have now been included in the criminal code. Hacking serves as an example of this. Snooping around on someone's computer, even if you did not have permission to do so, was not punishable until 1993. Hackers could only be prosecuted if they proceeded to do something punishable, such as destroying the computer once they had broken into it. In 1993, breaking into computers was made an offence in its own right, and included in the Criminal Code. Later the requirements that security had to have been breached and that the intention was unlawful were dropped. Gradually, the liability to punishment due to hacking has been extended and more and more actions undertaken by hackers have become *punishable* actions. With this, crime has increased and so the labelling theory also predicts an increase in crime thanks to cyberspace. Because of cyberspace, new offences have been included in the Criminal Code – without an accompanying scrapping of as many existing crimes. If we also take into consideration that cyber criminals commit certain offences extremely frequently – take, for example, the downloading of child pornography – then the obvious conclusion has to be that cyberspace leads to more crime according to the labelling theory as well.

The various theoretical notions can be summarised as follows. Cyberspace extends the repertoire of human activity and at the same time leads to an increase in the number of offences. It thus increases the opportunities for breaking the law – with an actual increase in criminal activity as a consequence. Empirical research based on theory confirms that the potential for committing crimes is increasing and that these opportunities are being taken.. At the same time, empirical research shows that reality is not simple to predict using theories; it is too complex for this.

That covers some of the theoretical side of things. In the social sciences, theory on its own seldom confirms anything. Theories have to be *proven*; they must rest on evidence. Theories point to possibilities and probabilities, and help us with our observations. So, there is reason to assume that cyberspace leads to an increase in crime in our society – on the one hand because the characteristics of cyberspace seem favourable for criminal activity and on the other hand because cyberspace has qualities that are unfavourable for effective behaviour control by the authorities. It is then our task to research how reality actually works against this background, and how it develops. Is there evidence of an increase in crime? Are new perpetrators behind it? Or are they existing perpetrators committing new kinds of offences? Is there evidence of a displacement effect (compare Hesseling, 1994)? It is time to look at what has already been researched. What does the problem of deviant behaviour in cyberspace look like in practice? What do we know about it?

2.5 Deviant behaviour in cyberspace, special cyberspace

To start with, here's a somewhat disappointing announcement: we don't know an awful lot about it. But this is the reason why my chair is described as 'Police studies – paying particular attention to issues of cyber safety', because for the safety of our society it is high time we found out more about it.

Aberrant behaviour is a concept that is broader than criminality. We see deviant behaviour that is not necessarily unlawful, particularly among the youth in cyberspace. Bullying is probably the most familiar example of this. Many schools have programmes that address cyber bullying. The law only starts to apply when bullying turns into threats, extortion or discrimination. This is also the case regarding information and communication of a sexual nature, where some may fall outside the reach of the law and yet is still considered to be deviant and unwelcome. I will however restrict myself here to cybercrime since there is enough about this phenomenon that we know nothing about.

The first questions that need answering are quantitative. How often do the various offences occur? How extensive is the damage? How many offenders or groups of offenders are active? These are questions that need answers so that policy priorities can be established and policies can be evaluated. But we don't have answers for even the simplest question 'How often do citizens and businesses fall prey to cybercrime?'

In July 2010, Dienst Nationale Recherche of the National Police Services Agency (NPSA) wrote a report about areas of attention in criminality. The version for the public contains the following:

> *'The growth of the cybercrime phenomenon and high tech crime continues unabated. In as much as it can be measured, the figures over the years demonstrate an exponential growth, in some areas up to 100% per annum. This growth is made possible to an extent because the rapid technological developments in society give rise to new "attack vectors". Alongside this, security awareness in society in this regard is often low. Also, the speed and creativity with which cyber criminals react and adapt their modus operandi is high. The dividing line between high tech crime and other forms of criminality is becoming blurred.' (KLPD, 2010b)*

On August 27, 2010, MP for the Socialist Party, Gesthuizen, posed questions about cybercrime to the Minister of Justice (Lower House, 2010Z11937). I have listed four of these below; they illustrate the somewhat impoverished state of knowledge in my field of research:

- Question 1: Are you aware of the report about the exponential growth of cybercrime in the Netherlands?
- Question 2: How many cases are there annually? Is this measured on the basis of reports? If so, how extensive do you estimate the problem to actually be, given that not all cases are reported to the police?
- Question 3: How many of the cases that are reported are actually solved and lead to prosecution of offenders? Are you satisfied with the results? If not, what do you intend to do to increase the percentage of crimes solved?
- Question 4: Where do you think the bottlenecks are to an effective response from the police? How are you going to address these bottlenecks?

At the moment there are no proper answers to these questions, but people are working on them. Together with my colleagues, I am working with the NPSA, the police force's Programme for Combating Cybercrime and the Central Bureau for Statistics on a nationwide study into victims of cybercrime among citizens. This should introduce cybercrime as a permanent element in the national security monitor. A national study into victims of cybercrime in business is also on the agenda, but is as yet in the early stages. This shortage of knowledge means that, at present, all policies developed to tackle cybercrime are insufficiently grounded. Whether these measures are effective is entirely unclear due to a lack of research in this respect. Policies to tackle cybercrime at present are mainly a question of estimating as best we can how things are developing and accessing the mechanisms at work.

It is however possible to say something concrete about the extent of cybercrime in the Netherlands. Less than 1% of reports filed by the police involve this kind of crime (Domenie et al., 2009). That is not much. A small study among 1,246 Frisian Internet uses showed, however, that willingness to report cybercrime by victims is low: no more than 4.2% (ibid.). The average percentage of reporting for all kinds of offline crime is 26.7% (CBS, 2010). The percentage of those who report cybercrime is thus six to seven times lower than the average for offline crime. So there is apparently more at play than the 'less than 1%' leads us to suspect.

In the study among Frisian Internet users, it emerged that 2.7 of them had been victims of hacking and 1.2% of e-fraud (excluding 'attempts at') during the previous year (Domenie et al., 2009). During this study, respondents were asked if they had fallen victim during the previous two years. It is not possible to halve the percentages in order to say something about victimhood in one year because that is not how it works when people are asked to indicate how often they experienced a given phenomenon over a given period of time (compare Van der Vaart, 1996). What we can state is that of the Frisian Internet users, not more than and presumably less than 2.7% were victims of hacking in one year, and not more than and presumably less than 1.2% were victims of e-fraud.

From a panel study among 6,896 respondents from 4,353 households and aged 16 years or older, it emerged that 2.2% of the respondents had fallen victim to digital threats in the previous year. It was particularly those under the age of 25 that reported this kind of victimisation (Van Wilsem, 2010a). Prior analysis of the same database, but then only among those who indicated that they used computers on occasion, and who moreover had no missing values for the variable used on the analysis (N = 6,201), showed that 2.5% of the respondents had fallen victim to online fraud in the previous year – in the sense that they had bought goods online that had never been delivered (Van Wilsem, 2010b). Obviously there are various kinds of online fraud (compare Van der Hulst & Neve, 2008; Leukfeldt et al., 2010), but the panel were not asked about these. Victimisation here too was mainly concentrated among those in the younger age groups. 'Respondents under the age of 35 are relatively frequent victims (more than 4%) and the risks are particularly low among those above the age of 55 (around 0.5%' (2010b – in press).

Table 2.1 Victimhood cybercrime compared to offline criminality

Type of offence	**Percentage of victims**	**Measured per 1 or 2 years?**	**N (sample)**
Cybercrimes			
Hacking*	2.7	2	1,246
E-fraud*	1.2	2	1,246
Threats#	2.2	1	6,896
Fraud#	2.5	1	6,201
Offline criminality			
Break ins^	1.3	1	200,000
Cycle theft^	5.4	1	200,000
Pick pocketing^	1.8	1	200,000
Abuse^	1.1	1	200,000
Sexual offences^	1.5	1	200,000

* among Frisian Internet users.

Source: * Domenie et al., 2009; # Van Wilsem, 2010a, 2010b; ^ CBS, 2010.

These scanty figures for victimhood in the Dutch setting lead to the preliminary conclusion that victimisation due to hacking, online threats and e-fraud is not negligible. These percentages are similar in size to those for victims of offline offences such as break ins (1.3%), cycle theft (5.4%), pick pocketing (1.8%), abuse (1.1%) and sexual offences (1.5%) (CBS, 2010). From this perspective, cybercrime is indeed a bigger social problem than the 'less than 1% of crimes registered by the police' leads us to suspect (Table 2.1).

More is known about the nature of cybercrime than about its extent and developments in the field. For instance, Van Wilsem's (2010a, 2010b) finding that victimization is concentrated among the younger age groups is something that we also saw in Leukfeldt et al.'s study (2010). Van Wilsem's analysis of 665 police files involving cybercrime concluded that significantly both the perpetrators and the victims of cybercrime are often to be found in the younger age groups. People aged 24 and younger are conspicuous as perpetrators of hacking, hate speech and dissemination of child pornography. Cybercrime, more so than other unlawful behaviour, is apparently the domain of younger people. Studies also describe how perpetrators operate, their motives and their background characteristics (e.g., Van der Hulst & Neve, 2008; Leukfeldt et al., 2010).

One of the most important findings in the study by Leukfeldt et al. is that cybercrime, just like offline crime, has become an everyday occurrence. Under the heading 'Cybercrime belongs to the people', they wrote:

> *'At the start of this study and on the basis of literature, the media and policy documents, we had an image of high-tech cybercrime that operates from abroad in organised groups that claim their victims on a large scale. This image needs to be re-evaluated. Our files show that it is especially "minor offences" that are committed by more or less everyday suspects operating individually. This does not mean that there are no organised cybercriminals active in the Netherlands. However, we did not come across many reports against such groups in our study of the files. Possible the work of such criminal groups is not recognised as such, not even by the victims. In the files we did see evidence of the presence of organised crime: we saw instances of deposit fraud in which the victims were told that they had won a prize; we saw that a person suspected of downloading child pornography had acquired the material from an organisation. But in general organised crime hardly plays a role in the files.' (2010: 254)*

The NPSA's Team High Tech Crime specifically discusses groups of organised cybercriminals, operating internationally in their *Crime profile analysis* (KLPD, 2010a). Cybercrime may be everyday and it may belong to the people, but as is the case with ordinary crime there are also 'professionals' that commit crimes through criminal cooperation and in technically advanced ways. This high-tech crime is 'growing exponentially', according to the NPSA, and is made possible by a combination of technological development (new opportunities for crime) and low security awareness in society.

> *'Botnets are the spinal cord of high-tech crime. They are used for a range of activities, from sending spam to stealing identities. In addition to this, underground Internet forums play an important role in the high-tech crime world. They can be seen as the digital meeting places where supply and demand come together and where people exchange tips, tricks and insights. Collaborations between high-tech criminals are mostly virtual. They know each other from forums and only by nicknames. The specialist nature of high-tech crime practically necessitates extensive cooperation between criminals. More and more groups are now involved in the full range of activities, from infections to appropriating money, all under their own control.' (KLPD, 2010a: 181)*

> *'Depending on their specific modus operandi, various services are employed such as laundering networks, malware writers, translators, botnet herders, skimmers, spammers, hackers, financial specialists, bulletproof hosting providers, or whatever is necessary to achieve their aims. There is a wide range of modi operandi and a large degree of inventiveness.' (2010a: 89)*

High-tech criminals aim primarily at financial rewards. 'This by no means excludes the same techniques from being used for non-financial goals such as cyber warfare or revenge, but in the field of high-tech crime it is generally about financial reward' (KLPD, 2010a: 89).

The NPSA concludes that high-tech crime is developing rapidly, both in extent and complexity (techniques, relationship networks). The damage from cybercrime is difficult to measure through 'a shortage of information, misclassifications and changing terminology' (2010a: 111). Despite this, the NPSA calls this trend alarming because the losses due to high-tech crime continue to rise and double, in some cases annually, despite a clear growth in attention being paid to the combating of this kind of criminality.

The annual Govcert Trend Report on cybercrime (Govcert, 2009) contains a lot of information about recent developments in attacks and security. Summarised, Govcert mentions the following as important trends:

- Internet safety is waning.
- Internet users and their software remain vulnerable to cyber criminals.
- Weaknesses in the Internet's fundamental structure make it vulnerable.
- Krypton graphic techniques become obsolete faster than assumed.
- Threats move with new applications (e.g., mobile Internet).
- Abuse of personal information is a structural problem.
- Ideological conflicts will have a cyber-component from now on.
- International cooperation within the security community is on the increase.
- Prevention and tracking of cybercrime is achieving success.

Those who wish to explore further the nature of cybercrime in the Dutch context can consult recent studies about this kind of crime, either by way of literature research (Van der HUlst & Neve, 2008), or police files (Leukfeldt et al., 2010), or a victim survey (Van Wilsem 2010a 2010b), or through expert insights into security (Govcert, 2009).

I will now move from cybercrime to ways to combat it. We have just seen that cyberspace brings new kinds of crime in its wake. Not only that, the indications are that more offences are being committed in our society than was previously the case. In a healthy society, these kinds of developments will not pass without a reaction; people will rise to the challenge. Initially, Internet users themselves will take steps, for example by installing good computer security software, by not responding to suspect or tempting offers and through careful management of personal data. In the second line of defence against cybercrime we find moderators, web managers, Internet service providers, software producers and hardware suppliers. We extend greater responsibility for cyberspace safety to Internet security companies and other private sector players than we do to the average end user. If citizens and these other parties are unsuccessful, they can appeal to the authorities' enforcement apparatus. Although we have seen that willingness to report cybercrime is low, I have recently seen that private institutions and the police are joining forces more often in the battle against cybercrime. The police have taken measures to be better equipped, for example as witnessed by the Programme for Combating Cybercrime (*Programme Aanpak Cybercrime*) and all the initiatives linked to this. This will undoubtedly lead to citizens and businesses reporting cybercrime more readily. All in all, the role of the police in combating cybercrime will increase.

Peculiar to police intervention is that it goes hand in hand with the legal authority to act. I will now turn to this aspect.

2.6 The police and authority

To start with, the police can and may, just like anybody else, use the Internet as a source of information that everyone has access to, in police jargon: it is an open source. In criminal cases, however, the police and the justice department are allowed to go further than others. They have powers that are intended especially for investigations in cyberspace. Generally, these powers are derived from European directives; many of the substantive laws concerning cyber safety are also the consequence of European laws and regulations.

An example of this is the Council of Europe's Convention on Cybercrime of November 23, 2001 (ETS no. 185) that resulted in the Dutch Computer Crime II Act of June 1, 2006 (which came into effect on September 1, 2006). Among other things, this act led to the inclusion in the Code of Criminal Procedure the so-called 'bevriezingsbevel' (art. 126ni Code of Criminal Procedure). This allows the public prosecutor to order an Internet provider to 'keep available' certain client information for the purposes of criminal investigation.

The European Parliament and the Council of Europe's Data Retention Directive of March 2006 (2006/24/EC) lead to a change in the Telecommunication Act in the Netherlands on September 1,2009. Through this law, those offering telecommunications services now have to store information about the surfing and telephone habits of their clients for a period of 12 months 'for the benefit of investigations, tracking and prosecution of serious crime' (art. 13.2a Telecommunications Act; see Appendix 1). Obviously, those offering telecommunication service are also obliged to hand over this information to the police and the justice department should they require it on the basis of an article in the Code of Criminal Procedure (art. 13.4 Telecommunications Act).

The first book in the Code of Criminal Procedure contains various other articles that are relevant to authority in cyberspace, including the means to search the computers of suspects, the requisition of passwords, storing of information and making data inaccessible (125i – 125n CCP; see Appendix 2). The law is continually developing, both in the formal and material sense. The Lanzarote Convention of October 25, 2007, for example, resulted in the grooming of minors becoming a punishable offence (248e Criminal Code). Recently the media reported that a 37 year old man from Den Bosch was prosecuted as the first suspect under this act.

> *'The man, originally from Eindhoven, was arrested in his home on May 15 on suspicion of grooming: using the Internet to systematically approach minors and win them over with a view to having sex with them. He got into trouble as he was about to make a date to meet a 12 year old girl from Almere with whom he had had contact for some time through the social networking site Habbo (a meeting place for teenagers in particular) and the chat programme MSN. Detectives took action once the man had proposed a concrete place and date for a sexual encounter, sent her directions for how to get there and a travel schedule.'*
> *(de Volkskrant, August 20, 2010)*

Meanwhile, another proposed law to do with cybercrime is in the pipeline, this time making 'fencing of data' illegal.[7] These are essential changes to the law, but the question of whether the police are keeping pace arises, given that even the recording of arbitrary cybercrime reports is already causing problems for the police staff responsible for taking down statements (Toutenhoofd et al., 2009).

[7] See Draft legislation

Police powers are also changing very quickly. This proposed law includes giving the public prosecutor the authority to demand that information be made inaccessible. Yet whether the police and the justice department use these specific cybercrime related powers, and if so, to what effect, and if not, why not, and which obstacles they come across, are all questions for which we don't have answers. This is not a good situation to be in. For a start, those representing the people should be monitoring law enforcement. Secondly, it is also crucial for the police themselves that the use of these powers is evaluated because this can help them in their work.

Apart from special means of force, the Code of Criminal Procedure also contains special powers of investigation. These powers have a history that is worth mentioning here. At the beginning of the 1990's, the police found themselves in a crisis situation regarding investigations. This crisis came to light in 1996 through the Parliamentary Inquiry into Investigation Methods (Van Traa Commission) and was described in their thick report entitled *On investigations*. The police had created this crisis in the years leading up to this inquiry because of their generous interpretation of the law. In their drive to round up criminal gangs, they went too far in their methods, and acted more or less according to the principle: if it is not explicitly forbidden by law, then it is permitted. Many of the methods that had developed in the field had no basis in law, and as such there was no supervision of the police in crucial areas. Van Traa dressed the police down in no uncertain terms about the various investigatory methods in use at the time.

> *'It is for this commission beyond dispute that there has been a proliferation in methods of investigation during the last five to ten years. These methods are only partially regulated in law. (…) The freedom and actual possibilities open to the investigation services has been insufficiently regulated by law.' (PEO, 1996:427)*

The commission emphasised the importance of having a legal basis to support the work of the police and the justice department.

'Many observation methods lack a specific legal foundation. In case law, observation methods are often judged legal on the basis of article 2 of the Police Act 1993 and article 141 and 142 of the Code of Criminal Procedure. It is the opinion of the commission that this basis is too narrow. Specific standards are necessary for observation (tracking), tapping, scanning, using technical aids, 'look-inside-a-house operations'[8] and the use of information gathered through observation.' (1996:429)

On February 1, 2000 the Special Investigatory Powers Act 2000 (*Wet BOB*) came into effect as a direct consequence of the parliamentary inquiry. The aim of BOB Act was to standardise investigations and make them more transparent and easier to monitor according to the principle: if it is not explicitly permitted, then it is *prohibited.* The police are not allowed to invent new methods to combat crime, no matter how good their intentions are. The special investigatory powers of the BOB Act are laid down in the Code of Criminal Procedure under 'special powers for investigations'. Examples of these powers include: the systematic observation of a crime suspect (126g CCP), the systematic acquisition of information about such a suspect (126j CCP) and pseudo-purchasing – which means that undercover police agents are authorised to do business with suspects in an effort

[8] Without the owner knowing this.

to win their confidence so that more insights can be gleaned into the crimes under investigation (126i CCP).

Pseudo-purchasing shows us that law-makers are moving with the times and that they are also taking policing in cyberspace into account when it comes to special investigatory powers (see Appendix 3). Initially, pseudo-purchasing involved receiving goods, such as drugs or weapons, from the suspect, and offering services to the suspect. The Computer Crime II Act added that pseudo-purchasing included acquiring (buying or trading) of computer data.

I have covered a few of the powers available should a cybercrime have been committed and the police have a suspect in their sights. However, there is more to police work than this. It also involves detecting potential problems, charting them and preventing problems from actually arising. For this the police have developed an arsenal of techniques, such as carrying out neighbourhood scans (Van Panhuis, 2008), conducting crime projection analyses (Moerland & Rovers, 2000; Moerland & Boerman, 2003; Van Panhuis, 2008; DNR, 2010), creating threat assessments (Boerman et al., 2008) and sketching offender profiles (Van Ruth, 2008), to mention a few. These methods support police efforts for safety in cyberspace, despite the fact that work still remains to be done to fine tune them.

A word of warning is called for here. Since *On investigations* two things have changed. Firstly, the impact of Van Traa's hard words of warning has softened somewhat, and secondly we now have cyberspace. Cyberspace presents the police with new law enforcement and investigatory issues. The police are not exactly sure what permissible methods are on the Internet. Legislators have regulated various powers for the police and the justice department, as I have just mentioned. But these powers don't automatically provide answers to questions such as whether the police are permitted to carry out surveillance operations, whether they are permitted to take part in virtual communities of a dubious nature, such as paedophile networks, or whether they are permitted to block unlawful information using filter techniques. If they are allowed to carry out these activities, then they need to know how and under which circumstances they are permitted. Once again the police are looking for the middle path between on the one hand, the principle that all that is not expressly forbidden is permitted, and on the other hand, that only that which is expressly permitted is allowed. The somewhat rigid principles of the Van Traa commission are not automatically the basis of their thinking. The police seem more inclined to once again to seek out the boundaries of the law.

An example of this is a report that appeared in the press in 2008 which stated that the police had hacked the computers of criminals to gather information during an investigation. The danger of experimenting with new investigatory techniques is that the police will once again find themselves in an investigation crisis, this time in cyberspace. The Minister of Justice recognises this danger. In his letter to parliament of June 29, 2009, the minister reports that it has become apparent that 'there is a need for an explanation of the laws and regulations and how to apply the special investigatory powers regarding the Internet' (TK, 2008/09, 28.684, no. 232). In connection with the searching of computers belonging to criminals, he also announced in this letter that 'the need for legislation tailored specifically to the situation in the Netherlands' will be further explored. In response to this, the draft legislation 'Reinforcing the fight against cybercrime' has been put forward, containing proposals to change the law as follows:

- 'to arrive at an independent arrangement regarding the powers of the public prosecutor to render information on the Internet inaccessible';

- make ‘fencing of computer information’ illegal;
- extend ‘the criminal provisions regarding eavesdropping, tapping or recording of confidential communications’.

This draft legislation is a recent illustration of how legislators are responding to new developments in the digital world: new and more extensive criminal provisions are devised so that deviant behaviour in cyberspace is brought under the auspices of criminal law, and new powers are created so that the police and justice department have grounds upon which to tackle cybercrime. What is happening here is not unusual: new opportunities to commit crime arise in society, criminals use these opportunities and society responds by taking measures to stop these crimes. We ought to have regulations and other facilities at our disposal for enforcing the law including a police force with the powers and the capacity to apply them adequately, particularly since the Internet has become such a crucial part of our society.

Just about every single new regulation to enforce the law in cyberspace attracts both words of approval as well as strong criticism. The latter generally comes from the minority but expresses an anxiety that is deeply rooted in our society. For this reason, it is good to take it into consideration. This anxiety is related to the creation of a police state, as it is known. The combination of new technology in the hands of the police apparatus, together with ever increasing powers, bring to the minds of many an Orwellian society. Often critics interpret new powers as an infringement of their right to privacy; this is also the case with the draft legislation just mentioned.[9] But what is happening in our society is not what Orwell predicted in *1984*. He was wrong in one important aspect. It is important to recognise this because there are lessons to be learned for policing in cyberspace. Let us stop to refresh our memories, consider the book in question and the discussion that goes with it.

2.7 Orwell’s *1984* … and more[10]

George Orwell’s novel, *1984*, was published in 1949. He looked 35 years into the future and did so almost 30 years before IBM launched their first personal computer onto the market (that was in 1981). Orwell wrote about a society in which the authorities monitored citizens via omnipresent ‘telescreens’ that could not be switched off. These machines were televisions, video cameras and intercoms all in one. The views of the leader are continuously to be heard on the television, a leader who goes by the comforting name of Big Brother. The video camera part of the machine comes equipped with an intercom function and is intended to observe people and correct them should they display deviant behaviour. The authorities make no secret of the fact that they are constantly watching their citizens. On the contrary, everywhere posters on the walls remind them ‘Big Brother is watching you’.

Winston and Julia are the protagonists in the novel. We are first introduced to Winston, who feels that he is different to the rest, that he has the right to his own thoughts and time to himself. This is of course highly suspect. Julia and Winston fall in love, so much so that they dare to flout the supervision of Big Brother. Together they create their own world in a room above a junk store, somewhere in a forgotten and somewhat shady neighbourhood. In the climax of the novel it turns out that the shopkeeper is connected to the Thought Police. ‘There was a snap as though a catch had

[9] http://www.vkblog.nl/bericht/326717/Minister_Hirsch_Ballin_legt_bom_onder_rechtsstaat.

[10] Parts of this section have been published previously (Stol, 2003).

been turned back, and a crash of breaking glass. The picture had fallen to the floor, uncovering the telescreen behind is. "Now they can see us," said Julia. "Now we can see you," said the voice' (Orwell, 1949: 230-1). Winston and Julia stand naked against the state apparatus and are arrested. The Thought Police instil in them state discipline in the Ministry of Love until they are physically exhausted and spiritually broken. 'Almost unconsciously he traced with his fingers in the dust on the table: 2+2=5. "They can't get inside you," she had said. But they could get inside you. (…) But it was all right, everything was all right, the struggle was finished. He had won the victory over himself. He loved Big Brother' (Orwell, 1949: 303, 311).

This is how the expression 'Big Brother' or 'Orwellian society' became proverbial for a government that uses information technology to discipline its citizens. The authorities acquire information technology and use it everywhere and constantly to monitor its citizens. These same authorities have far-reaching powers and citizens who don't toe the line are picked up and put under pressure for as long as it takes for them to let go of their idiosyncratic thoughts and adopt the philosophy of the state as the truth. In this society, privacy is suspect, for traitors have thoughts that undermine society and customs. And this is why more information technology in the hands of the authorities is, for many, linked to far-reaching infringements of privacy and other civil rights.

Orwell's novel falls within a philosophical tradition involving tension between rational-technological thinking on the one hand and essential human aspect, such as ethics, feelings, intellect, emotions, originality and aesthetics on the other. In short, the tension between machinery and humanity. Various authors refer to the mechanical aspect of this using various terms such as Rationalisation (Weber, 1922), The Machine (Mumford, 1934), Technology (Ellul, 1954), Technological Rationality or 'Techno-logic' (Marcuse, 1964), Discipline (Foucault, 1975), Surveillance (Lyon, 1994) and Technology (Fukuyama, 2002). Some are more radical than others, but they all arrive at a shared conclusion: the technological complex is dominating more and more. This immediately raises the question of what space remains for being human.

Some authors point to the possibility of the problem solving itself because people will gradually reconcile themselves with the technological complex. They will transform into machine-people that Haraway (1991) calls *Cyboras* for short, and they will no longer struggle with it. 'He loved Big Brother,' is how Orwell summarises this. Mills (1959) speaks of 'cheerful robots'. In Aldous Huxley's dystopia *Brave New World* (1932), people have succumbed en masse to a life controlled by technology. According to Fukuyama, this is the biggest fear that people have of modern technology, 'that we could undergo this change without realising that we have lost something of great value' (2002: 128).

Orwell does not debate the issue in abstract terms like many of the other authors generally do. He was not a scientist or philosopher, but worked for the police, in the army and in education – and he was a writer.[11] Orwell's strength in *1984* was that he got to the core of the discussion, magnified it and sketched the dilemma in concrete images, in images that large groups of people can understand. There are no conflicting concepts in his work, no invisible hand of history and no structures without acting subjects, but real-life characters – Winston and his lover Julia – in a body and mind conflict with real-life police officers that have at their disposal the power and the technology.

[11] According to the preface of *1984*, Penguin Books edition, London, 1990.

The police, the authorities and technology find themselves at the heart of this discussion. The government apparatus that comprises a combination of the police, authorities and technology together form the very concrete machinery for which we should be afraid, according to Orwell that is.

The police in our society are indeed the strong arm or power apparatus of the authorities. The police have the monopoly of violence, but it is not theirs to do with as they please. According to article 2 of the Police Act 1993, the police carry out their task 'in subordination to the authorised powers'. When it comes to law enforcement – in cyberspace too – the police are under the command of the public prosecutor, and the Minister of Justice bears ultimate responsibility. He in turn answers to parliament. The press record the process. So there is supervision of the powers that be. Yet are we paying sufficient attention? Or is it, as Fukuyama claims, that something precious is being lost?

Critics claim that extensions to police powers in cyberspace, as laid down in the draft legislation mentioned above, bring in their wake the loss of things of value – namely our privacy and our fundamental rights – as discussed on *de Volkskrant*'s weblog (www.vkblog.nl, July 29, 2010). A paragraph entitled 'Minister Hirsch Ballin puts a bomb under the constitutional state' includes the following: 'This is in fact the introduction of Internet censorship and an outrageous attempt to restrict the right to freedom of expression and freedom of information.'

The French sociologist Jacques Ellul was decidedly negative about the combination of police and technology. In *The Technological Society*, he writes the following – and I am affording myself a long quote because as long ago as 1954 Ellul put into words the fear for police with technology to much better effect than many webloggers of today:

> *'Another example is the police. The police have perfected to an unheard of degree technical methods both of research and of action. Everyone is delighted with this development because it would seem to guarantee an increasingly efficient protection against criminals. Let us put aside for the moment the problem of police corruption and concentrate on the technical apparatus, which, as I have noted, is becoming extremely precise. Will this apparatus be applied only on criminals? We know that this is not the case; and we are tempted to react by saying that it is the* state *which applies this technical apparatus without discrimination. But there is an error of perspective here. The instrument tends to be applied* everywhere *it* can *be applied. It functions without discrimination – because it exists without discrimination. The techniques of the police, which are developing at an extremely rapid tempo, have as their necessary end the transformation of the entire nation into a concentration camp. This is no perverse decision on the part of some party or government. To be sure of apprehending criminals, it is necessary that* everyone *be supervised. It is necessary to know exactly what every citizen is up to, to know his relations, his amusements, etc. And the state is increasingly in a position to know these things. This does not imply a reign of terror or of arbitrary arrests. The best technique is one which makes itself felt the least and which represents the least burden. But every citizen must be thoroughly known to the police and must live under conditions of discreet surveillance. All this results from the perfection of technical methods.' (1954: 100)*

Ellul wrote this in 1954 when the police had no computers to be seen anywhere. The first experiments with computers were carried out by the police in the Netherlands in 1966, when they computerised the Identification Service (Stol, 1996), more than ten years after Ellul wrote his critical text. Ellul's work is very gloomy, his take on the police and technology is very dark. Just like Foucault, Ellul ascribes the police with substantial powers and, just like Foucault and Orwell for that matter, he concentrates on what the police are capable of doing with technology and how they can use it to observe and regulate the way citizens behave. But that's not the full story. The reality nowadays shows a different picture.

Today I have been talking about policing in cyberspace. When it comes to law enforcement in cyberspace the police are faced with a range of problems, such as processing an enormous amount of data from databases that have been confiscated and working on cases involving suspects operating from abroad. The biggest problem facing the police, however, is their lack of expertise. They do not know enough about the nature and extent of cybercrime, about the way perpetrators work, about who the perpetrators are, about victimhood, about the legal provisions regarding cybercrime, and, last but not least, they do not know enough about which measures are effective to combat the various kinds of cyber criminality. It is a familiar problem. I noticed it for the first time at the end of the 1990's in my own research (Stol et al., 1999) and things haven't changed much since then (PWC, 2001; Stol, 2003; LPDO, 2003; Van der Hulst & Neve, 2008; Toutenhoofd et al., 2009). This, incidentally, is not a typically Dutch problem (Griffiths, 2005). The police themselves know that they have a knowledge gap and are taking various steps to address this. There is the national police Programme for Combating Cybercrime (PAC) and, in connection with this, a number of initiatives are being explored to gain insight into the various aspects of cybercrime.

It should be noted here that the knowledge problems within the police force have various forms. There are experts working for the police force who are familiar with cyberspace and cybercrime. Here I have in mind, at a national level, the NPSA's cybercrime specialists in the field of high-tech crime and child pornography, and also the experts from the Digital Technology and Biometrics department of the Netherlands Forensic Institute (NFI). At a regional level, there are various digital detectives in various places who have sound knowledge of cybercrime and how to tackle it. Yet although these experts have specialist knowledge about cybercrime, they still do not know enough about it. I make this observation without apportioning blame. If blame is to be apportioned, then I am inclined to question why it is that politicians and researchers left this shortage of knowledge unattended for such a long time. I suspect that the answer to this is that no one has recognised properly how serious cyberspace has become as part of our everyday world. I also suspect that politicians and social scientists look upon these technological developments with too much humility.

This knowledge problem concerns not only those responsible for recording crimes and the average person at the counter but the whole police force, including experts and the various management levels – because it is the management that are expected to outline policy to do with cybercrime and currently they have to do this without proper information about the nature and extent of the matter.

Our police have considerably more technology to hand than the police in the Ministry of Love in *1984*. Modern computers, databases, tapping equipment, analysis and investigation tools, data logging devices and so on render the telescreens in *1984*, with which the police had to keep their citizens under control, to child's play. Yet we have to admit that our police are anything but in control. Citizens make use of the extra degree of freedom that technology, and cyberspace in particular, affords them (compare De Sola Pool, 1983) and expand their opportunities by doing so, as do criminals. The authorities are active too. More and more activities in cyberspace are being regulated in terms of the law and the police are being given more powers. But despite their technology and their powers, the police cannot keep up with developments and they do not have their citizens in their grasp. Cyberspace leads to an increase in unlawful acts. On balance, the authorities (the police) have lost control rather than gained control of citizens' behaviour.

Police with more information technology and greater powers at their disposal in a technological environment are frequently associated with the arrival of an Orwellian society. At the beginning of the 1990's, I researched the effect of new information technology on police officers on the beat. At the time, something revolutionary was afoot: for the first time ever, police officers stored all the information about citizens and addresses on a police computer that they could consult later, as though it was a huge police memory bank. Project leaders and police chiefs expected that this would result in a more vigorous police performance, particularly when called out to fights and disturbances. Those running amok – because their details were all on file now - would be confronted with police intervention and a police record, arrest and confiscation. During my time as a participatory observer on the streets, however, I didn't see a rise of more rigorous police interference with citizens – no glimpse of an Orwellian society (Stol, 1996). Today I see a police force wrestling with cyberspace and cybercrime. At the same time, I don't see a police force that knows how to turn the existing technology that they have at their disposal into more rigorous, or if you like, more vigorous or more effective police supervision; I don't see a police force that know how to employ these new tools so that they have a greater influence on the comings and goings of citizens. Why is it that the police in our society are not developing according to the expectations of Orwell (1934) and Ellul (1949), despite this wealth of modern technology?

2.8 Beyond Orwell: the theory of technological enforcement

Orwell was right in one respect: if it is possible for a police state such as the one he sketches to arise, then it is through a police apparatus with far-reaching powers and advanced information technology. You will say: if the police are so far behind in terms of knowledge, if they know so little about cybercrime, then it is no wonder that they do not know how to convert this new technology into more rigorous police actions, and it will never amount to anything. This gap in knowledge plays a part in the current situation but this is not a definitive and lasting impediment. Deficits can be dealt with. Expertise can be acquired or sub-contracted through collaborative efforts. The crux of Orwell's concept lies in the combination of intention and technology.

The intention of Orwell's government is to have total control of all citizens, everywhere and at all times. The authorities strive to eliminate individuality, to have total subordination to the state, so that people think and act as prescribed by 'the party'. The question of why the government would want this, I'll leave to one side. The vision of 'the state' as the only social entity, with citizens that are no more than uniform and powerless – and preferably without will – cogs in the wheel, is a vision that has been around for a long time thanks to Sir Thomas More, an Englishman who described in his novel, *Utopia*, in 1516 perhaps the archetype of this kind of society. The Utopians have everything they want, but they too are under the constant eye of a malevolent government that intervenes rigorously at the slightest departure from the norm (More, 1516). Utopia is therefore not a paradise but a nightmare, a vision that is more than four hundred years old. Information technology is the new element that Orwell emphasises centuries after More. That is what Orwell brings to the table. The more or less implicit message in his novel is that the authorities are now striving for total control and that information technology is the vehicle with which they may finally achieve this. Information technology may thus trigger an evil streak in the authorities. Information technology carries the promise of absolute knowledge about citizens, and with it absolute power – because power is knowledge and it generates more power, and so on. Information technology makes it possible for the authorities to expand into a fully-fledged control machine.

Whether authorities have essentially evil, machine-like intentions, I'll leave to one side. I am mainly concerned here with the principles of information technology and in particular how this translates to policing in cyberspace. In Orwellian terms, the question is: is more information technology in the hands of the state really the strategy for Big Brother? Regarding our own police and cyberspace, the question is: in order to take on the increase in cybercrime, do the police have to use more information technology, as Orwell suggests?

Now I have arrived at the point where my analysis deviates from Orwell's representation of the matter. The answer is: no, because authorities that wish to influence the way citizens behave should not start to employ information technology *themselves*, but should ensure first and foremost that the citizens they have in mind are the ones that employ it. This is where the theory of technological enforcement that I mentioned applies (Stol, 2004). This reads as follows: 'technology primarily regulates the behaviour of those who actually use it.'

This theory is based on various observations. The principle is actually old and was used at the beginning of the 20th century in the American vehicle industry. The first assembly line technology used in Henry Ford's factory tied the employees to their workplace and regulated their behaviour extensively. In this way, the management kept their hands, not only figuratively, but literally free (Pieterson, 1981).

In my research into police work and information technology (e.g., Stol, 1988, 1996; Stol & In 't Velt, 1991), the theme regarding behaviour regulation is that the comings and goings of police officers becomes more visible to their superior officers and that they have to align their behaviour to what the machine asks of them (information collection, inputting of data, and work speed) when they use a computer. Police computers regulate the behaviour of police officers themselves to a far greater extent than the behaviour of citizens. This effect is so obvious that police officers invariably complain about the pressure that the machines exert, particularly when recording a statement or documenting work that has been carried out. If we explore further, we see even more consequences for the comings and goings of people within the police organisation: computer users have to be trained, systems have to be developed, and new versions have to be implemented. Managers spend time in meetings about computerisation, every now and again politicians have to report on the state of affairs regarding police computerisation, and so on. All of this keeps the police busy.. The question remains: what effect does information technology have on the behaviour of citizens in general and criminals in particular?

Here is a finding from a different neck of the woods. In 2006 and 2007, the municipality of Leeuwarden carried out an experiment in the city centre using cameras to tackle nightlife related violence. The experiment had clearly observable effects on the behaviour of the government personnel involved. Police officers changed their surveillance patterns, they recorded work related incidents more often and they had to go through the camera recordings. Police chiefs had meetings about the project, at the municipality the various people responsible were constantly running around organising the camera surveillance and the town council had to be appraised of their activities. From the project evaluation, however, it was clear that those the cameras were focussed on hardly changed their behaviour at all. The goal of 'reducing violent crime' was not achieved at either location. The aim of 'increasing feelings of security' was achieved, albeit only among one of the four target groups – people on a night out. The question, however, remains whether this was as a result of camera surveillance or because of the increase in police surveillance that accompanied it (Kerstens et al., 2008).

My last example is about the combating of cybercrime. In 2007, the Dutch police started blocking websites containing pornographic images of children. The project was costly in terms of time for the detectives who had to filter the material, time that they would rather have used to track criminals. 'One of the detectives mentioned the disproportionate burden on the available capacity within the corps. "This experiment is somewhat out of control, in part because of the commotion surrounding it. We've taken a path and it seems as though there is no turning back, added to which it is not clear what the results will be"' (Stol et al., 2008: 128). The latter was confirmed by the project evaluation: it showed that there was insufficient reason to assume that this technical measure affected the behaviour of Internet users intent on searching the web for child pornography.

Technology primarily regulates the behaviour of those who actually use it, and only indirectly – if at all – the behaviour of others at whom the technology is directed. This is according to the theory of technological enforcement. There is evidence to suggest that a government that is concerned about safety in cyberspace should therefore avoid using the very same technology that they want to use to regulate people's behaviour in cyberspace in their attempts to enhance safety. The government would be better off encouraging citizens to use technology. Those who use information technology become more visible to their environment, sometimes directly and very literally, sometimes because they leave a digital trail in their wake. They do this when they use the Internet, discount cards, access cards, client cards, season train cards, credit cards, debit cards and mobile phones. People's movements can be fairly accurately reconstructed on the basis of this usage. The population has signed itself up for technology on a massive scale and report, on a voluntary basis, and several times a day, exactly where they are, what they are doing, with whom they've been in touch and which route they've taken. Twitterers take it a step further and give explicit accounts of what they're doing on a continual basis. Big Brother in *1984* couldn't have done a better job.

Citizens can also use technology to monitor one another informally. The police project *Kiezen of Helen* (a play on words for the saying 'take it or leave it') is an example of this. The aim is that citizens are given access to an Internet facility that allows then to check for themselves whether things offered for sale on cyberspace are registered as stolen. In an unrelated case, a police officer once told me about a proposed project regarding theft of consignments from trucks. The idea was that truck drivers could keep an eye on their vehicles through cameras mounted in parking places using their mobile phones. I never heard whether the project was implemented, but the police officer's way of thinking was refreshing: don't get involved with technology yourself, rather let the people concerned do it. The police too readily apply old reflexes: reaching for new technology to combat crime as the police force. The police still have to learn not to get involved themselves. They don’t have the capacity to solve the problem of criminality on their own, regardless of the technology at their disposal, and that applies to cyberspace as well.

The theory of technological enforcement puts the police onto a different track and warns them, as it were, against embracing technology too hastily and too ambitiously as a new instrument to tackle delinquent behaviour. There will always be exceptions, and on the basis of these, the theory can be fine-tuned.

With this theory in mind, what can we say, for example, about the ‘twittering officer on the beat’ – a phenomenon that recently made the news? ‘The Netherlands has about fifty of these officers. They are pioneers who see Twitter as a means to expand the accessibility of the police’ (*de Volkskrant*, August 24, 2010). My initial reaction when I read this report was: they are moving with the times, that’s a good thing. Moreover, it is good that the police experiment with what new technology can deliver. But it will have become clear that the theory of technological enforcement contains a warning against this initiative. The police are using new technology themselves. However, ‘being accessible’ is not a police task and should therefore not be a goal in itself. It is a means to an end. The goal is enforcing law and order. The question is how using twitter can contribute to this police task. It clearly impacts on the behaviour of the police officers involved and that their comings and goings become more visible. ‘So, time to relax. Watching football with Kasabian’s “Fire” blaring on the headphones. Wife giving disapproving looks’ according to one of the tweets (ibid.) Wasn’t the original idea behind police information technology that the police would gain more insight into the comings and goings of citizens? It seems as though the opposite is happening. According to the theory of technological enforcement, it should be citizens that are doing the twittering. Then local police officers will get more insight into their activities – instead of the other way round. I hope, nevertheless, that this twitter experiment continues and that the police check carefully how this new technology contributes to the enforcement of the law.

Obviously a good relationship with the public is a prerequisite for gathering information and for getting support when the police need it, for example, for solving cases or controlling public disorder in the neighbourhood. The benefits of this new way of working will reveal themselves over time; this is not a problem. Drawbacks arise when the police use new technology and fail to seriously evaluate how they contribute to their goals, something that happens too often for my liking.

My critical remarks are not intended as arguments for stopping the Twitter experiment. I applaud experiments involving new IT because the police need to find out what works and should not shun innovation. At the same time, I am a passionate advocate for effective evaluation. It involves a lot of work, but goals must be achieved.

Another novelty in the force is ‘Internet surveillance’. What does theory have to say about this? For Internet surveillance, police officers use technology to carry out surveillance in cyberspace. Whenever we see that officers are the ones using technology, caution is in order according to the theory. After all, it is the behaviour of agents that is being regulated and made more visible. This is not a goal but an investment. What advantages does it have? Internet surveillance is a tool that should be used sparingly, only if the police are searching for something very specific. I advocate avoiding the use of the term ‘Internet surveillance’. It sounds too much like unfocussed monitoring. Surveillance may be useful in the neighbourhood, in a shopping centre or in an entertainment area, but as things stand I can’t see surveillance in cyberspace as a useful way of employing police capacity

– unless they are specifically searching for an individual or information about a particular incident, in which case I would not call it Internet surveillance but an investigation.

The theory of technological enforcement points out that as soon as the police use technology, they must constantly ensure that they are not tying themselves down and thus do not have enough time to exercise their influence on the behaviour of citizens. Technology acts like syrup: if you touch it too much, you get stuck and bogged down. Your movement slows down, you get distracted by it, and it takes more and more effort to rid yourself of it. The citizen you're trying to find stays out of reach. This should be a strong warning to the police in cyberspace. Cyberspace is a world that can only be accessed through technology. How can you enforce the law in a world where you get bogged down as soon as you enter it?

As an aside, because I can hear someone thinking: why don't cyber criminals get bogged down? Cyber criminals run the same risk, and they know that. They are very familiar with the theory of technological enforcement, but in their circles it is the theory of technological crime. They have derived two strategies from this. Firstly, they make sure that they remain as invisible as possible, for example through false identities and cryptography (encryption). This is how they avoid becoming visible through their use of technology. Secondly, they themselves use technology as sparingly as possible: they let others do it, generally their victims and potential victims, but also their gullible sidekicks. This is how cyber criminals avoid becoming stuck behind the computer and addicted to it, or worse still, becoming visible. They let their victims download and activate viruses, they let their victims log onto false websites and enter their own information, they let their victims unwittingly transfer money, and so on. Together these two strategies form, as it were, a Teflon layer for cyber criminals.

Cyber criminals that do get stuck, because they get involved with technology too much, get noticed and picked up. Botnets are by all accounts a clever criminal strategy. (Botnets are networks of computers that criminals have command of without the owners knowing about it.) Criminals let others do the work on their computers while they stay in the background as much as possible – to avoid getting bogged down. The police have given priority to tackling botnets in the hope that, by doing so, they will scratch the criminal cyber Teflon layer.

Now I will return to the main theme of my argument. Citizens have signed up to technology en masse and voluntarily report their whereabouts, what they are doing, with who they are in contact and which route they have taken several times a day. They do so willingly. Twitterers take this a step further and continuously give an explicit report on their comings and goings. Orwell could never have predicted that citizens would voluntarily succumb to technology in this way. In his world, it is the authorities that get busy with technology, and get more control as they apply more technology. As you have just learnt, this is a mistaken assumption. The theory of technological enforcement maintains that you should not use technology yourself, you should hand it over to others! Let others work with it. Observe how the banks have mobilised us with technology. Witness how chain stores have seduced people with loyalty cards into handing over their personal information and revealing their purchasing habits. In short: the authorities should make good use of the fact that citizens love using technology.

They can do this in two ways. To start with, the authorities can supply citizens with information technology that they can use to help combat cybercrime. The police project '*Kiezen of Helen*', mentioned above, is an example of this. The idea behind this is that citizens are given software which they can use to establish whether second hand goods offered for sale online are stolen or not. This is the right line of thought.

The second way is that the police should analyse the digital tracks that criminals leave, should they have a suspect in their sights. Use the fact that they are linked to technology and as such have become visible. Perhaps it is possible to encourage suspects to use more technology and by doing so expose themselves even more – obviously within the limits of the law.

So much for police strategy. Another matter altogether is that the police cannot leave their organisation undisturbed.

2.9 The police organisation

I have the distinct impression that the police have not yet fully grasped the implications of digitalisation in our society. Once again, there are calls for a national police force because this would benefit the combating of organised crime. That may well be, but if the police want to be alert in their response to the digitalisation of society, it will require more than this, or a different response.

To start with it should be noted that it is not sufficient for the police to set up a special department or appoint experts. The digitalisation of society is not something that can be addressed by a department: it requires a total change and that requires reflecting on the whole police organisation. Digitalising is also not an issue that we should narrow down to cybercrime because that would mean that the police and justice department would approach the matter in terms of investigations and prosecutions. The crux of the matter is that the police should assess all their work processes and tools to see if they are sufficiently aligned with their current digital environment.

This means that the police are faced with two important organisational issues: firstly they have to ensure that they have sufficient knowledge and the right skills to be able to operate in the digital world, and secondly they have to divide tasks – or implement division of labour – and subsequently align the various sub-tasks so that an effective, unified whole is created. These two issues are of course linked, because if knowledge is unevenly distributed this will impact on how the tasks can be divided.[12] I will discuss a few specific aspects requiring attention.

To start at the beginning: police receive requests for help from the public or they take the initiative themselves. There may have been a fight or a crime may have been committed. Increasingly we see a link with cyberspace, regardless of the type of incident. The fight may be between neighbours, for example, and they have goes at each other, not only around the house, but also on Hyves and LinkedIn. The abuse is not only physical, it also involves pictures that have appeared on the Internet. Incidents that have no connection to the Internet are becoming rare – unless of course you pretend that this link doesn't or can't exist. It may be that the incident is directly connected with cyberspace – I've given you two examples – or that the police end up in cyberspace once they start dealing with the incident, for example when they start looking for background information, evidence or witnesses. If the police start an investigation on their own initiative, this may also happen, for example if they are tackling youth gangs, drug dealers, or some other criminal manifestation. For the same reasons, they cannot avoid cyberspace.

The police are therefore involved with cyberspace in all aspects of their work, provided they take their work seriously, that is. For this reason, cyberspace is not only a matter for digital detectives or other specialists. Every member of the police staff must be able to find his or her way

[12] I will not elaborate here on the necessity to have adequate equipment in place.

around in this new world. As I mentioned earlier, this is not the case at the moment, not by a long way.

Not every police member of staff requires the same kind of knowledge. Those who take down statements need a different kind of knowledge about cyberspace than detectives or officers on the beat. There is evidence of a serious shortfall in knowledge (compare Toutenhoofd et al., 2009). Reports with an element of cybercrime, for instance, are often handled inadequately. Staff registering the report often don't know what to do with the digital side of the case. An important organisation issue is how the police should get the right expertise, at the right time, in the right spot.

As far as this issue is concerned, the police have been following a path for a long time that, to my mind, is dubious. Several years ago, so-called infodesks were installed in the police force because the average detective could no longer be expected to search through the police computer systems available. In 1996, the police work group, Open Sources (*Open Bronnen*) of the criminal investigation department's improvement programme, Accacia, saw a report with an optimistic title *'What would you like to find out?'* (WOB, 1996) which offered the Internet as a source of information.

Over the years several positions have been created for people to help detectives who were searching for information, such as information desk staff, information analysts and open source experts. Detectives ask questions and others gather the information for them. This may sound useful, but it isn't always. There are various problems to do with communications between the people asking the questions and the information specialists – if these people actually find each other, because the thresholds can sometimes be high if the detectives and information desk staff don't know each other well (compare Van Treeck & Stol, 1996; 2000). Dealing with questions like 'Has this person got antecedents?' or 'Whose name is this car registered in?' generally goes well. These questions are specific enough. Where it often goes wrong is because of obstacles in a relational sense: surprisingly often, people don't get hold of each other, either because they don't want to bother each other or because they don't get on very well (e.g., Algemene Rekenkamer, 1998; Van Treeck & Stol, 2000; Leukfeldt, 2007). Open-ended questions such as 'What do we know about suspect X?', 'Who does Y hang out with?' and 'Which gang is involved in this?' are particularly difficult to deal with. Information staff can go on the Internet and come back with a CD full of information that the detective doesn't know what to do with. It seems that, through the years, the police have implemented a troublesome division of labour here, and now have to rethink how to approach the information side of detective work.

Obviously it is useful for detectives if information staffs help them to search for certain information, but this only works if the detectives take the lead in terms of searching and thinking things through. They have to have an overview of the world in which they are combating crime, and from there be able to pass on to support staff concrete questions that don't include too many sub-questions. What we see now is that detectives are complete strangers to cyberspace, they hand the searching over to others and subsequently have no idea what to do with the information they get back – because not only is there too much of it, it also originates in a world that they don't understand. I think that it is no exaggeration to speak of an erosion of the work of detectives. Division of labour has gone too far. It is as though police work can be compared to making pins, an example that Adam Smith used in 1776 (Smith, 1776) to demonstrate the advantages of division of labour: one makes the head, another makes the shaft and a third joins them together - *et voilà*: it is much faster than each person making their own individual pin in the traditional way. The difference is this: the police produce knowledge, and that it's a different kettle of fish to making pins or any other object that can roll off the assembly line.

I advocate for a revitalisation of the profession that I conveniently refer to here as 'the ordinary detective'. Detectives must be familiar with the world in which they are combating crime, and they must therefore also know their way around cyberspace. They can be assisted in this, but they must always be in charge of the search for information and deciding which direction that this search should take. In addition, they ought to be able to interpret the information that they find. These days it is no longer possible if they do not have sufficient insight into what is and is not possible in cyberspace. This may be a question of selection, and perhaps an issue of training. The question here, too, is: how can the police ensure they close the cyberspace related knowledge gap at the right time and place? Training in this field will have to be ongoing, flexible and fast, not too centralised or on a large scale, but focussed on specific needs and using *distance learning.*

The knowledge impulse that I am proposing is not without its limits. Police officers have to be familiar with cyberspace. They can also tap into knowledge from outside the organisation by working with experts from the business and academic worlds. This is not happening often enough. There are bound to be a lot of IT experts that are willing to help the police when it comes to issues of cyber safety. Here, too, we must differentiate between the specialist departments within the force and the force in the broadest sense, as an organisation. Specialists within the police are in contact with other experts; that is not the issue. Lack of knowledge is mainly found among the generalists: the officers on the ground and the general investigation departments. There are bound to be IT experts that would readily help the local police station with the digital aspects of its work. For this reason I am calling for a national Voluntary Policing in Cyberspace network. This network would not be a temporary solution but a new way of organising the force. For the foreseeable future, developments in cyberspace will be moving at such a pace that there will always be a need for new experts. This can be accomplished using a flexible concept of temporary relations.

In brief, the police will have to use several approaches to address the issues related to gaps in knowledge. Police officers need to know more about cyberspace, and the police should be able to draw on specialist knowledge easily. I have now arrived at the second organisational issue, where it seems that changes will impact more profoundly on the police organisational structure, where education, training and networks cannot provide an adequate solution.

The first issue is furnishing of proof in criminal cases. Make no mistake: it is not only the Digital Investigation department that is involved; this issue impacts on all work processes within the force. It involves information, the central control room, taking down of statements, work in the neighbourhoods, investigations, the Public Prosecution Service and the judiciary. Everyone involved in the legal chain needs to know how criminal evidence is presented in our modern digital world. Everyone must act accordingly and everyone must collaborate with other organisations and with citizens. And if the police know how they should be doing this, then they should also prove that they do. The core issue here is how digital evidence in criminal cases ought to be secured. The first sub-question is which evidence should be gathered, the second, how should this evidence be gathered and the third, by whom.

Research by the Cyber Safety Lectorate (Toutenhoofd et al., 2009) shows that, when cybercrimes are reported, police staff ask citizens to secure their digital evidence, like copies of e-mails or information about IP addresses. The question is whether it is the correct procedure to ask citizens to search out and secure evidence. In any event it is a fairly radical departure from normal police practice. In break-ins, for instance, it is not customary to ask citizens to search for and take finger print samples, or to look for footprints and make casts of them. Take note: the police have protocols that dictate the correct way to make plaster of Paris imprints and how to make a cast. But when it comes to cyberspace, police ask the citizens to muddle around, how else to describe it? I understand why they do it, because there is not instruction for dealing with it and staff at the counter are looking for the best way forward. Even a junior lawyer would know what to do with evidence gathered in this way. The organisational problem facing the police involves managing volumes. Cases with digital components are on the increase. Before long the police won't have the manpower to start digital tracking of all cases with a digital component, even if they had the necessary expertise and skill. This is an issue that the police and the Public Prosecution Services will have to address.

The second organisational issue that impacts on the organisation structure of the force is the internationalisation of criminality thanks to cyberspace. The problem is easy to predict. Minor cases of whatever nature ought to be reported to the nearest neighbourhood police post. Until recently, this involved cycle theft, abuse, muggings, break-ins, car theft, fights between neighbours, unruly youths, and so on. Rarely, if ever, did officers at the counter have to deal with cases that had a foreign element. If a case had an international aspect to it, then it was handed over to a special team. Working on an international case was not part of an average neighbourhood cop's job. Recent studies show that 23.3% of all hacking cases (N = 60) the suspect was operating from abroad, and in e-fraud cases, that percentage was 14.5 (N = 166). The average for the two offences is 16.8%, i.e., one out of six. It is not difficult to predict that the police will have to deal with a rapidly growing number of cases with an international character. They need not necessarily be serious cases: they could involve small time criminals, operating on their own, from Finland or Portugal, who use everyday fraud to earn a bit of money on the side, and are clever enough not to seek victims in their own country. The police and justice department don't have an answer yet to such internationally operating small time criminals that, together, form a growing volume of 'common international crime', or 'international minor crime', if you will. In connection with this, we will come across internationally operating frequent offenders and international revolving door criminals. There will have to be new international collaborations and procedures implemented to tackle all these new cases of common minor offences with an international element.

Of course there are also cyber criminals who operate internationally, and in an organised way. The police and justice department will have to deal with them too. This is already the case, for instance, the NPSA's Team High Tech Crime. Organised crime has been the impetus for many years for the police to scale up her operations, witness the recent return of discussions about a national police force. The developments are following the familiar lines of scaling up and international treaties. What is new for the police is the just mentioned common minor international crime. This calls for the development of a new modus operandi because the system for combating international crime will otherwise be overloaded. I have mentioned three assignments confronting the police:

- reorganise acquisition of expertise: increase it and make it more flexible;
- organise the securing of evidence upon reporting of crime with a cyber-element, because everything the police tackle depends on a good start;
- develop systems to combat common small-scale international crime.

How this should all be done will require research. One thing is clear to me: bureaucracy as an organisational concept falls short. Bureaucracy as an organisational form is particularly strong in a stable environment. Time and again the same problems can be solved using standard actions and entrenched procedures. But for the police there is no such thing as a stable environment in cyberspace. This environment calls for flexibility, speed, and creativity, and is therefore better suited to organisational procedures that use collaboration in the form of constantly changing networks. According to the police specialists I've spoken to, the criminals discovered this long ago. They use this principle on Internet forums, to forge coalitions of convenience with other criminals, and to combine effectively the knowledge and skills required to carry out their plans.

The other thing that won't work in the changes that are required is a top-down approach. The police cannot avoid change; that much is clear. Cyberspace and cybercrime are forcing themselves upon us. With its national Programme for Combating Cybercrime, the police have designed an organisation that is prepared for change. The big question is how an advance group like this can spread its ideas within the organisation. This will fail entirely if it is done using a top-down approach and official policy regulations. The approach should be horizontal, via networks on the work floor. It is not a sinecure for change in a large organisation (compare Homan 2005, 2006) – particularly when so little is known about the phenomenon that is forcing the organisation to adapt.

You will by now have noticed that the thread running through my argument is a shortage of knowledge. This shortage has many consequences, big and small, and one of these consequences is that I stand before you today. It may be the intention of those in the legal chain to address this shortage of knowledge, to find out more about what is going on in cyberspace, but to do this there has to be knowledge! In a considerable number of cases there is someone who has this knowledge and can help, but in a shocking number of cases, we are empty handed. For instance, we still have no idea how many cases of victimization there are nationally. We have no idea how often citizens and businesses fall victim to cybercrime. We know very little about the perpetrators. We don't know how to effectively prevent or predict the youth from going off the rails in cyberspace. We don't know what to do with the research finding that almost a quarter of those suspected of spreading child pornography are under the age of 25 (8.3% are in the 12 to 17 age group and 15.5% in the 17 to 24 age group). We know little about how internationally organised cybercrime works, and so on. We are even further away from finding explanations. In short, this is a job for academia, a research assignment.

2.10 Research

I will contribute to this research assignment from my endowed chair. I essentially differentiate three kinds of research questions (Stol et al., 2000): 'what' questions, 'why' questions and 'how' questions.[13] I will describe these three briefly.

In large research projects, 'what' questions are often the first part of the study, and then the research goes on to find an explanation, and often a solution too. From a purely scientific point of view, being involved with 'what' questions alone is of limited interest. It is the format for looking for

[13] Elsewhere I mention four (Stol et al., 2000), but here I classify 'difference questions' under 'what questions' because both cases involve descriptive research.

explanations and solutions. In our field, we are dealing with unbroken ground. There are many 'what' questions requiring an answer. Even if we would rather see explanations and solutions, we can't skip the first step. It involves descriptive research that will throw light on the question of what is going on in cyberspace. What kinds of threats are there in cyberspace? How often do citizens and business have to contend with the various kinds of insecurity? How often are people and businesses victims or perpetrators when it comes to cybercrime? Who are these victims and perpetrators? How do perpetrators go about their business? What does organised cybercrime entail? What are the police doing in cyberspace? How does the legal chain function in cybercrime cases? What differences are there between the various countries? There is much to be done. An example of a study that my research group has conducted is *Verkenning cybercrime in Nederland 2009* [*Investigating cybercrime in the Netherlands 2009*] (Leukfeldt et a., 2010). It sketches the various kinds of cybercrimes, partly on the basis of police files. At the moment we are working on a nationwide study of cybercrime victimization among citizens, on research into the flow of police reports about cybercrime through the criminal law process and, together with Bureau Beke, on research into the illegal trade in cultural goods in cyberspace.

'Why' questions are more difficult. Our task is to find explanations for the things we observe. Why is it more often than not young people that spew hate speech in cyberspace? Why does a seventeen year old girl log onto a profile site for 40 hours a week, for three years in a row? Why don't citizens report cybercrime in so many of the cases? Why do most reported cases fail to lead to a conviction? Why are women the ones who are so active when it comes to e-fraud? And so on. These sorts of questions call for theories. Theories are merely an attempt to describe what it is that is at the basis of the things that explain the regularities of our society (compare Giddens, 1989). In other words: if we use observed regularities as our point of departure – for example 'noticeably often, e-fraud offenders are female', then the theory aims at describing the underlying causes, in this case to describe what it is that explains why a considerably number of these perpetrators are women. Theory is not an abstract toy for academics but an instrument for people who want to understand the everyday world around them. Why is this? What processes are they based on? How does it work? (compare Akers & Sellers, 2009). Plans of action can be derived from theories.

Theory plays a role in my research in two ways. Given my background with the police force, it will not surprise you that I often start with day-to-day things, with empirical observations on the basis of questions that stem from a curiosity about policing in cyberspace, such as 'Who are the victims of cybercrime?' or 'What tracking methods do the police use in cyberspace?' Empirical observations require explanations, a search for a theory that can help clarify the findings. This could be an existing theory or a new theory, such as the theory of technological enforcement that I spoke about earlier. This reflects an inductive scientific approach which entails starting with observations and using these to find general principles. That is theory-forming research. The second role that theory plays is that it can serve as a basis from which to do research – this is called theory driven or hypothesis testing research. This reflects a deductive scientific approach. The departure point here is theory: observations are done to test whether the theory is upheld or needs to be modified.

The field of police studies moving through cyberspace is a peculiar state of affairs. All established theory about policing, youth, disturbances and crime, for example, has been developed in a world without cyberspace. The question that arises is this: is the theory correct when it comes to what is happening in cyberspace? Is the theory that has been developed in the old world robust and will it hold true? Can the old offline theory help us to explain what is going on in the online world? Can policy measures still be based on established theories? Or are other principles at play? We don’t know. This is the challenge for the academics.

After ‘why’ questions, ‘how’ questions are the last ones in the range. These are also known as effect questions. The focus here is on the way in which specific problems can be tackled: what methods are effective. Measures are aimed at sorting the various types of effects, for instance: the government uses information to encourage people to be careful with their passwords and other personal information, which is intended to contribute to lowering the risk of victimization. The police are given new powers in cyberspace and the question is whether these are used and, if so, to what effect. Police staff are supported in recording cybercrime reports and the question is whether this will lead to greater satisfaction among those reporting crimes and to more convictions. The police implement a national reporting centre for Internet related fraud and the question is whether this will lead to more cases being solved and a reduction in e-fraud. Obviously this kind of evaluation research always has a ‘why’ component. We want to be able to understand the findings for the benefit of future measures. An example of an effect study conducted by my group was *Filteren van kinderporno op Internet* [Filtering child pornography on the Internet] (Stol et al., 2008), which we did together with the VU University in Amsterdam. This research was about what is and is not possible regarding the filtering and blocking of websites that contain child pornography material, and the methods initially chosen by the police to do so. The conclusion was that the approach chosen in the Netherlands at the time had no basis in law, that it was not clear whether the approach was effective and that it cost the police heavily in terms of administrative work, which was not the intention. The Minister of Justice modified policies and since then the police are looking for more effective solutions.

The research programme under the auspices of my professorship focuses on all three types of questions. Initially, the emphasis is on ‘what’ questions because much remains unknown and policy concerning cyber safety needs knowledge of the facts as a foundation. The emphasis will gradually move to the ‘why’ questions because the job of science is to help us understand reality. Wherever possible, the programme includes ‘how’ or effect questions. The programme is based on three themes:

- *Trends in cybercrime*. This focuses on the nature and extent of cyber criminality, on perpetrator and victim characteristics, on the modi operandus of criminals and the techniques they use. It also involves the police approach to cybercrime and the way the legal chain operates.
- *Youth and cyber safety*. This involves four security issues: cyber bullying, unsolicited communication of a sexual nature, crime involving the youth as victims or perpetrators and excessive Internet usage. It involves the question of how problems can be prevented or, if prevention fails, how they can be recognised in the early stages.
- *Businesses and cyber safety*. This theme involves victimization of businesses and the question of which measures are effective against cyber criminals in this regard.

All three of these aspects involve ‘what’ questions, ‘why’ questions and effect questions. This is how I arrived at the work that has to be done. Fortunately I am not alone in this.

2.11 Acknowledgements

I would like to start by thanking the Boards of Governors of both the Open University and the NHL University of Applied Science in particular for the trust they have placed in me by appointing me extraordinary professor of Police Studies – relating specifically to cyber safety issues. It is a sign of courage to establish an endowed chair related to such unknown territory. I would also like to thank the Board of Governors of the Police Academy for the structural cooperation that has developed around the cyber safety theme. The Cyber Safety Lectorate is going to be the joint lectorate of the NHL Applied University and the Police Academy. With this, a long-standing wish will be fulfilled, creating a network in which the NHL University, the Open University and the Police Academy join their forces.

Ultimately, cooperation at organisational level comprises the working relationships between people. From this position I would like to thank my new OU colleagues for their hearty welcome to the south of the country and for the cooperation that is already in full swing. I would particularly like to thank Herman van de Bosch and Arno Korsten for their enthusiastic contribution to establishing the chair, and Thijs Homan because his instant and welcoming reception of the Cyber Safety theme into this capacity group demonstrates that he not only knows a lot about innovation and change as an academic, but also that he can find space for new things in a practical sense.

I cannot emphasise enough how great the group of people are that I work with every day. First and foremost I am referring to the people involved with the Cyber Safety Lectorate, both the researchers and other colleagues. I also include my colleagues at the Open University and the Police Academy, and I count myself lucky that we have such a flexible working relationship that crosses the boundaries of these organisations. Because, even though we do sometimes live in cyberspace, society is and remains an undertaking dependent on people.

I have spoken.

References

Akers, R.L. & C.S. Sellers (2009). *Criminological Theories.* New York: Oxford -University Press.

Algemene Rekenkamer (1998). *Uitwisseling van rechercheinformatie tussen CRI en -politieregio's* [Exchange of detective information between CRI and the regional police]. Den Haag: Sdu.

Becker, H.S. (1963). *Outsiders. Studies in the Sociology of Deviance.* New York: The Free Press.

Berger, P. & T. Luckman (1987, oorspr. 1966). *The social construction of reality.* -Harmondsworth: Penguin Books.

Bittner, E. (1967). Police discretion in emergency apprehension of mentally ill persons. *Social problems*, *14*, 278-292.

Blauw Research (2010). *Online thuiswinkelen in Nederland. Essential Facts* [Online home shopping in the Netherlands. Essential Facts]. -Rotterdam: Blauw Research.

Boerman, F., M. Grapendaal & A. Sey (2008). *Nationaal dreigingsbeeld 2008. -Georganiseerde criminaliteit* [National Threat Assessment 2008. Organised Crime]. Zoetermeer: KLPD.

Bunt, H.G. van de & J. Rademaker (1992). *Recherchewerk in de praktijk. Een casestudy naar recherche en informatievoorziening.* Lochem: Van den Brink.

Cachet, A. (1990). *Politie en sociale controle* [The police and social control]. Arnhem: Gouda Quint.

Cachet, A. & P. Versteegh (2007). Politie en samenleving [The police and society]. In C.J.C.F. Fijnaut, E.R. Muller, U. Rosenthal & E.J. van der Torre (red.), *Politie. Studies over haar -werking en organisatie* [The police. Studies about their operating procedures and organisation] (pp. 1043-1078). Deventer: Kluwer.

Calhoun, C, J. Gerteis, J. Moody, S. Pfaff & I. Virk (Eds.) (2007). *Contemporary -sociological theory. Second edition.* Oxford: Blackwell.

CBS (2010). *Integrale veiligheidsmonitor 2009. Tabellenrapport* [Integral Security Monitor 2009. Report Tables]. Den Haag/Heerlen: CBS.

DNR (Dienst Nationale Recherche) (2010). *High Tech Crime. Criminaliteitsbeeld-analyse 2009* [High Tech Crime. Criminality assessment analysis 2009]. Driebergen: KLPD.

Domenie, M.M.L., E.R. Leukfeldt, M.H. Toutenhoofd & W.Ph. Stol (2009). *Werkaanbod cybercrime bij de politie* [The police force's cybercrime related workload]. Leeuwarden: NHL Hogeschool.

Elias, N. (1984, oorspr. 1939) (twee delen). *Het civilisatieproces* [The process of civilisation]. Utrecht/Antwerpen: Het Spectrum.

Ellul, J. (1964, oorspr. 1954). *The technological society.* New York: Vintage Books.

Feest, J. & E. Blankenburg (1972). *Die Definitionsmacht der Polizei.* Düsseldorf: -Bertelsmann Universitätsverlag.

Ferwerda, H. (2008). Theorie over criminaliteit [Criminality theories]. In W.Ph. Stol & A.Ph. van Wijk, -*Inleiding criminaliteit en opsporing* [Introduction to criminality and investigation] (pp. 23-35). Den Haag: Boom Juridische uit-gevers.

Finstad, L. (2003). *Politiblikket.* Oslo: Pax Forlag.

Foucault, M. (1979, oorspr. 1975). *Discipline and punish.* New York: Vintage Books.

Foucault, M. (1985). *Ervaring en waarheid* [Experience and truth]. Nijmegen: Te Elfder Ure.

Fukuyama, F. (2002). *De nieuwe mens: onze wereld na de biotechnologische revolutie* [The new human: our world after the biotechnological revolution]. Amsterdam/Antwerpen: Contact.

Giddens, A. (1984). *The constitution of society.* Cambridge: Polity Press.

Giddens, A. (1989). *Sociology.* Cambridge: Polity Press.

Giddens, A. (1993). Structuralism, Post-structuralism and the Production of Culture. In A. Giddens & J. Turner (Eds.), *Social Theory Today* (pp. 195-223). Cambridge: Polity Press.

Govcert (2009). *Trendrapport 2009. Inzicht in cybercrime: trends en cijfers* [Trend report 2009. Insights into cybercrime: trends and figures]. Den Haag: Koninklijke Broese en Peereboom.

Griffith, R.E. (2005). How Criminal Justice Agencies Use The Internet. In A. -Pattavina (Ed.), *Information Technology and the Criminal Justice System* (pp. 59-77). Thousand Oaks: Sage.

Haraway, D. (1994, oorspr. 1991). *Een cyborg manifest* [A cyborg manifest]. Amsterdam: De Balie.

Heijder, A. (1989). *Management van de politiefunctie* [Managing the police function]. Lochem/Arnhem: Van den Brink en Gouda Quint; oratie, Vrije Universiteit Amsterdam.

Hesseling, R. (1994). *Stoppen of verplaatsen? Een literatuurstudie over gelegenheids-beperkende preventie en verplaatsing van criminaliteit* [Stop it or shift it? A study of the literature about preventing opportunistic crime and transferring criminality]. Arnhem: Gouda Quint.

Hirschi, T. (1969). *Causes of delinquency.* Los Angeles: University of California Press.

Holtackers, M. (2007). Theorieën over jeugdcriminaliteit: relevant voor de politiepraktijk? In A.Ph. van Wijk & E.J.A. Bervoets, *Politie en jeugd: een inleiding voor de praktijk* [Police and the youth: an introduction to practical policing] (pp. 23-38). Den Haag: Elsevier.

Homan, Th.H. (2005). *Organisatiedynamica. Theorie en praktijk van organisatie-verandering* [Organisation dynamics. Theory and practice of organisational change]. Den Haag: Sdu.

Homan, Th.H. (2006). *Wolkenridders. Over de binnenkant van organisatieverandering* [Opinion formers. On the inside of organisational change]. Heerlen: OUNL.

Hoogenboom, A.B. (1994). *Het politiecomplex* [The police complex]. Arnhem: Gouda Quint.

Hulst, R.C. van der & R. Neve (2008). *High-tech crime. Inventarisatie van literatuur over soorten criminaliteit en hun daders* [High-tech crime. Inventory of literature on types of crime and their perpectrators]. Den Haag: WODC.

Huxley, A. (1986, oorspr. 1932). *Heerlijke nieuwe wereld* [Brave new world]. Amsterdam: Bert Bakker.

In 't Velt, C.J.E. (1991). *Onder ons gezegd en geschreven. Een cultuuronderzoek naar informatie-gebruik in een Amsterdamse politiedienstgroep.* Amsterdam: Vrije Universiteit.

In 't Velt, C.J.E. (1996). Het oplossen van diefstaldelicten. *Tijdschrift voor de politie*, *58*(3), 6-10.

In 't Velt, C.J.E. (1999). *Politie en omgevingsanalyse. De rol van computerbestanden bij het oplossen van diefstallen.* Den Haag: Elsevier Bedrijfsinformatie.

Kerstens, J., M. Toutenhoofd & W.Ph. Stol (2008). *Wie niet weg is, is gezien. Geval-studie over een proef met cameratoezicht in de Leeuwarder binnenstad* [Hide and seek. Case study of an experiment . Den Haag: Boom Juridische uitgevers.

KLPD (2010a). *High tech crime; criminaliteitsbeeldanalyse 2009.* Driebergen: DNR.

KLPD (2010b). *Overall beeld Aandachtsgebieden.* Driebergen: KLPD.

Leukfeldt, E.R. (2007). *Onder de loep. Een observatieonderzoek naar recherchewerk en informatiegebruik.* Leeuwarden: NHL Hogeschool.

Leukfeldt, E.R., M.M.L. Domenie & W.Ph. Stol (2010). *Verkenning cybercrime in Nederland 2009.* Den Haag: Boom Juridische uitgevers.

Leukfeldt, E.R. (2010). *The E-fraudster. A Criminological Perspective.* Leicester: -University of Leicester.

LPDO (Landelijk Project Digitaal Rechercheren) (2003). *Visie op digitaal opsporen.* Zoetermeer: LPDO.

Lyon, D. (1994). *The electronic eye, the rise of surveillance society.* Cambridge: Polity Press.

Marcuse, H. (1964). *One Dimensional Man.* Boston: Beacon Press.

Merton, R.K. (1968). *Social Theory and Social Structure.* New York: The Free Press.

Mills, C.W. (1983, oorspr. 1959). *The sociological imagination.* Harmondsworth, -Penguin Books.

Moerland, H. & B. Rovers (2000). *Criminaliteitsanalyse in Nederland.* Den Haag: Elsevier.

Moerland, H. & F. Boerman (2003). *De praktijk van de criminaliteitsanalyse.* Den Haag: Elsevier.

More, T. (1987, oorspr. 1516). *Utopia.* Harmondsworth: Penguin Books.

Mumford, L. (1963, oorspr. 1934). *Technics and civilization.* New York: Harcourt Brace Jovanovich.

Orwell, G. (1989, oorspr. 1949). *Nineteen eighty-four*. Harmondsworth: Penguin Books.

Panhuis, P. van (2008). Informatiegestuurde politie en criminaliteitsanalyse. In W.Ph. Stol & A.Ph. van Wijk, *Inleiding criminaliteit en opsporing* (pp. 221-235). Den Haag: Boom Juridische uitgevers.

PEO (Parlementaire Enquêtecommissie Opsporingsmethoden) (1996). *Inzake Opsporing.* Den Haag: Sdu.

Pieterson, M. (red.) (1981). *Het technisch labyrint*. Meppel: Boom.

PWC (Profit for the Worlds Children) (2001). *Kinderpornografie en Internet in Nederland. Een overzicht van de huidige situatie, knelpunten in de bestrijding, suggesties voor verbeteringen.* Haarlem: PWC.

Ruth, E. van (2008). Daderprofilering. In W.Ph. Stol & A.Ph. van Wijk, *Inleiding criminaliteit en opsporing* (pp. 237-250). Den Haag: Boom Juridische uitgevers.

Smith, A. (1987, oorspr. 1776). *The Wealth of Nations.* Middlesex: Penguin Books.

Sola Pool, I. de (1983). *Technologies of freedom.* Cambridge: The Belknap Press of -Harvard University Press.

Steden, R. van (2007). *Privatizing Policing.* Den Haag: Boom Juridische uitgevers.

Stol, W.Ph. (1988). *Automatisering bij de politie: meldkamerwerk en kwaliteit van de arbeid.* Amsterdam: Gemeentepolitie Amsterdam.

Stol, W.Ph. & C.J.E. In 't Velt (1991). Politie en informatietechnologie. Veranderingen in politieoptreden? *Tijdschrift voor criminologie*, *33*(3), 256-278.

Stol, W.Ph. (1994). *Beelden van politiestraatwerk uit observaties in Europa en Amerika: hun inhoud en betekenis.* Dordrecht/Amsterdam: SMP/VU.

Stol, W.Ph. (1996). *Politie-optreden en informatietechnologie. Over sociale controle van politiemensen*. Lelystad: Koninklijke Vermande.

Stol, W.Ph., R.J. van Treeck & A.E.B.M. van der Ven (1999). *Criminaliteit in cyberspace. Een praktijkonderzoek naar aard, ernst en aanpak in Nederland.* Den Haag: Elsevier.

Stol, W.Ph., C.J.E. In 't Velt & R.J. van Treeck (2000). *Praktijkboek politieonderzoek.* Den Haag: Elsevier.

Stol, W.Ph. (2003). Sociale controle en technologie. De casus politie en kinderporno op het internet. *Amsterdams Sociologisch Tijdschrift*, *30*(1/2), 162-182.

Stol, W.Ph. (2004). *Handhaven: eerst kiezen, dan doen. Technische mogelijkheden en beperkingen.* Den Haag: Ministerie van Justitie.

Stol, W.Ph., A.Ph. van Wijk, G. Vogel, B. Foederer & L. van Heel (2006). *Police -Patrol Work in The Netherlands. An observational study in an international perspective.* -Frankfurt: Verlag für Polizeiwissenschaft.

Stol, W.Ph. (2007). Informatie voor politiewerk: basisprincipes. In C.J.C.F. Fijnaut, E.R Muller, U. Rosenthal & E.J. van der Torre, *Politie, studies over haar werking en organisatie* (pp. 381-398). Deventer: Kluwer.

Stol, W.Ph., H.W.K. Kaspersen, J. Kerstens, E.R. Leukfeldt & A.R. Lodder (2008). *Filteren van kinderporno op internet.* Den Haag: Boom Juridische uitgevers.

Stol, W.Ph. (2010). Filteren van internet: een politietaak? *Orde van de dag*, *49*(1), -43-49.

Tex, C. den (2008). *Cel*. Breda: De Geus.

Tienstra, J. (2008). *Cybercrime haatzaaien.* Leeuwarden: NHL Hogeschool.

Torre, E.J. van der & W.Ph. Stol (2000). *Waardevolle politieverhalen. Politie en Marokkaanse jongeren.* Den Haag: Elsevier.

Toutenhoofd, M.H., S. Veenstra, M.M.L. Domenie, E.R. Leukfeldt & W.Ph. Stol (2009). *Politie en cybercrime. Een onderzoek naar de intake van het werkaanbod cybercrime door de politie.* Leeuwarden: NHL Hogeschool.

Treeck, R.J. van & W.Ph. Stol (1996). *Naar de HKD nieuwe stijl. Evaluatie van drie pilots.* Utrecht: In-pact.

Treeck, R.J. van & W.Ph. Stol (2000). *Infodesks bij de politie en hun bijdrage aan -recherchewerk.* Houten: In-pact.

Vaart, W. van der (1996). *Inquiring into the past. Data quality of responses to retrospective questions.* Amsterdam: Vrije Universiteit.

Veenstra, S., J. Kerstens & W. Stol (2009). Cyberpesten: wangedrag in cyberspace en gedragsverklarende theorie. *Panopticon, 30*(4), 77-81.

Weber, M. (1990, oorspr. 1922). *Wirtschaft und Gesellschaft.* Tübingen: J.C.B. Mohr (Paul Siebeck).

Wilsem, J. van (2010a). Digitale en traditionele bedreiging vergeleken. Een studie naar risicofactoren van slachtofferschap. *Tijdschrift voor criminologie, 52*(1), 73-87.

Wilsem, J. van (2010b). Gekocht maar niet gekregen. Slachtofferschap van online oplichting nader onderzocht. *Tijdschrift voor Veiligheid, 9*(4), 15-29*.*

Wilterdink, N. & B. van Heerikhuizen (1993). *Samenlevingen.* Groningen: Wolters-Noordhoff.

WOB (Werkgroep Open Bronnen) (1996). *Wat wil je weten? Eindrapportage werkgroep open bronnen.* Rotterdam: Werkgroep Open Bronnen.

Appendix 1
Sections of law pertaining to the obligation to retain traffic data

Section 13.2a Telecommunications Act
1. The following definitions apply in this section:
a. *data*: the traffic and location information as intended by article 11.1, subsection b and d respectively, as well as information related to these that is necessary to identify a subscriber or user;
b. *attempt to call without a result*: communication whereby the phone call does connect but remains unanswered or is answered by the network management system.
2. the providers of public telecommunications networks or public telecommunications services will store the data designated in the appendix belonging this Act, insofar as they are generated or processed as part of the network or services provided, as required for research, investigations, or prosecutions of serious crimes.
3. The data referred to in the subsection 2 will be stored by the providers for a period of twelve months calculated from the date of communication.
4. The obligation referred to in the subsection 2 relates to data from attempts to call without a result, insofar as these data are generated, processed and stored or logged by the providers in providing public telecommunications networks or public telecommunications services.

Section 13.4 communications Act
1. Providers of public telecommunications networks or public telecommunications services will comply immediately with a claim on the grounds of article 126n or article 126na, or article 126u or article 126ua of the Code of Criminal Procedure or on request on the grounds of section 28 of the Intelligence and Security Services Act 2002 for the provision of data about a user of a public telecommunications network or a public telecommunications service relating to that user.
2. Providers of public telecommunications network and public telecommunications services will comply immediately with a claim on the grounds of article 126na(1), article 126ua(1), or 126zi of the Code of Criminal Procedure or requisitions on the grounds of article 29 of the Intelligence and Security Services Act 2002 to provide data relating to the name, address, postcode, place of residence, number and type of service of a user of public telecommunications network or a public telecommunications service.
3. Providers of public telecommunications network and public telecommunications services will comply with a claim on the grounds of article 126na(2), 126ua(2) or 126zi of the Code of Criminal Procedure or requisitions on the grounds of article 29 of the Intelligence and Security Services Act 2002 to retrieve and provide the data referred to in subsection 1 in a manner to be determined by an order in council. In order to be able to comply obligations, the providers will store data in a manner to be determined by an order in council for period of twelve months starting on the date that the data were processed for the first time.
4. On the recommendation of Our Minister of Justice, Our Minister, Our Minister of the Interior and Kingdom Relations and Our Minister of Defence, regulations can be laid down by an order in council regarding the way in which providers will comply with a claim or a requisition, as referred to in subsections (1), (2) and (3), the registration of statistical data and the periods within which those data will be made available and the way in which the information as referred to in subsections (1), (2) and (3) will be held available. The recommendations for an order in council to be established

pursuant to the first sentence will not be made earlier than four weeks after the draft has been presented to both the Houses of the States General.

Article 126n Code of Criminal Procedure
1. In cases where a crime is suspected as defined in article 67(1), the public prosecutor can, in the interests of the investigation, requisition data about a user of a communications service and the communication traffic relating to that user. The requisition can only relate to data designated by the order in council and can concern data that:
a. had been processed at the time of the requisition, or
b. were processed after the time of the requisition.
2. The requisition referred to in paragraph (1) can be addressed to any provider of a communications service. Article 96a(3) applies *mutatis mutandis*.
3. If the requisition concerns data as mentioned in paragraph (1), second sentence under b, the requisition will relate to a period of at most 3 months.
4. The public prosecutor will draw up a record of the requisition, mentioning the following:
a. the crime and, if known, the name or otherwise and as accurate as possible a description of the suspect;
b. the facts or circumstances that show that the conditions referred to in paragraph (1), first sentence, have been met;
c. the name or otherwise and as accurate as possible a description of the person about whom the data is requisitioned, if known;
d. the requisitioned data;
e. the period covered by the requisition, if it concerns data as referred to in paragraph (1), second sentence under (b).
5. If the request concerns data as referred to in paragraph (1), second sentence under b, the requisition will be terminated as soon as it no longer meets the conditions as mentioned in paragraph (1), first sentence. The public prosecutor will draw up a record of any amendment, addition, extension or termination of the requisition.
6. By or pursuant to an order in council, regulations can be laid down relating to the manner in which data are requisitioned by the public prosecutor.

Article 126na Code of Criminal Procedure
1. In cases where a crime is suspected, the investigating officer can, in the interests of the investigation, requisition data relating to the name, address, postcode, place of residence, number and type of service of a user of a communications service. Article 126n(2) applies *mutatis mutandis*.
2. If the data referred to in paragraph (1) are not known to the provider and they are required for the application of article 126m or article 126n, the public prosecutor can, in the interests of the investigation, demand that the provider retrieve and provide the requisitioned data in a manner to be determined by an order in council.
3. In case of a requisition as referred to in paragraph (1) or paragraph (2), article 126n(4) under a, b, c, and d, applies *mutatis mutandis* and article 126bb does not apply.
4. By or pursuant to an order in council, regulations can be laid down relating to the manner in which data are requisitioned by the investigating officer or the public prosecutor.

Article 126u Code of Criminal Procedure
1. In a case as referred to in article 126o(1), the public prosecutor can, in the interests of the investigation, requisition data about a user of a communications service within the meaning of article 126la and communication traffic relating to that user. The requisition can only relate to data indicated by the order in council and can concern data that:
a. had been processed at the time of the requisition, or
b. were processed after the time of the requisition.

2. The requisition referred to in paragraph (1) can be addressed to any provider of a communications service. Article 96a(3) applies *mutatis mutandis*.
3. If the request pertains to data as mentioned in subsection (1), the second sentence under b, the request will relate to a period of at most 3 months.
4. The public prosecutor will make a written report of the request, mentioning the following:
a. a description of the organised relationship;
b. the facts or circumstances that show that the conditions referred to in (1), first sentence, have been met;
c. if known, the name or otherwise an as accurate as possible description of the person about whom the data is requested;
d. the data requested;
e. if the data requested relates to that referred to in subsection (1), second sentence under b, the period covered by the request.
5. If the request pertains to data as referred to in subsection (1), second sentence under b, the request will be terminated as soon as it no longer meets the conditions as mentioned in subsection (1), first sentence. The public prosecutor will prepare a written report for changes, additions, extension or termination of the request.
6. By or pursuant to an order in council, regulations can be laid down to determine the manner in which data are requested by the public prosecutor.

Article 126ua Code of Criminal Procedure (see above corrections for this article).
1. In cases as referred to in article 126o(1), the investigating officer can, in the interests of the investigation, request data relating to the name, address, postcode, place of residence, number and type of service of a user of a communications service. Article 126u(2) applies *mutatis mutandis*.
2. If the data referred to in subsection (1) are not known to the provider and they are required for the application of article 126t or article 126u, the public prosecutor can, in the interests of the investigation, request that the provider retrieve and provide the requested data in a manner to be determined by an order in council.
3. In case of a request as referred to in subsection (1) or subsection (2), article 126u(4) under a, b, c, and d, apply *mutatis mutandis* and article 126bb does not apply.
4. By or pursuant to an order in council, regulations can be laid down to determine the manner in which data are requested by the investigating officer or the public prosecutor.

Article 126zi Code of Criminal Procedure (see above corrections for this article)
1. If there are indications of a terrorist crime the investigating officer can, in the interest of the investigation, request data relating to the name, address, postcode, residence, number and type of service of a user of a communications service as referred to in article 126la. Article 126n(2) and (3) apply *mutatis mutandis*.
2. If the information referred to in subsection (1) is not known to the provider and is required for the application of article 126zf or article 126zg, the public prosecutor can, in the interest of the investigation, order the provider to retrieve and provide the data in a manner to be determined by order in council.
3. Article 126na(3) and (4) apply *mutatis mutandis*.

Appendix 2
Articles of law pertaining to searching of computerised works

Article 125i Code of Criminal Procedure
The examining judge, the public prosecutor, the deputy public prosecutor and the investigating officer have the authority, under the same conditions referred to in articles 96b, 96c(1), (2) and (3), 97(1) to (4), and 110(1) and (2), to search the location where data have been stored or recorded on a data storage device. They can record these data in the interests of the investigation. Articles 96(2), 98, 99 and 99a apply *mutatis mutandis*.

Article 96b Code of Criminal Procedure
1. In the event that a criminal offence is discovered as it is being committed or in the event that a crime is suspected as defined in article 67(1), the investigating officer has the authority to confiscate a means of transport, with the exception of the living quarters if the inhabitant has not granted his or her permission, to search it and to effect entry to this means of transport.
2. If it is necessary for the purpose of exercising the authority granted pursuant to paragraph (1), the investigating officer can:
a. order the operator of the transport to stop the transport and
b. subsequently move the transport to a place designated by the officer or order the operator of the transport to move it to that place.

Article 96c Code of Criminal Procedure
1. In the event that a criminal offence is discovered as it is being committed or in the event that a crime is suspected as defined in article 67(1), the public prosecutor has the authority to search any location for the purposes of confiscation, with the exception of a residence if the inhabitant has not granted his or her permission, and an office of a person who has the authority to grant immunity, as referred to in article 218.
2. The deputy public prosecutor can exercise this authority in cases of extreme emergency and in cases that cannot wait for the public prosecutor to take action. He requires the authorisation of the public prosecutor in order to do so. If this authorisation cannot be requested in a timely manner on account of the urgency of the case or unavailability of the public prosecutor, this authorisation can be granted by the public prosecutor within three days after the search. If the public prosecutor refuses to grant this authorisation, then he or she will ensure that the consequences of the search are reversed as far as possible.
3. Searching locations in accordance with the provisions of paragraph (1) will take place under the supervision of the public prosecutor or, in the event that paragraph (2) applies, under the supervision of the deputy public prosecutor.
4. Article 96(2) applies *mutatis mutandis*.

Article 97 Code of Criminal Procedure
1. In the event that a criminal offence is discovered as it is being committed or in the event that a crime is suspected as defined in article 67(1), the public prosecutor can, in cases of extreme emergency and in cases that cannot wait for the examining judge to take action, search the following locations for the purposes of confiscation:

a. a residence if the inhabitant has not granted his or her permission, and
b. an office of a person who has the authority to grant immunity, as referred to in article 218.
2. The public prosecutor requires the authorisation of the examining judge for searches as referred to in paragraph (1). Reasons must be given for this authorisation.
3. If the case cannot wait for the public prosecutor to take action, then the deputy public prosecutor will have the authority to carry out a search. Paragraphs (1) and (2) will apply *mutatis mutandis*. The authorisation of the examining judge shall be requested if possible through the intermediation of the public prosecutor.
4. If the examining judge has authorised the deputy public prosecutor to search a residence without the permission of the inhabitant for the purposes of confiscation, the deputy public prosecutor in question will not require authorisation to enter that residence as referred to in section 2 of the General Act on Entry into Dwellings (Algemene wet op het binnentreden).
5. Article 96(2) applies *mutatis mutandis*.
Article 67 Code of Criminal Procedure
1. An order can be issued for pre-trial detention in the event that there is suspicion of:
a. a crime which, according to its statutory definition, is punishable by a term of imprisonment of four years or more;
b. one of the crimes defined in articles 132, 138a, 138b, 139c, 139d(1) and (2), 161e(1), under 1°, and (2), 137c(2), 137d(2), 137e(2), 137g(2), 285(1), 285b, 300(1), 321, 323a, 326c(2), 350, 350a, 351, 395, 417a and 420c of the Criminal Code;
c. one of the crimes described in:

- section 1221(1), Health and Welfare of Animals Act (Gezondheids- en welzijnswet voor dieren);
- section 175(2), under b, or subsection (3) in conjunction with subsection (1), under b, of the Road Traffic Act 1994 (Wegenverkeerswet 1994);
- section 30(2), of the Civil Authority Special Powers Act (Wet buitengewone bevoegdheden burgerlijk gezag);
- sections 52, 53(1) and 54 of the Military Service (Conscientious Objectors) Act (Wet gewetensbezwaren militaire dienst);
- section 31 of the Betting and Gaming Act (Wet op de kansspelen);
- section 11(2), of the Opium Act (Opiumwet);
- section 55(2), of the Weapons and Ammunition Act (Wet wapens en munitie);
- sections 5:56, 5:57 and 5:58 of the Financial Supervision Act (Wet op het financieel toezicht);
- section 11 of the Domestic Exclusion Act (Wet tijdelijk huisverbod)

2. The order can also be given in the event that no fixed abode in the Netherlands can be established in respect of the suspect and the person is suspected of having committed a crime which is brought before the courts, which crime is punishable by imprisonment according to its statutory definition.
3. The preceding paragraphs only apply if the facts or circumstances demonstrate that there is incriminating evidence against the suspect.
4. Notwithstanding the provisions of paragraph (3), incriminating evidence is not required for a warrant for arrest under suspicion of a terrorist crime.

Article 125j Code of Criminal Procedure
1. In the event of a search, an investigation can be conducted from the location of the search into data stored in computerised work in another location, which data are reasonably necessary to bring the truth to light. If such data are found then they can be recorded.
2. The investigation will not extend further than insofar as the persons working or living at the location where the search takes place have access to the computerised work with the permission of the rights holder to the computerised work from that location.

Article 125k Code of Criminal Procedure
1. Insofar as is specifically required by the interests of the investigation, an order can be given to provide access to the computerised work or parts thereof that are present, in the event that article

125i or article 125j are applicable to the person who is reasonably presumed to have knowledge of the manner in which a computerised work is secured. The subject of the order is required, if requested, to comply with the order by disclosing the knowledge about the security system.
2. Paragraph (1) applies *mutatis mutandis* in the event that encrypted data is found in a computerised work. The subject of the order will be the person who can reasonably be presumed to have knowledge of the manner in which the data are encrypted.
3. The order as referred to in paragraph (1) will not be issued to the suspect. Article 96a(3) applies *mutatis mutandis*.

Article 125l Code of Criminal Procedure
No investigation will be conducted into data that have been entered by or on behalf of persons who have the authority to grant immunity as referred to in article 218 insofar as their obligation to maintain secrecy extends to such data, unless they grant permission for such investigation. An investigation into computerised work that stores such data will only take place insofar as this does not breech professional or official secrecy, unless those persons give their permission.

Article 125la Code of Criminal Procedure
In the event of an investigation to record data found with a provider of a public telecommunications network or a public telecommunications service that are not intended for that provider or do not originate from it, the public prosecutor is only authorised to determine that cognisance is taken of these data and that they are recorded, insofar as they evidently originate from the suspect, are intended for the suspect, are related to the suspect or have served in the committing of the punishable offence, or that it is evident that the punishable offence has been committed in relation to these data. The public prosecutor requires prior written authorisation, to be granted by the examining judge upon his/her claim for it.

Article 125m Code of Criminal Procedure
If an investigation leads to the recording of data or their being rendered inaccessible, then the persons concerned will be given written notification as soon as possible about the recording or rendering inaccessible of those data and the nature of the data that have been recorded or rendered inaccessible. This notification will not be made if it is not reasonably possible to do so.
2. The public prosecutor or, in the event that the examining judge has applied the authority to search, the examining judge can decide that the notification to a person concerned referred to in paragraph (1) will be deferred as long as it is not in the interests of the investigation to notify this person.
3. Persons concerned are, within the meaning of this article:
a. the suspect;
b. the person responsible for the data;
c. the rights holder to the location where the search has taken place.
4. If the person concerned is the suspect, then notification can be waived in the event that this person is informed of the recording of the data and the nature of the recorded data through their inclusion in the procedural documents.

Article 125n Code of Criminal Procedure
1. As soon as it becomes apparent that the data recorded during the investigation are not significant to the investigation, they will be destroyed.
2. The person who recorded the data will be responsible for their destruction. An official record will be made of the destruction and will be included in the procedural documents.
3. The public prosecutor can determine that data recorded during a search can be used for:
a. a criminal investigation other than the one for which authority has been exercised;
b. processing with the intention of obtaining information on the involvement of persons in crimes and acts as referred to in section 10(1), parts a and b of the Police Data Act (Wet politiegegevens).

4. If paragraph 3, part a, is applied then, notwithstanding paragraph (1), the data need not be destroyed until the other investigation is completed. If paragraph 3, part b, is applied, then the data need not be destroyed until the Police Data Act no longer permits storing of the data.

Article 125o Code of Criminal Procedure
1. If during the search of a computerised work data are found relating to a punishable offence or that have aided the committing of a punishable offence, the public prosecutor or, during a preliminary judicial investigation, the examining judge can determine that the data be rendered inaccessible insofar as this is necessary to stop the punishable offence or to prevent new punishable offences.
2. Rendering data inaccessible is understood to mean taking measures to prevent the controller of the computerised work referred to in paragraph (1) or third parties from taking further cognisance or making further use of the data, as well as to prevent the further distribution of these data. Rendering inaccessible is also understood to mean the removal of the data from the computerised work, preserving the data required for the purposes of the criminal proceedings.
3. As soon as the interests of the criminal proceedings no longer require the measures referred to in paragraph (2) to be lifted, the public prosecutor or, during a preliminary judicial investigation, the examining judge shall determine that the data again be made available to the person controlling the computerised work.

Article 126n Code of Criminal Procedure
1. In cases where a crime is suspected as defined in article 67(1), the public prosecutor can, in the interests of the investigation, requisition data about a user of a communications service and the communication traffic relating to that user. The requisition can only relate to data designated by an order in council and can concern data that:
a. had been processed at the time of the requisition, or
b. were processed after the time of the requisition.
2. The requisition referred to in paragraph (1) can be addressed to any provider of a communications service. Article 96a(3) applies *mutatis mutandis*.
3. If the requisition concerns data as referred to in paragraph (1), second sentence under b, the requisition will relate to a period of at most 3 months.
4. The public prosecutor will draw up a record of the requisition, mentioning the following:
a. the crime and, if known, the name or otherwise and as accurate as possible a description of the suspect;
b. the facts or circumstances that show that the conditions referred to in paragraph (1), first sentence, have been met;
c. the name or otherwise and as accurate as possible a description of the person about whom the data is requisitioned, if known;
d. the requisitioned data;
e. the period covered by the requisition, if it concerns data as referred to in paragraph (1), second sentence under (b).
5. If the requisition concerns data as referred to in paragraph (1), second sentence under b, the requisition will be terminated as soon as it no longer meets the conditions as referred to in paragraph (1), first sentence. The public prosecutor will draw up a record of any amendment, addition, extension or termination of the requisition.
6. By or pursuant to an order in council, regulations can be laid down relating to the manner in which the data are requisitioned by the public prosecutor.

Article 126nc Code of Criminal Procedure
1. In cases where a crime is suspected the investigating officer can, in the interests of the investigation, requisition certain stored or recorded identifying personal information from the person who is a reasonably eligible subject of such requisition and who processes data for non-personal purposes.

2. Identifying information are understood to include:
a. name, address, postcode, place of residence and postal address;
b. date of birth and gender;
c. administrative characteristics;
d. in the case of a legal entity, instead of the information referred to in a and b: name, address, postal address, legal form and place of business.
3. A requisition as referred to in paragraph (1) cannot be addressed to the suspect. Article 96a(3) applies *mutatis mutandis*. The requisition cannot relate to personal information concerning a person's religion or personal beliefs, race, political affinity, health, sexual life or membership of a trade union.
4. A requisition as referred to in paragraph (1) is written and states:
a. a description of the person to whom the identifying information in the requisition relate;
b. the identifying information that are being requisitioned;
c. the period within which and the manner in which these information are to be provided;
d. the legal basis of the requisition.
5. In cases of extreme emergency a requisition as referred to in paragraph (1) can be issued orally. If this is the case, the investigating officer will draw up the requisition in writing afterwards and will deliver it within three days after the requisition is delivered to the person to whom the requisition is addressed.
6. The investigating officer will draw up an official record of the identifying information in which he/she will state:
a. the information referred to in paragraph (4);
b. the information issued;
c. the crime and, if known, the name or otherwise and as accurate as possible a description of the suspect;
d. the facts or circumstances that show that the conditions referred to in paragraph (1) have been met.
7. By or pursuant to an order in council, regulations can be laid down relating to the manner in which data are requisitioned by the investigating officer and the manner in which the data is requisitioned and supplied.

Article 126nd Code of Criminal Procedure
1. In cases where a crime is suspected as defined in article 67(1), the public prosecutor can, in the interests of the investigation, requisition certain stored or recorded data from the person who can be reasonably presumed to have access to this data.
2. A requisition as referred to in paragraph (1) cannot be addressed to the suspect. Article 96a(3) applies *mutatis mutandis*. The requisition cannot relate to personal data concerning a person's religion or personal beliefs, race, political affinity, health, sexual life or membership of a trade union.
3. A requisition as referred to in paragraph (1) is written and states:
a. if known, the name or otherwise an as accurate as possible a description of the person or persons about whom the data is requisitioned.
b. an as accurate as possible a description of the data that is being requisitioned and the period within which, as well as the manner in which these data are to be provided;
c. the legal basis of the requisition.
4. In cases of extreme emergency a requisition can be issued orally. If this is the case, the public prosecutor will draw up the requisition in writing afterwards and will deliver it within three days after the requisition is delivered to the person to whom the requisition is addressed.
5. The investigating officer will have an official record of the data which will state:
a. the data referred to in paragraph (3);
b. the data provided;
c. the crime and, if known, the name or otherwise and as accurate as possible a description of the suspect;

d. the facts or circumstances that show that the conditions referred to in paragraph (1) have been met.
e. the reason why the data are being requisitioned in the interests of the investigation.
6. In cases where a crime is suspected other than as referred to in paragraph (1), the public prosecutor can, in the interests of the investigation, make a requisition as referred to in that paragraph with the prior written authorisation of the examining judge. The examining judge will grant authority on the claim of the public prosecutor. Paragraphs (2) up to and including (5) apply *mutatis mutandis*.
7. By or pursuant to an order in council, regulations can be laid down to determine the manner in which data are requisitioned and provided.

Article 126ni Code of Criminal Procedure
1. In cases where a crime is suspected as defined in article 67(1), that given the nature or the connection with other offences committed by the suspect pose a serious threat to the rule of law, the public prosecutor can, in the event that the interests of the investigation urgently require it, demand from the person who can be reasonably presumed to have access to certain data, that at the time of the requisition are stored in a computerised work and for which it can reasonably be assumed that they are particularly vulnerable to loss or change, that these data be saved and kept accessible for a period of at most ninety days. The demand cannot be addressed to the suspect.
2. If the demand is addressed to the provider of a communications service within the meaning of article 126la and the demand relates, in part or in whole, to the data as referred to in article 126n(1), the provider is obliged to disclose as soon as possible the data that are necessary to identify other providers whose services were used during the communication.
3. The demand is issued in writing or orally. In the event that the demand is issued orally, the public prosecutor will draw up the demand in writing as soon as possible and will deliver a certified copy of it, within three days after the demand has been issued orally, to the person to whom the demand is addressed. The following will be stated in the demand and in drawing it up in writing:
a. an as accurate as possible a description of the data that are to be kept accessible;
b. the date of the demand;
c. the legal basis of the demand;
d. the period during which the data are to remain accessible, and
e. whether paragraph (2) applies.
4. The public prosecutor will issue the demand and, in the event that the demand is issued orally, he/she will draw up a written record of it,stating the following:
a. the data as referred to in paragraph (3)
b. the crime and, if known, the name and otherwise an as accurate as possible a description of the suspect; and
c. the facts or circumstances that show that the conditions referred to in paragraph (1) have been met.
5. The demand can be extended once at the most for a period not exceeding ninety days. Paragraphs (2), (3) and (4) apply *mutatis mutandis*.

Appendix 3
Amendments to special police powers in cyberspace: undercover purchasing

Section 126i former (undercover purchasing and provision of service) (came into effect 1-2-2000: Special Investigatory Powers Act 2000 (*Wet BOB*))
1. In cases where a crime is suspected as defined in article 67(1), the public prosecutor can, in the interests of the investigation, order the investigating officer to confiscate goods from or provide services to the suspect.
2. When executing the order, the investigating officer cannot drive the suspect to commit punishable offences other than that or those intended by the suspect beforehand.
3. The order for undercover purchasing or provision of service will be in writing and will state:
a. the crime and, if known, the name and otherwise an as accurate as possible a description of the suspect;
b. the facts or circumstances that show that the conditions referred to in paragraph (1) have been met;
c. the nature of the goods or services;
d. the manner in which the execution of the order will be given, including the punishable acts, and
e. the time at which or the period within which the execution of the order is given.
4. An investigating officer as referred to in paragraph (1) is understood to include a person in public service to a foreign state that meets the requirements as to be designated by an order in council.
5. Article 126g, paragraphs (6) up to and including (8) applies *mutatis mutandis*.
Notification of amendment 126i: Bulletin of Acts and Decrees, volume 2006, no. 300
Article 126i is amended as follows:
1. Paragraph (1) will read as follows:
1. In cases where a crime is suspected as defined in article 67(1), the public prosecutor can, in the interests of the investigation, order the investigating officer to
a. confiscate goods from the suspect,
b. confiscate from the suspect data that are stored, processed or transferred by means of a computerised work, through a public telecommunications network, or
c. provide the suspect with services.
2. In paragraph (3), under c, insert after «goods»: data.

Section 126i new (undercover purchasing and provision of service) (came into effect 1-9-2006: Computer Crime Act II (Wet computer-criminaliteit-II))
1. In cases where a crime is suspected as defined in article 67(1), the public prosecutor can, in the interests of the investigation, order the investigating officer to
a. confiscate goods from the suspect,
b. confiscate from the suspect data that are stored, processed or transferred by means of a computerised work, through a public telecommunications network, or
c. provide the suspect with services.
2. When executing the order, the investigating officer cannot drive the suspect to commit punishable offences other than that or those intended by the suspect beforehand.
3. The order for undercover purchasing or provision of service will be in writing and will state:
a. the offence and, if known, the name and otherwise an as accurate as possible a description of the suspect;

b. the facts or circumstances that show that the conditions referred to in paragraph (1) have been met;
c. the nature of the goods, data or services;
d. the manner in which the execution of the order will be given, including any punishable acts, and
e. the time at which or the period within which the execution of the order is given.
4. An investigating officer as referred to in paragraph (1) is understood to include a person in public service to a foreign state that meets the requirements as to be designated by an order in council.
5. Article 126g, paragraphs (6) up to and including (8) applies *mutatis mutandis*.