Criminaliteit in de Virtuele Ruimte

Amsterdam, mei 2002

Pepijn van Amersfoort (DSP-groep)
Leon Smit (TNO/FEL)
Mark Rietveld (DSP-groep)

Inhoudsopgave

Samenvatting

In opdracht van het onderzoeksprogramma Politie en Wetenschap heeft de DSP-groep een onderzoek verricht naar criminaliteit in de virtuele ruimte. In deze rapportage zijn de bevindingen van dit onderzoek neergelegd. Voor dit onderzoek is een begeleidingscommissie gevormd waarvan u de samenstelling kunt vinden in bijlage A.

Het gebied van de criminaliteit in de virtuele ruimte is in veel opzichten terra-incognita. In dit rapport wordt een basis gelegd voor de aanpak van en onderzoek naar deze vorm van criminaliteit. De nadruk ligt daarom op het krijgen van grip op criminaliteit in de virtuele ruimte. De centrale onderzoeksvraag van dit onderzoek luidt dan ook:

'Wat is de aard en omvang van criminaliteit in de virtuele ruimte?'

Deze vraag werd als volgt nader uitgewerkt:
1 Het door middel van een globale probleemanalyse breed in kaart brengen van de voor de ontwikkeling van de criminaliteit relevante aspecten in de digitalisering van de samenleving.
2 Het in kaart brengen van de effecten van deze digitalisering op de huidige en toekomstige mogelijkheden voor bestrijding; lopend van preventief tot repressief. Daarbij komt ook de organisatie van de bestrijding van deze vormen van criminaliteit aan bod.

Om deze uitwerkingen gestalte te geven is een analyse gemaakt van relevante literatuur en zijn interviews gehouden met sleutelfiguren binnen en buiten de politieorganisatie.

In de eerste plaats kan een onderscheid gemaakt worden tussen de begrippen 'new crimes' en 'old crimes' en 'new tools' en 'old tools'. De new crimes zijn in dit verband de vormen van criminaliteit die als doelwit slechts de (gegevens in) moderne computer- en telecommunicatieapparatuur kunnen hebben (bijvoorbeeld hacking). Old crimes zijn alle andere, meer 'traditionele' vormen van criminaliteit zoals diefstal. De andere dimensie in deze afbakening heeft betrekking op de instrumenten waarmee de criminaliteit wordt gepleegd. 'New tools' zijn alle moderne elektronische digitale technieken met behulp waarvan criminaliteit wordt gepleegd. Criminaliteit in de virtuele ruimte in brede zin heeft dus betrekking op die vormen van criminaliteit waarbij een 'digitale' component aanwezig is als instrument of als doelwit. Hierbij wordt de categorie 'new crimes, new tools' nog apart onderscheiden als 'criminaliteit in de virtuele ruimte in enge zin'.

Tabel A Crimes versus Tools

		Tools	
		Old	New
Crimes	Old	**1**- *old crimes, old tools*: - diefstal van geheugenchips uit computers door middel van braak-	**2**- *old crimes, new tools* - oplichting van consumenten door een nep website-
	New	**3**- *new crimes, old tools* - ontregelen van digitale meet-apparatuur (gas, licht, elektra)-	**4**- *new crimes, new tools* - hacking[1] -

Criminaliteit in de virtuele ruimte onderscheidt zich van 'traditionele' vormen van criminaliteit, omdat gebruik gemaakt wordt van een aantal aspecten van de digitalisering van de maatschappij. Er worden hiervoor de volgende zeven aspecten onderscheiden:

- Plaats en Afstand;
- Tijd en Frequentie;
- Anonimiteit;
- Kopieerbaarheid;
- Manipuleerbaarheid;
- Beschikbaarheid van informatie en
- Beschikbaarheid van apparatuur.

Werkdefinitie

Criminaliteit in de virtuele ruimte wordt met behulp van deze analyse gedefinieerd als die vormen van *criminaliteit* waarbij gebruik wordt gemaakt van *digitale dataopslag of datacommunicatie* én waarbij één of meerdere aspecten van de digitalisering van de criminaliteit *bepalend* zijn voor het gepleegde delict.

Over de omvang van criminaliteit in de virtuele ruimte is op dit moment weinig objectieve en betrouwbare informatie boven tafel te krijgen. Aan de ene kant is dit het gevolg van de onduidelijkheid die tot nu toe bestaat over een definitie van deze vorm van criminaliteit. Hiernaast wordt er vrijwel geen onderzoek gedaan naar het vóórkomen van deze vorm van criminaliteit. In deze studie is er een aantal bronnen in kaart gebracht waaronder politieregistratie en de gegevens van contactpersonen binnen het bedrijfsleven. Uit deze gegevens kan echter geen beeld gegenereerd worden van de omvang van criminaliteit in de virtuele ruimte.
In hoofdstuk 2 van dit rapport wordt een bloemlezing gegeven over verschijningsvormen van criminaliteit in de virtuele ruimte. De nadruk ligt hierbij op veel verschillende vormen van fraude en oplichting waarvan het plegen door digitale technieken worden vergemakkelijkt.

In hoofdstuk 3 worden de gevolgen van de digitalisering weergegeven die de Nederlandse politie ondervindt bij de aanpak van criminaliteit in de virtuele ruimte. Allereerst wordt de organisatie van de aanpak van cybercrime bij de politie geschetst. Deze is georganiseerd volgens het 'kennislagenmodel' waarbij de kennis gespecialiseerder wordt naarmate men verder van de Basispolitiezorg afstaat. De Bureau's Digitale Expertise en Bureau's Digitale Recherche (BDE's en BDR-en) vormen binnen de politieregio's de speerpunten bij de bestrijding van criminaliteit in de virtuele ruimte. Zij zijn verantwoordelijk voor het uitvoeren van een groot deel van het digitale 'speurwerk'.

Noot 1 Onder 'hacking' wordt verstaan het zich zonder toestemming van de beheerder toegang verschaffen tot een computersysteem. Hiervoor is het vaak noodzakelijk dat deze door middel van een netwerk zijn verbonden met andere computersystemen.

Mocht er behoefte zijn aan meer gespecialiseerde kennis dan kunnen deze eenheden terecht bij een afdeling van het Nederlands Forensisch Instituut (NFI) en het Korps Landelijke Politiediensten (KLPD). Op hun beurt zorgen de BDE's ervoor dat de basiskennis met betrekking tot digitaal rechercheren ook overgedragen wordt aan de politiemensen aan de basis van de politieorganisatie. Dit laatste verloopt niet altijd zonder problemen. Dit onder andere als gevolg van de werkdruk waar de medewerkers van de BDE's aan bloot staan. Zij houden zich hoofdzakelijk bezig met het leveren van een digitale component aan de ondersteuning van 'traditionele' recherchezaken inzake (seksueel) geweld en veel minder met 'nieuwe' vormen van criminaliteit als hacking. Een probleem dat wordt gesignaleerd, is dat de aangiftebereidheid voor 'nieuwe' vormen van criminaliteit vrij laag is. Daarbij komt dat deze vormen van criminaliteit in termen van schade en prioritering vaak niet door het 'case-screeningsmodel' komen. Er kan dus vaak aan dit soort zaken niet worden gewerkt omdat de prioriteiten van de korpsen elders liggen.

Naast de politie houden ook andere opsporingsdiensten en het bedrijfsleven zich bezig met de bestrijding van criminaliteit in de virtuele ruimte. Van de bijzondere opsporingsdiensten zijn vooral de FIOD en de Opsporingsdienst Buma-Stemra (ODBS) zeer actief aanwezig in de virtuele ruimte. Door deze laatste dienst wordt veel aandacht besteed aan de bestrijding van overtredingen van de Auteurswet. Daarbij ligt de nadruk op piraterij die wordt gepleegd met winstoogmerk. Ook banken en creditcardmaatschappijen hebben oog voor de gevolgen die digitalisering van de maatschappij heeft voor de veiligheid van haar netwerken en producten. Deze organisaties worden nogal eens geconfronteerd met het aspect van de 'afstand' van criminaliteit in de virtuele ruimte. De delicten worden veelal gepleegd vanuit een land waar Nederland geen rechtsmacht heeft. De samenwerking met buitenlandse politie en justitie is wat dat betreft aan verbetering toe.

Cybercrime, de 'nieuwe' vorm van criminaliteit die in feite niet zo nieuw is, is gerelateerd aan een brede maatschappelijke ontwikkeling, namelijk de digitalisering van de samenleving. De bestrijding van de toenemende mogelijkheden voor onveiligheid en criminaliteit door de digitalisering is daarmee niet een taak van de politie alleen. Om deze reden moet er een Integraal Veiligheidsplan voor criminaliteit in de virtuele ruimte worden opgezet, waarin de rollen en taken van een groot aantal betrokken partijen worden uitgewerkt.

Hienaast moet de verspreiding van kennis over moderne ICT- en communicatietechnologie en de invloed hiervan op de opsporing een speerpunt worden binnen de keten van politie en justitie. Daarbij moeten de BDE's hun registraties standaardiseren en verbeteren. Er moet vanuit politie en justitie zowel dader- als slachtofferonderzoek worden geïnitieerd naar criminaliteit in de virtuele ruimte. Onderdeel hiervan is dat in het werk van de digitale recherche meer aandacht diens te komen voor het eigen werkgebied van de digitale recherche: de 'new crimes'.

Ook moeten de Nederlandse overheid en politie het initiatief nemen om een vast samenwerkingsverband tussen internationale opsporingsinstanties op het gebied van criminaliteit in de virtuele ruimte op poten te zetten. Het case-screeningsmodel moet aangepast worden zodat meer rekening gehouden wordt met cybercrime. Voor zowel preventie als repressie van delicten in de virtuele ruimte is het wenselijk dat de politie meer actief patrouilleert op openbaar toegankelijke netwerken, net als in de niet-virtuele ruimte (meer blauw in cyberspace).

Summary

The DSP group has conducted a study on cyberspace crime, commissioned by the Police and Science research program. This report presents the results of this study. An advisory committee was formed for this study, the composition of which can be found in appendix A.

The field of cyberspace crime is in many respects terra incognita. This report lays the foundation for policies and research methods dealing with this form of crime. The focus is therefore on getting a handle on cyberspace crime. Hence the central research question for this study:

'What is the nature of cyberspace crime, and what is its scale?'

This question was further elaborated as follows:

3 Mapping those aspects in the digitization of society that are relevant to the development of crime by means of an outlined problem analysis.
4 Mapping the effects of aforementioned digitization on current and future possibilities for discouragement policies; moving from preventive action to repressive action. The organization of discouragement policies of these forms of crime is also discussed here.

In order to give shape to these results, relevant literature was analyzed and interviews were held with key figures both inside and outside the police organization.

First of all, a distinction can be made between the concepts of 'new crimes' and 'old crimes', and 'new tools' and 'old tools'. In this respect, new crimes are considered the forms of crime the object of which can only be the (data in) modern computer and telecommunication equipment (e.g. hacking). Old crimes are defined as all other, more 'traditional' forms of crime, like theft. The other dimension to this distinction concerns the tools that are used in committing the crimes. 'New tools' are defined as all modern electronic digital techniques that are used to commit crimes. Cyberspace crime in the broader sense therefore concerns those forms of crime that contain a 'digital' component as a tool or as its objective. The category 'new crimes, new tools' is referred to separately as 'cyberspace crime in the strictest sense'.

Table A Crimes versus Tools

		Tools	
		Old	New
Crimes	Old	**1**- *old crimes, old tools*: - theft of memory chips from computers by means of burglary-	**2**- *old crimes, new tools* - defrauding consumers with a fake website-
	New	**3**- *new crimes, old tools* - deranging digital measuring equipment (gas, light, electricity)-	**4**- *new crimes, new tools* - hacking[2] -

Note 2 The term 'hacking' is defined as the accessing of computer systems without the authorization of the system administrator. This often requires a network connection to other computer systems.

Cyberspace crime differs from 'traditional' forms of crime because a number of aspects of society's digitization practices are employed. The following seven aspects are distinguished in regard to this:

- Location and Distance;
- Time and Frequency;
- Anonymity;
- Copyability;
- Manipulability;
- Availability of information;
- Availability of equipment.

Working definition
Based on this analysis, cyberspace crime can be defined as those forms of *crime* in which *digital data storage or data communication* are used, and in which one or more aspects of the digitization of crime are *defining* for the committed offence.

At this moment, little reliable objective information regarding the scale of cyberspace crime can be acquired. This is partly the result of the lack of clarity that exists concerning a definition of this form of crime. On top of this, there has been very little research on the occurrence of this form of crime. A number of resources are mapped out in this study, including police registration and data from contact persons within the business community. However, this data fails to produce a reliable picture of the current scale of cyberspace crime.
Chapter 2 of this report contains a miscellany on various forms of cyberspace crime. The focus lies on many different forms of fraud and deception that are easier to commit by means of digital techniques.

Chapter 3 reports on the consequences of digitization that the Dutch police encounter in fighting cyberspace crime. First, the organization of police policy in fighting cyberspace crime is outlined. This is organized according to the 'knowledge layers model' in which the knowledge becomes more and more specialized the further it is removed from basic police duties.
The Digital Expertise Bureaus (*Bureau Digitale Expertise* – BDE) and the Digital Investigation Bureaus (*Bureau Digitale Recherche* - BDR) spearhead cyberspace crime investigations within the various police regions. They are responsible for conducting a large part of digital investigations. Should there be a need for more specialized knowledge, these units can make use of a department of the Netherlands Forensic Institute (*Nederlands Forensisch Instituut* - NFI) and the Netherlands National Police Agency (*Korps Landelijke Politiediensten* - KLPD). For their part, the BDEs make sure that basic knowledge regarding digital investigation is also passed on to the police officers at the core of the police organization. This does not always occur without problems, which is partly a result of the work pressure to which BDE employees are exposed. They are mainly preoccupied with providing a digital component to the support for 'traditional' investigations concerning (sexual) harassment, and much less with 'new' forms of crime like hacking. A problem that has been observed is that the willingness to report 'new' forms of crime is rather limited. In addition, these forms of crime often do not make it through the 'case-screening model' in terms of damage and prioritization. This means that these kinds of cases are often ignored because the police forces' priorities lie elsewhere.

Apart from the police, several other investigation departments as well as the business community are also occupied with fighting cyberspace crime. Among the special investigation departments, the Fiscal Information and

Investigation Service (*Fiscale Inlichtingen- en Opsporingsdienst* - FIOD) and the Buma-Stemra Investigation Service (*Opsporingsdienst Buma-Stemra* - ODBS) are especially active and have a strong presence in cyberspace. The ODBS is focused for a large part on fighting breaches of copyright law. Their main target is piracy committed with a profit motive. Banks and credit card companies are also aware of the consequences the digitization of society has for the safety of their networks and products. These organizations are often faced with the 'distance' aspect of cyberspace crime. Many offences are committed in countries in which the Netherlands do not have jurisdiction. In that respect, cooperation with foreign police and judiciary is in need of improvement.

Cyberspace crime, the 'new' form of crime – which actually is not new at all – is related to a broad social development, namely the digitization of society. The fight against the increasing possibilities for crime and lack of safety due to digitization is therefore not a task for the police alone. This is why an Integral Safety Plan for cyberspace crime should be formulated, in which the roles and tasks of a great number of parties involved are elaborated.

In addition, the spread of knowledge about modern ICT and communication technology and its influence on investigation should be made a spearhead within the chain of police and judiciary. Furthermore, the BDEs should standardize and improve their registrations. From the side of the police and the judiciary, research should be initiated on perpetrators as well as victims of cyberspace crime. This also partly entails that the digital investigation department should pay more attention to its own field: the 'new' crimes'.

Moreover, the Dutch government and police should take the initiative in setting up regular cooperation between international investigation departments in the field of cyberspace crime. The case-screening model should be adapted in order to provide increased attention for cyberspace crime. It is desirable for the prevention as well as the repression of cyberspace crime that the police patrol more actively on publicly accessible networks, just like they do on the streets (more uniforms in cyberspace).

1 Inleiding

In opdracht van het onderzoeksprogramma Politie en Wetenschap heeft de DSP-groep (voorheen Van Dijk, Van Soomeren en Partners) in samenwerking met TNO-FEL een onderzoek uitgevoerd naar criminaliteit in de virtuele ruimte.
Dit lijkt een weinig problematische openingszin van een onderzoeksrapport, maar schijn bedriegt. 'Waar gaat jullie onderzoek nu over?' is de vraag die ons als onderzoekers het meest is gesteld. Het beantwoorden van deze vraag bleek moeilijker dan wij bij aanvang van het onderzoek hadden verwacht.

Criminaliteit in de virtuele ruimte of 'cybercrime'[3] is een relatief nieuw verschijnsel. De digitalisering van de maatschappij heeft de laatste decennia een grote vlucht genomen. Illustratief hiervoor zijn onder andere de toename van het aantal computers in privé-bezit, het toenemende aantal mensen dat zich op het internet begeeft en toenemende digitalisering van vele apparaten (lopend van telefoon tot magnetron, van boordcomputer in de auto tot meters voor water, gas en elektra). Met deze snel toenemende digitalisering verandert de maatschappij en daarmee ook het maatschappelijke verschijnsel van de criminaliteit.
Ondanks de grote hoeveelheid aan publicaties over technische ontwikkelingen, beveiligingsproblemen en (schijnbare) beveiligingsoplossingen, is het gebied van criminaliteit in de virtuele ruimte feitelijk terra-incognita. Wij hebben gepoogd in dit rapport de basis te leggen voor onderzoek naar cybercrime. Een cruciale stap daarbij is het krijgen van grip op de materie en het geven van een kader voor onderzoek naar en de aanpak van criminaliteit in de virtuele ruimte.

In samenwerking met de speciaal voor dit onderzoek samengestelde begeleidingscommissie (zie bijlage A) werd zeer regelmatig over de voortgang van het onderzoek maar zeker ook over de inhoud ervan, van gedachte gewisseld. Zij hebben hierdoor waardevol bijgedragen aan het eindproduct zoals het nu voor u ligt. Wij als onderzoekers zijn hen dank verschuldigd.

1.1 Vraagstelling van het onderzoek

Binnen dit onderzoek stond de volgende probleemstelling centraal:
'Wat is de aard en omvang van criminaliteit in de virtuele ruimte?'

Deze vraag werd als volgt nader uitgewerkt:
1 Het door middel van een globale probleemanalyse breed in kaart brengen van de voor de ontwikkeling van de criminaliteit relevante aspecten in de digitalisering van de samenleving.
2 Het in kaart brengen van de effecten van deze digitalisering op de huidige en toekomstige mogelijkheden voor bestrijding; lopend van preventief tot repressief. Daarbij komt ook de organisatie van de bestrijding van deze vormen van criminaliteit aan bod.

Noot 3 Wij zullen deze begrippen in dit rapport als synoniemen gebruiken.

1.2 Leeswijzer

In hoofdstuk 2 wordt een analyse gemaakt van criminaliteit in de virtuele ruimte. Er wordt door middel van een afbakening en definiëring van criminaliteit in de virtuele ruimte duidelijk gemaakt op welke aspecten van criminaliteit de digitalisering invloed heeft en hiernaast welke (nieuwe) vormen van criminaliteit zijn ontstaan door de digitalisering.
De resultaten die uit deze analyse komen worden in hoofdstuk 3 vertaald naar de gevolgen voor de opsporing. Hierbij wordt aandacht besteed aan de vraag hoe de bestrijding van criminaliteit verandert onder invloed van digitalisering en tegen welke problemen de politie aanloopt bij de aanpak van cybercrime.
Hoofdstuk 4 bevat ten slotte de conclusies en aanbevelingen die uit het onderzoek naar voren zijn gekomen. Hierbij wordt ook aandacht besteed aan de aanpak van criminaliteit in de virtuele ruimte in de (nabije) toekomst. De kenmerken van de digitalisering van de criminaliteit (hoofdstuk 2) en de gevolgen voor de opsporing (hoofdstuk 3) worden hier verder uitgewerkt met betrekking tot hun consequenties voor de toekomst voor de aanpak van cybercrime.

2 Cybercrime

Voor de aanpak van criminaliteit in de virtuele ruimte, en ook voor de organisatie van deze aanpak, is het van belang inzicht te hebben in het fenomeen cybercrime. Los van mythevorming rond dit onderwerp is een analyse van het begrip 'criminaliteit in de virtuele ruimte' noodzakelijk.
Ook voor de beantwoording van de centrale vraagstelling binnen dit onderzoek naar de aard en omvang van criminaliteit in de virtuele ruimte is het van belang dat dit begrip goed wordt afgebakend en gedefinieerd.

In dit hoofdstuk wordt een afbakening en definitie voorgesteld van 'criminaliteit in de virtuele ruimte'. Deze afbakening is niet eenvoudig. Er zijn zeer veel verschillende verschijningsvormen van criminaliteit waarbij een digitale component valt te onderscheiden. Deze verschijningsvormen laten zich niet gemakkelijk in traditionele misdaadcategorieën plaatsen. Het hanteren van deze traditionele misdaadcategorieën levert op deze manier niet het gewenste inzicht op over wat cybercrime nu eigenlijk is.

De afbakening en definitie van criminaliteit in de virtuele ruimte wordt in dit hoofdstuk in drie stappen aangepakt.

- In de eerste plaats wordt, aan de hand van een door de Engelse National Hi-Tech Crime Unit (NHTCU) gemaakte indeling van criminaliteit, afgebakend wat zeker *niet* behoort tot criminaliteit in de virtuele ruimte.
- Als tweede stap wordt vervolgens bekeken welke aspecten van de digitalisering van de samenleving relevant zijn voor het begaan en aanpakken van deze vormen van criminaliteit.
- Als laatste stap kan aan de hand van de gemaakte afbakening en de omschreven aspecten een definitie worden gegeven van criminaliteit in de virtuele ruimte.
- Tenslotte wordt aan het einde van dit hoofdstuk een aantal delicten dat onder de definitie valt verder uitgewerkt om de aspecten van de digitalisering van criminaliteit nader te duiden.

2.1 Old en New crimes - een eerste afbakening

Voor een eerste afbakening van criminaliteit in de virtuele ruimte wordt aansluiting gezocht bij het door de Engelse National Hi-Tech Crime Unit (NHTCU) gemaakte onderscheid tussen 'old versus new crimes' en 'old versus new tools'. Met het onderscheid tussen old en new tools worden hier de *instrumenten* met behulp waarvan delicten worden gepleegd bedoeld. Onder new tools kunnen alle moderne digitale en elektronische technieken worden verstaan: GSM's, computers, GPS- en, etc. De old tools zijn op hun beurt alle 'ouderwetse' (niet-digitale) gereedschappen waarmee misdrijven worden gepleegd.

De begrippen old crimes en new crimes dienen ervoor om een ander onderscheid te maken: dat tussen verschillende *doelwitten* van criminaliteit. De new crimes kunnen slechts worden gepleegd 'tegen' moderne digitale (opslag)instrumenten als computersystemen. Men kan hierbij denken aan het onklaar maken van de systemen of het manipuleren van gegevens die daar op staan. Het doel hiervan is bijvoorbeeld het systeem onbruikbaar maken of de daarin opgeslagen gegevens te vernietigen of te veranderen ter eigen gewin.

Bij dit onderscheid staan kenmerken van de aard van het strafbare feit centraal. New crimes kunnen alleen gepleegd worden ten opzichte van een object dat wat betreft de inhoud digitaal van aard is. De specifieke eigenschappen van de digitale inhoud van het object maakt dat deze vormen van criminaliteit worden onderscheiden van 'old crimes'.

Tabel 2.1 Crimes versus Tools

		Tools	
		Old	New
Crimes	Old	**1**- *old crimes, old tools*: - diefstal van geheugenchips uit computers door middel van braak-	**2**- *old crimes, new tools* - oplichting van consumenten door een nep website-
	New	**3**- *new crimes, old tools* - ontregelen van digitale meet-apparatuur (gas, licht, elektra)-	**4**- *new crimes, new tools* - hacking[4] -

Uit deze tabel valt af te leiden dat een gedeelte van de criminaliteit dat gericht is tegen computersystemen of andere digitale apparatuur, oude vormen van criminaliteit betreft die gepleegd worden met oude, traditionele gereedschappen. Dit is de criminaliteit in kwadrant 1. Het enige hier relevante aspect van de digitale apparatuur is dat zij een bepaalde economische waarde vertegenwoordigt. Deze categorie delicten vormt geen onderdeel van criminaliteit in de virtuele ruimte (zie paragraaf 2.3). Uiteraard vallen in deze categorie ook alle andere traditionele en klassieke vormen van criminaliteit.

Een vermoedelijk omvangrijke categorie delicten vindt men terug in kwadrant 2: old crimes, new tools. In deze categorie vallen alle vormen van criminaliteit waarvan het plegen door middel van digitale middelen wordt vereenvoudigd. Het in de matrix genoemde voorbeeld kan eenvoudig worden uitgebreid met uiteenlopende delicten als het verspreiden van kinderpornografie, handel in verboden middelen, fraude, bedreiging, etc., etc.

In kwadrant 3 vinden we een beperkt aantal soorten delicten. Hier worden de old tools gebruikt om elektronische apparatuur te beschadigen of te manipuleren: bij deze vormen van criminaliteit wordt digitale apparatuur door middel van 'traditionele' methoden (zoals een inbraak bijvoorbeeld) als doelwit van criminaliteit. Het onderscheidende aspect hierbij is dat digitale apparatuur het doelwit is van deze 'old tools': het kan voor criminelen interessant zijn om computerapparatuur van een ander plat te leggen of gegevens hierop te veranderen of te vernietigen.

Hetzelfde 'new crimes' - principe geldt voor de delicten in kwadrant 4. De delicten in dit kwadrant kunnen ook slechts gepleegd worden tegen computersystemen en andere digitale apparatuur. Het verschil met de delicten in kwadrant 3 is dat er in deze categorie noodzakelijkerwijze gebruik moet worden gemaakt van de new tools . In deze categorie worden (de gegevens in) computersystemen 'het slachtoffer van' delicten die gepleegd worden door gebruik te maken van andere digitale apparatuur. Het soort delicten dat in deze categorie valt, is vrij beperkt: men kan naast de in het voorbeeld genoemde hacking- praktijken ook bijvoorbeeld denken aan het tegen de wil van

Noot 4 Onder 'hacking' wordt verstaan het zich zonder toestemming van de beheerder toegang verschaffen tot een computersysteem. Hiervoor is het vaak noodzakelijk dat deze door middel van een netwerk zijn verbonden met andere computersystemen.

de beheerder 'manipuleren' van elektronische meet- en regelsystemen via een netwerkverbinding.

Naar aanleiding van de bovenstaande indeling kan men 'criminaliteit in de virtuele ruimte' op twee manieren afbakenen:

- 'Cybercrime in enge zin'. In deze categorie vallen de delicten in kwadrant 4: de new crimes, new tools. ICT- apparatuur vormt binnen deze categorie zowel het doelwit als de middelen van deze vormen van criminaliteit. Deze delicten spelen zich ook in de meeste gevallen af buiten de fysieke werkelijkheid, maar bijvoorbeeld binnen de werkelijkheid van een computernetwerk. Ze zijn dan ook met recht 'virtueel' te noemen.
- 'Cybercrime in brede zin'. Dit zijn alle delicten binnen de kwadranten 2, 3 en 4: hier wordt ofwel gebruik gemaakt van digitale instrumenten bij het plegen van de delicten, dan wel vormt (de data in) ICT- apparatuur het doelwit van het delict.

Het is duidelijk dat 'Virtuele criminaliteit in enge zin' het 'hart' zal vormen van de definitie van criminaliteit in de virtuele ruimte. Bij de delicten binnen de tweede categorie is deze afbakening wat minder duidelijk. Valt bijvoorbeeld drugshandel met behulp van een GSM nog binnen deze definitie? Ditzelfde geldt voor de delicten in kwadrant 3; valt het stelen van computergegevens met behulp van 'old tools' nog binnen criminaliteit in de virtuele ruimte? Hiernaast lijkt het er op dat deze categorieën ook in elkaar kunnen overlopen: de grenzen tussen de categorieën zijn niet 'hard'.

Om een antwoord op deze vragen te formuleren en tot een verdere afbakening te komen zijn als tweede stap in de volgende paragraaf een aantal aspecten op een rij gezet die criminaliteit in de virtuele ruimte kunnen onderscheiden van traditionele criminaliteit. Deze aspecten betreffen zaken die specifiek een rol spelen bij criminaliteit in de virtuele ruimte. Het betreft hier zowel aspecten die het plegen van delicten vergemakkelijken als wel aspecten die opsporingsinstanties tot dienst zouden kunnen zijn bij de aanpak van criminaliteit in de virtuele ruimte.

2.2 Specifieke aspecten van criminaliteit in de virtuele ruimte

De digitalisering van de samenleving heeft gevolgen voor de mogelijkheden voor het plegen van delicten. Daarentegen worden ook de mogelijkheden voor de aanpak van criminaliteit verruimd. De kern achter deze nieuwe mogelijkheden wordt gevormd door bepaalde kenmerken van de digitalisering. Bepaalde aspecten van digitale technieken zorgen voor nieuwe mogelijkheden.

Er zijn zeven belangrijke kenmerken van digitalisering die de spelregels rond criminaliteit en de aanpak daarvan veranderen:

1 Plaats en Afstand
Met behulp van ICT- technologie kan tussen dader en slachtoffer of plaats delict en dader een grote afstand gecreëerd worden. Bij een fysiek grotere afstand ziet de dader minder van de gevolgen van zijn daden en is er minder kans op terughoudendheid of berouw. Anderzijds kent de dader de voor hem gunstige lokale omstandigheden en de specifieke zwakheden van zijn slachtoffer slechter. Ook kan een dader de mogelijkheden van een *juridisch* grotere afstand benutten door zijn daden te plegen in een jurisdictie die geen macht over hem kan uitoefenen (bijvoorbeeld een ander land).

2 Tijd en Frequentie
Een delict kan door middel van ICT- technologie relatief gemakkelijk duizenden keren herhaald of gelijktijdig begaan worden. Een kleine winst per delict levert dan toch uiteindelijk veel gewin op.

3 Anonimiteit
Daders kunnen eenvoudiger anoniem opereren. Hiermee verwant is het probleem van authenticiteit: het is niet eenvoudig te achterhalen met wie je van doen hebt. Aan de nullen en enen kun je niet zien wie van deze digitale techniek gebruik heeft gemaakt.

4 Kopieerbaarheid en Gemak van verspreiding
De kopieerbaarheid van informatie speelt onder andere bij criminaliteit omtrent auteursrechten en intellectuele eigendomsrechten. Het is zeer gemakkelijk snel (misleidende) informatie en software te verspreiden. Van belang is ook dat kopieën kunnen worden gemaakt zonder verlies van informatie, kwaliteit en zonder het origineel aan te tasten. Dit geeft bijvoorbeeld aanleiding tot discussie over welke schade er is op het moment dat er een kopie van een bestand wordt gemaakt. Kan men in zo'n geval spreken van diefstal? Het origineel is tenslotte vaak nog in onveranderde staat aanwezig.

5 Manipuleerbaarheid en Uitwissen van sporen
Het veranderen van bits in digitale opslagsystemen is in sommige digitale systemen zeer eenvoudig. Zo kunnen sommige gegevens, opgeslagen in computerbestanden of chipkaarten, op een gemakkelijke manier worden gemanipuleerd. Dit hangt uiteraard af van de toegankelijkheid van de digitale informatie: dit is eenvoudiger bij normale PC's dan bij de chipkaarten van de banken.
Digitale sporen van criminaliteit kunnen op systemen die onder controle zijn van de dader snel en onherkenbaar worden gewist. Sporen die op netwerken worden achtergelaten die niet onder zijn controle zijn , kunnen echter door opsporingsinstanties worden achterhaald.

6 Beschikbaarheid van informatie
De informatiekosten die een dader maakt om zijn daden voor te bereiden worden lager als deze informatie gemakkelijk te vinden is: bijvoorbeeld op een openbaar toegankelijk netwerk als het internet. Criminele kennis kan makkelijk worden uitgewisseld of worden ingewonnen. Hier staat tegenover dat de mogelijkheden van de overheid of slachtoffers om te waarschuwen tegen criminele praktijken ook groter zijn.

7 Beschikbaarheid apparatuur
Tien jaar geleden, voor de internet explosie, werd de PC ontdekt als universeel en goedkoop alternatief voor diverse dure meet- en regelapparatuur. De dure oscilloscoop bleek vervangbaar door een goedkope PC en kwam daarmee binnen bereik van veel meer mensen, ook in ontwikkelingslanden. Deze 'democratiserende' werking van lage kosten en hoge beschikbaarheid vergroot nu ook de toegankelijkheid tot cybercrime. Kosten voor criminaliteit in de virtuele ruimte kunnen met betrekking tot netwerkcriminaliteit beperkt blijven tot een PC en mogelijke enkele interface kaarten. Vaak zijn de kosten voor aanschaf van apparatuur dus laag en is deze apparatuur makkelijk verkrijgbaar. Er zijn echter ook specifieke verschijningsvormen van cybercrime waarvoor grote investeringen gedaan moeten worden. Zeer specialistische, krachtige of op eigen specificaties gemaakte apparatuur kan zeer kostbaar zijn.

Sommige van deze aspecten zoals tijd en frequentie (aspect 2) vergroten met name het aantal slachtoffers dan onder bereik van criminelen valt. Andere aspecten zoals de anonimiteit (aspect 3) spelen personen met een criminelen intentie op een andere wijze in de kaart. Kopieerbaarheid en manipuleerbaarheid (aspecten 6 en 7) brengen nieuwe objecten van criminaliteit in beeld.

Bovenstaande kenmerken van digitalisering en netwerken kunnen criminaliteit bevorderen maar mogelijk ook tegenwerken, afhankelijk van wie de middelen hanteert. Hieraan wordt later in dit rapport nog aandacht besteed.

2.3 Een werkdefinitie van Cybercrime

Uitgaande van de afbakening van criminaliteit in de virtuele ruimte en de in de voorgaande paragraaf beschreven effecten van de digitalisering op criminaliteit, is het mogelijk een werkbare definitie te geven van criminaliteit in de virtuele ruimte:

Definitie Cybercrime

Cybercrime is *criminaliteit* waarbij gebruik wordt gemaakt van:
a *digitale dataopslag of datacommunicatie* en
b waarbij één of meerdere effecten van de digitalisering van de criminaliteit *bepalend* zijn voor het gepleegde delict (zie punten 1 tot en met 7 van de vorige paragraaf).

Hoe meer een specifiek delict gekenmerkt wordt door de digitale component ervan en hoe meer het steunt op de effecten van de digitalisering zoals ze hiervoor zijn beschreven, des te meer is het een vorm van criminaliteit die valt binnen het gebied van de virtuele criminaliteit. De definitie levert op deze manier niet een waterdichte afbakening van het gebied van Cybercrime, maar het is vooralsnog een goede werkdefinitie om grip te krijgen op de criminaliteit in de virtuele ruimte. Het moge verder duidelijk zijn dat de 'grensgevallen' van de definitie zich vooral bevinden binnen de eerder genoemde 'virtuele criminaliteit in brede zin; voor de subcategorie van delicten binnen de 'virtuele criminaliteit in enge zin' is dit eenvoudiger. Een voorbeeld van zo'n grensgeval kan dit wellicht verduidelijken:

Als men een frauduleuze boekhouding bijhoudt in een spreadsheetprogramma op een PC, in plaats van in een eenvoudig papieren schriftje, dan verandert er alleen iets aan het medium waarin of waarop de gegevens zijn opgeslagen. In dit voorbeeld wordt daarbij wel gebruik gemaakt van digitale technieken (de computer). Aan het andere element van de definitie wordt echter niet voldaan: er wordt geen gebruik gemaakt van de specifieke eigenschappen van de digitale technieken om deze vorm van criminaliteit te plegen. Dit verandert als er wel gebruik wordt gemaakt van één van de eigenschappen. Plaatst men de bestanden van de PC op een webserver in Costa Rica (aspect: afstand en kopieerbaarheid) dan is het voor de Nederlandse politie meteen moeilijker om deze administratie veilig te stellen. Hetzelfde geldt als het bestand door de fraudeur is versleuteld weggeschreven op de PC, zodat niet meer herkenbaar is wat er in staat (aspecten kopieerbaarheid, manipuleerbaarheid en anonimiteit). De vormen van fraude uit de laatste twee voorbeelden vallen wel binnen de definitie die hierboven is gegeven, de eerste vorm niet

Het is duidelijk dat de aspecten die genoemd worden onder b. in de definitie dan ook een *inperking* zijn van de vormen die onder a. vallen. Categorie a is in beginsel veel ruimer dan categorie b.

2.4 Omvang van criminaliteit in de virtuele ruimte

Helaas moet geconcludeerd worden dat op dit moment de omvang van criminaliteit in de virtuele ruimte niet objectief bepaald kan worden. Wij hebben op diverse wijzen geprobeerd deze informatie boven tafel te krijgen, maar er blijken geen bronnen te zijn waarop we met enige mate van betrouwbaarheid, objectief de omvang van cybercrime kunnen vaststellen. In de eerste plaats zijn de volgende bronnen in kaart gebracht:

- De Bureaus Digitale Expertise (BDE) van de politie;
- Politieregistraties van misdrijven in de virtuele ruimte;
- Bronnen binnen het bedrijfsleven: sleutelpersonen bij Internet Service Provider's (ISP's), banken, verzekeringsmaatschappijen en andere bedrijven als potentieel 'slachtoffer' van computercriminaliteit;
- de zogenaamde 'Hacker Community' als mogelijke bron van 'daders' van virtuele criminaliteit via het internet.

De interviews met medewerkers en hoofden van de BDE's en de mensen van de centrale eenheid digitale recherche van het Korps Landelijke Politiediensten (KLPD) bleken een goede bron voor een kwalitatief beeld van de werkzaamheden van de Nederlandse politie op het gebied van digitaal recherchëren. Er bleken geen gegevens beschikbaar over:

- door de Nederlandse politie behandelde zaken van virtuele criminaliteit en
- de mogelijke omvang van het verschijnsel cybercrime.

In het volgende hoofdstuk in de paragraaf 3.1 komen we hierop terug.

Vanuit eigen ervaring die de onderzoekers hebben met politieregistraties binnen de bedrijfsprocessensystemen als HKS, BPS en X-pol, weten zij dat deze registraties weinig informatie bevatten over criminaliteit in de virtuele ruimte. Deze bronnen zijn dan ook niet bruikbaar voor een onderzoek naar de omvang van criminaliteit in de virtuele ruimte.

Ook Internet Service Providers (ISP's), verzekeraars en ander bedrijven hebben binnen het huidige onderzoek niet als bron voor het vaststellen van de omvang van cybercrime kunnen dienen. Men bleek over het algemeen niet bereid tot medewerking aan dit onderzoek en houdt incidenten van computercriminaliteit en de (preventieve) maatregelen die men neemt het liefst binnenshuis. In ieder geval bestaat er ook binnen het bedrijfsleven geen centrale, eenvoudig te raadplegen registratie voor deze vormen van criminaliteit.

Door een tweetal onderzoekers werd verder de hackersconferentie HAL2001 bezocht. Uit deze bijeenkomst is een beeld verkregen omtrent de subcultuur waarin een deel (de harde kern) van de hackers zich begeeft en bevindt. Een beschrijving hiervan treft u aan in bijlage D. Ook hier konden echter geen cijfermatige gegeven worden achterhaald met betrekking tot de omvang van hun (criminele) activiteiten.

Wat rest voor het krijgen van een beeld van de omvang van criminaliteit in de virtuele ruimte, zijn subjectieve indrukken van in het werkveld bij deze materie betrokken personen. In het volgende hoofdstuk komen we hier (kort) op terug.

2.5 Delictgroepen binnen de virtuele ruimte

Het Wetboek van Strafrecht biedt weinig houvast om tot een systematisering van delicten in de virtuele ruimte te komen. Gekozen is voor een categorisering op basis van vermogenschade en ander nadeel dan vermogensschade

(zie voor een vergelijkbaar onderscheid boek 6 van het Burgerlijk Wetboek). Verder kunnen schades voor natuurlijke personen, bedrijven en het publieke domein worden onderscheiden. Deze onderscheiden zijn hier gemaakt om enige systematiek te brengen in de beschrijving van een groot aantal verschijningsvormen van cybercrime. Uiteraard zijn andere indelingen ook mogelijk. In tabel 2.2 wordt dit onderscheid weergegeven.

Tabel 2.2 Verschijningsvormen cybercrime

Natuurlijke personen	(1) Vermogensschade
	(2) Aantasting persoonlijke levenssfeer
Bedrijven of rechtspersonen	(3) Vermogensschade
	(4) Aantasting reputatie
Publieke domein	(5) Aantasting publieke moraal

De beschrijvingen uit tabel 2.2 bieden meer inzicht in de zaken waarmee de diverse opsporingsinstanties geconfronteerd (kunnen) worden. Bij deze beschrijvingen dient de lezer de hiervoor gegeven definitie en de diverse aspecten van de digitalisering in gedachte te houden.

2.5.1 Vermogensdelicten overwegend gericht tegen natuurlijke personen

2.5.1.1 Oplichting en bedrog

Het plegen van oplichting en bedrog is nooit afhankelijk geweest van geavanceerde digitale middelen. Toch hebben de mogelijkheden van telecommunicatie aanleiding gegeven tot een grote groei van telemarketing fraude. Het betreft dan fraude gepleegd door sluwe verkopers die hun slachtoffers overwegend telefonisch benaderen. De omvang en aard van telemarketing fraude in de Verenigde Staten zijn te vinden op de website van de FBI[5].

> "Telemarketing fraud continues to grow and has been estimated by numerous government agencies to cost $40 billion annually and victimize millions of people. One case in Nevada involved 800,000 victims. The telemarketing industry employs over 3.4 million people, and industry estimates place total consumer spending through telemarketing at $500 billion per year.
> Telemarketing fraud and other fraud by wire matters can be very difficult crimes to investigate. Typically, individuals
> committing fraud by wire use multiple aliases, telephones, mail drops, and business locations. They can change their method of solicitation, product line, and other recognisable traits overnight. Their operations are mobile and their schemes are complex. Criminal intent is often difficult to prove, and the majority of individual losses are under prospective thresholds. The elderly population is particularly targeted and susceptible to telemarketers."

Het is verder moeilijk te achterhalen welk gedeelte van de totale telemarketing fraude in de hand gewerkt wordt door de inzet van ICT technologie. Een enigermate kwantitatief overzicht van de schade van internet fraude, met een onderverdeling naar wijze van benadering, betaling, misleidingschema en typering van slachtoffers is te vinden op www.fraud.com. Dit overzicht is voor 2001 hieronder weergegeven.

Noot 5 Zie http://www.fbi.gov/hq/cid/fc/ec/about/about_tm.htm , laatst geraadpleegd op 24 april 2002.

Tabel 2.3 Overzicht internetfraude VS 2001

	percentage	gemiddelde schade
Online Auctions	63%	$478
General Merchandise Sale	11%	$845
Nigerian Money Offers	9%	$6.542
Internet Access Services	3%	$568
Information Adult Service	3%	$234
Computer Equipment/Software	2%	$1.102
Work-At-Home	2%	$120
Advance Fee Loans	1%	?
Credit Card Issuing	0,6%	?
Business Opportunities and Franchises	0,4%	?

Uit deze tabel wordt duidelijk dat in de toptien van internet fraudes de online veilingen en online winkelen op nummer 1 en 2 staan , met 63% respectievelijk 11% van de alle gemelde fraudegevallen.

Een indrukwekkend overzicht van de misleidingschema's waarmee mensen bedrogen worden, inclusief die gevallen waarbij cyber-middelen ingezet worden, is te vinden op www.crimes-of-persuasion.com. Dit overzicht toont enerzijds de inventiviteit bij de bedenkers van deze criminaliteit en anderzijds de soms grote naïviteit bij de slachtoffers. Een willekeurig voorbeeld:

"Aspiring writers who place their hopes and dreams into the hands of fraudulent literary agents and publishing companies are often deceived into paying for an over-priced editing service, lied to about the qualifications of the editors, misled about the potential for acceptance by a publishing company, and ultimately rejected by fictitious literary agents or publishing houses.
The dreams and aspirations of unpublished writers make them an easy mark, falling for half-truths and dubious incentives. A recent investigation of one company showed $10 million had been paid by 6000 would-be authors seeking help getting their manuscripts edited and published while another company was ordered to pay $5 million in restitution to 4000 writers who used the services of these so-called "vanity presses", "book doctors" or "literary agents", which are noted for charging up-front fees but never delivering on their promises of fame, fortune and notoriety.
Writers are encouraged to believe that putting a book together is the quickest avenue to self-esteem, but after being duped, suffer a shame compounded by years of rejection letters from mainstream publishers. These companies take elaborate measures to disguise both the fact it is a vanity press and that most bookstores will simply not stock vanity press offerings."

In een variatie op dit schema worden mensen vooraf geld gevraagd voor publicatie op een 'belangrijke website'.

2.5.1.2 Gokken, 'snel geld schema's', piramidespelen, kettingbrieven

Waar de overheid gokken in de fysieke wereld reguleert, is een dergelijke regulering voor gokken via internet veel moeilijker gebleken. Op de derde plaats van de toptien van internet fraude staat met 9% van de gevallen de tamelijk klassieke Nigeriaanse aanbiedingen, die kennelijk toch veel slachtoffers maken. De bekende piramide spelen blijken ook in het virtuele domein geld op te brengen voor hen die het spel starten.

Een speciale vorm van kettingbrieven is aan een ieder met een E-mail account bekend. Regelmatig wordt men gewaarschuwd voor de komst van een computervirus (bijvoorbeeld het virus GoodTimes, dat nooit bestaan heeft) en wordt een vaak emotioneel beroep gedaan op de ontvanger om dit bericht door te geven aan vrienden en bekenden.
Op gelijke wijze circuleren berichten over vermiste of ernstig zieke kinderen. In 90% van de gevallen is sprake van misplaatste grappen (hoaxes), die op

het eerste gezicht onschuldig ogen, maar toch voor veel ophef en verlies van productieve uren kunnen zorgen.

2.5.1.3 Aannemen van valse identiteit

Diefstal van de identiteit (identity theft) stelt de dader in staat om met de persoonsgegevens van een ander creditcards aan te vragen, bestaande rekening over te nemen of leningen aan te gaan in naam van de ander. In de Verenigde Staten zijn 700.000 personen per jaar slachtoffer van deze vorm van criminaliteit[6].

Bij fraude op basis van identiteit wordt vaak tijdelijk gebruik gemaakt van de rechten die een ander heeft. Bijvoorbeeld het uitlenen van ziekenfondskaarten door legale vluchtelingen aan illegale vreemdelingen.
Een speciale manier van identiteitsfraude wordt gepleegd door lieden die domeinnamen registreren die lijken op een foutief gespelde reguliere domeinnaam, bijv. Disney. Argeloze bezoekers, waaronder kinderen, worden dan ofwel direct geconfronteerd met frauduleuze aanbiedingen of pornografisch materiaal, of worden gelokt door middel van een hyperlink naar een internetsite van het criminele bedrijf. Eén persoon had 130 varianten geregistreerd op een domeinnaam en is veroordeeld voor het tegen hun wil ophouden in CyberSpace van bezoekers. Het beeldscherm van de bezoeker vulde zich in kortste keren met 30 pop-up windows, die zeer hardnekkig terug bleven komen na wegklikken.

2.5.2 Aantasten persoonlijke levenssfeer

Cyberstalking
Artikel 426bis van het wetboek van Strafrecht definieert stalken als "Hij die wederrechtelijk op de openbare weg een ander in zijn vrijheid van beweging belemmert of met een of meer anderen zich aan een ander tegen diens uitdrukkelijk verklaarde wil blijft opdringen of hem op hinderlijke wijze blijft volgen."

Cyberstalking profiteert van de anonimiteit en van het gemak van verzending via Internet of SMS van bedreigingen. Een dergelijke bedreiging is fysiek minder bedreigend, maar het psychologisch effect is vrijwel even groot en vaak wordt zo een bedreiging gevolgd door een fysieke dreiging of door geweld. Een rapport van het Amerikaanse openbaar ministerie aan voormalig vicepresident Al Gore[7] geeft een goed overzicht van het probleem en somt de volgende overeenkomsten en verschillen op tussen stalking in de fysieke en de virtuele wereld:

Noot 6 Zie ook http://www.idtheftcenter.org/, laatst geraadpleegd op 24 april 2002
Noot 7 te vinden op (laatst geraadpleegd op 24 april 2002:
http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

Major Similarities

- Majority of cases involve stalking by former intimates, although stranger stalking occurs in the real world and in cyberspace.
- Most victims are women; most stalkers are men.
- Stalkers are generally motivated by the desire to control the victim.

Major Differences

- Offline stalking generally requires the perpetrator and the victim to be located in the same geographic area; cyberstalkers may be located across the street or across the country.
- Electronic communications technologies also lower the barriers to harassment and threats; a cyberstalker does not need to physically confront the victim.
- Electronic communications technologies make it much easier for a cyberstalker to encourage third parties to harass and/or threaten a victim (e.g., impersonating the victim and posting inflammatory messages to bulletin boards and in chat rooms, causing viewers of that message to send threatening messages back to the victim "author.")

Verdere voorbeelden van cyberstalking zijn:

A cyberstalker may send repeated, threatening, or harassing messages by the simple push of a button; more sophisticated cyberstalkers use programs to send messages at regular or random intervals without being physically present at the computer terminal. California law enforcement authorities say they have encountered situations where a victim repeatedly receives the message "187" on their pagers - the section of the California Penal Code for murder. In addition, a cyberstalker can dupe other Internet users into harassing or threatening a victim by utilizing Internet bulletin boards or chat rooms. For example, a stalker may post a controversial or enticing message on the board under the name, phone number, or e-mail address of the victim, resulting in subsequent responses being sent to the victim. Each message -- whether from the actual cyberstalker or others -- will have the intended effect on the victim, but the cyberstalker's effort is minimal and the lack of direct contact between the cyberstalker and the victim can make it difficult for law enforcement to identify, locate, and arrest the offender.

Intimidatie / Afdreiging

Deelname aan discussiegroepen en chat-sessies, maar ook uitwisseling van E-mail adressen, kan het gevaar opleveren van ongewenste intimiteiten of anderszins intimiderende uitingen. Met name kinderen zijn kwetsbaar, bijvoorbeeld als zij gevraagd worden om hun telefoonnummer of adres te geven.

Onlangs is een Nederlander aangehouden in de Verenigde Staten nadat hij in een 'chat-val' is gelokt door een politiefunctionaris die zich voordeed als een minderjarig meisje, waarmee de Nederlander seksuele intenties zou hebben. Dit is een goed voorbeeld van de complicaties die cybercrime oproept: een Nederlander wordt naar de Verenigde Staten gelokt met een opsporingsmethode die in Nederland niet toegestaan wordt in het Wetboek van Strafvordering.

2.5.3 Vermogensdelicten overwegend gericht tegen organisaties en bedrijven

Naast de vormen van criminaliteit die al in de eerdere paragrafen van dit hoofdstuk zijn genoemd, kunnen bedrijven ook slachtoffer worden van de onderstaande delicten.

Bedrijfsspionage
Bedrijfsspionage met cyber-middelen kan plaatsvinden op drie manieren:

- Verzending vanuit het bedrijf door medewerkers. Bedrijfsgeheimen kunnen verstuurd worden, maar ook minder flatteuze insider informatie komt op deze manier naar buiten, geventileerd door ontevreden maar verder niet-criminele medewerkers.
  Het kan ook voorkomen dat medewerkers in de vaak informele E-mail contacten met klanten of toeleveranciers toezeggingen doen die commerciële schade opleveren.
- Aanvallen van buitenaf. Het betreft hier het klassieke beeld van de malafide hacker of organisatie die bedrijfsgeheimen achterhaalt via toegang tot de databestanden. Het gaat dan om informatie over productenspecificatie, productieprocessen, klantenbestanden, offertes en onderhandelingstrajecten.
- Het onderscheppen van communicatie. Het ECHELON netwerk van afluisterstations, verondersteld te worden onderhouden door de Angelsaksische landen, zou het vergaren van bedrijfsinformatie als één van de doelstellingen hebben. Airbus Industries zou bijvoorbeeld een grote order verloren hebben aan Boeing nadat informatie over lopende onderhandelingen doorgespeeld was aan Boeing[8].

Inbreuk op auteursrechten en ontduiken van licentiegelden
Afgaande op de statistieken die door internetzoekmachines ('search engines') bijgehouden worden omtrent de meest gezochte internet sites, is het zoeken naar illegale software ('warez' in Internet jargon) op gelijke hoogte gekomen met het zoeken naar seks en MP3 bestanden. Het gaat dan bijvoorbeeld om het totale Microsoft Windows besturingssysteem of het totale Office pakket, die gekraakt zijn en tegen een lage prijs of gratis worden aangeboden. Ook binnen zogenaamde peer-to-peer netwerken (Kazaa, Napster) wordt volop gepirateerde software uitgewisseld.

Ontregelen en doorgronden van interne werking van digitale apparatuur
Digitale elektronica wordt in toenemende mate ingezet bij sloten en voor bewakingsdoeleinden. Als de interne werking van deze digitale elektronica achterhaald kan worden, is het soms mogelijk om het slot te ontsluiten. In andere gevallen kan met gericht geweld tegen de kwetsbare elektronische componenten of met het ontregelen van de telecommunicatievoorziening de bewaking uitgeschakeld worden.

Digitaal knoeien met registratie apparatuur
Ook knoeien met registratie apparatuur was mogelijk lang voor de komst van elektronische apparatuur, getuige het arrest van de Hoge Raad uit 1921 handelende over diefstal van elektriciteit door de meter te blokkeren met een pen (NJ 1921, 564). Ook het terugdraaien van de kilometerteller van een auto is een oud ambacht.

Tegenwoordig wordt digitale registratie toegepast in gas- en elektrameters, kilometertellers en de taximeters. Ook bij de aflevering van gassen en vloeistoffen (bijvoorbeeld een tankstation) of bij de bepaling van de samenstelling daarvan wordt digitale registratie apparatuur ingezet. Op al deze toepassingsgebieden is er inmiddels wel eens geknoeid met de apparatuur of is men op zijn minst wel op het idee gekomen.

Noot 8 onder andere genoemd op: (laatst geraadpleegd op 24 april 2002)
http://www.iptvreports.mcmail.com/ic2kreport.htm#N_70_

Manipulatie van draadloze (bijv. DECT) telefoons
In oude types draadloze telefoons konden anderen middels hun handset zich aanmelden bij een basisstation en bellen op de kosten van dat basisstation. Moderne DECT telefoons zijn daartegen beschermd middels PIN codes, maar waarschijnlijk is het merendeel van de in gebruik zijnde DECT telefoons in huizen of kantoren ingesteld op de fabrieksingestelde PIN code. Aldus kan toch gebeld worden op kosten van een ander, of kan communicatie onderschept worden.

Soms zijn mobiele telefoons kwetsbaar voor ingrijpen via het netwerk. Zo zouden GSM telefoons opengezet kunnen worden (off-hook) door bepaalde signalen vanuit het netwerk, en aldus kunnen dienen als handige afluistermicrofoon. Ook zouden bepaalde SMS berichten schade kunnen aanrichten. Er zijn hiernaast berichten dat de *waarschuwingen* tegen schadelijke SMS berichten onecht zijn en opgevat moet worden als een 'hoax'.

Nevenactiviteiten medewerkers
Het zonder toestemming privé gebruik van computers en internet door werknemers onder werktijd kan eigenlijk niet gerekend worden onder criminaliteit. Toch kan dit leiden tot een grote schadepost voor werkgevers en verdient alleen daarom al aandacht. De gedragsnorm voor wat acceptabel is en wat niet verschilt sterk per organisatie, sociaal-cultureel verband of land. Deze gedragsnormen zijn ook voor een groot gedeelte niet voldoende ontwikkeld binnen de maatschappij.

2.5.4 Aantasten reputatie van bedrijf

Marktmanipulatie en reputatie schade via verspreiden (valse) informatie
Bij dit vermogensdelict worden via Internet geruchten verspreid over een bedrijf, bijvoorbeeld over een aanstaande overname, interne problemen of een schadeclaim. Middels aandelen- of optiehandel met voorkennis kan dan geldelijk gewin worden behaald.
Geruchten en valse informatie kunnen ook reputatieschade opleveren voor bedrijven. Eventueel kan één en ander vergezeld gaan van afpersing.
Er zijn ook talloze gevallen waarin ex-medewerkers zich via een website in rancune verenigen bij het etaleren van de vuile was over hun voormalige werkgever.

2.5.5 Aantasten publieke moraliteit

Seks en kinderporno
Naar verluid zou de helft van de alle bezoeken aan websites te maken hebben met seks[9]. In het Westen is hiertegen overwegend weinig bezwaar, zolang het geen kinderporno betreft. Het verspreiden van kinderporno is wellicht het meest bekende voorbeeld van criminaliteit vergemakkelijkt door Internet en E-mail.

Aanzetten tot discriminatie
E-mail berichten worden vaak verkeerd begrepen en ontaarden soms nietsontziende polemieken. Nieuwsgroepen staan bekend om hun soms ellenlang uitgesponnen scheldpartijen, waarbij afstand en anonimiteit alle

Noot 9 Zie http://www.nytimes.com/library/national/science/health/051600hth-behavior-cybersex.html, laatst geraadpleegd op 24 april 2002.

terughoudendheid wegnemen. In opkomst zijn ook zogenaamde Hate Sites, die opruien tot religieuze, raciale, etnische en seksuele discriminatie[10].

Verspreiden van gevaarlijke informatie
Het tegengaan van het verspreiden van (zogenaamd) gevaarlijke informatie lijkt voorbehouden aan totalitaire regimes. Toch speelde dit nog onlangs in Nederland toen informatie over het bewerken en verspreiden van de Anthrax bacterie beschikbaar kwam op de site van Planet Internet.

Citaat van http://tecsoc.org/culture/culture.htm, geraadpleegd .

"Some governments see it as their duty to eradicate sentiments and publications they deem offensive or illegal -- but that is extremely difficult when the prohibited materials are online. A French court ordered Yahoo to make Nazi-related materials on its sites inaccessible to French citizens. Germany's highest court decided that even foreigners who post online materials illegal in Germany can be held accountable under German law. Is it feasible for countries to block off undesirable portions of the Internet? There is some speculation that fear of "subversive" information online is one reason China is planning its own separate Internet."

In de meer bizarre categorie valt de melding van jongeren in Zuid-Korea die zouden zijn aangezet tot zelfmoord middels gedetailleerde informatie hierover op het internet.

Overige
Er zijn nog vele verschijningsvormen die in deze paragraaf genoemd kunnen worden. Bijvoorbeeld het platleggen van de servers die gebruikt werden voor de chatsessie op Internet die kroonprins Willem-Alexander en Maxima een aantal dagen voor hun huwelijk hielden[11]. Dit incident heeft naast directe schade ook tot gevolg dat het vertrouwen dat burgers in de veiligheid in het virtuele domein hebben, aangetast wordt.

Noot 10 Zie ook http://www.civilrights.org/issues/hate/, laatst geraadpleegd op 24 april 2002.
Noot 11 KPN was technisch verantwoordelijk hiervoor en gaf aan dat er ruim drie *miljard* informatie-aanvragen naar de server werden gestuurd. Dat is ongeveer 190 aanvragen per Nederlander.

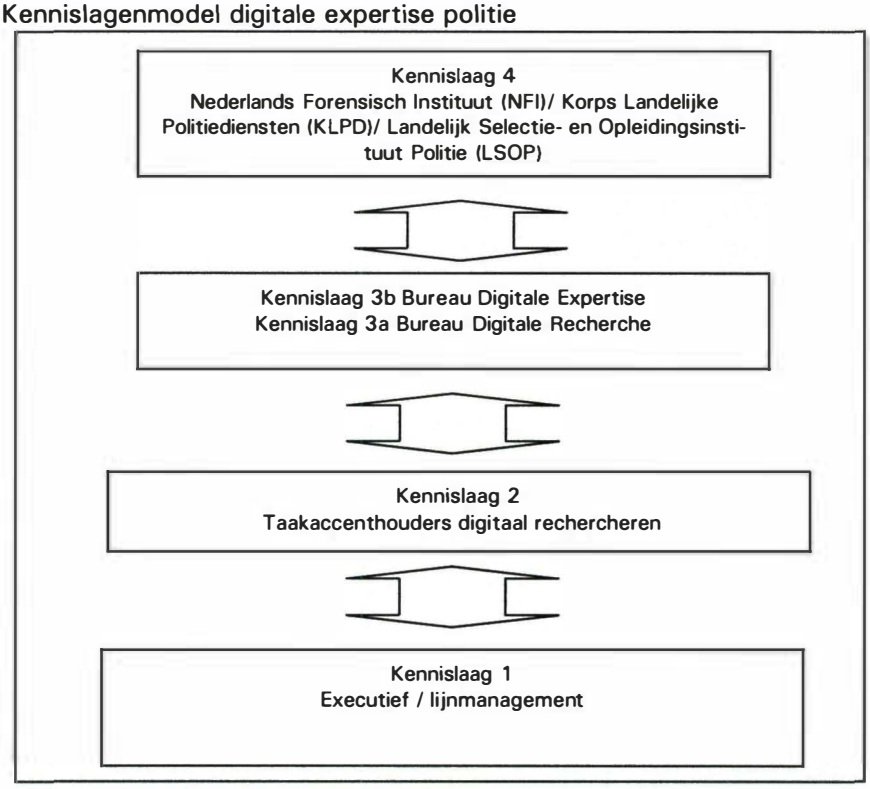
3 Gevolgen voor de aanpak van Cybercrime

In het voorgaande hoofdstuk is al aangegeven dat de digitalisering van de criminaliteit nieuwe mogelijkheden biedt. In dit hoofdstuk wordt nader ingegaan op de gevolgen hiervan voor de *aanpak* van criminaliteit in de virtuele ruimte.
Allereerst zal de huidige stand van zaken rond de organisatie van de aanpak van cybercrime bij voornamelijk de Nederlandse politie worden beschreven. Daarna worden per specifiek effect van de digitalisering van de criminaliteit (zoals beschreven in het voorgaande hoofdstuk) de gevolgen voor de opsporing beschreven.

3.1 Organisatie van de aanpak: stand van zaken bij de politie

Toen in begin jaren '90 duidelijk werd dat de politie de nodige kennis en ervaring ontbeerde om goed om te gaan met de ook toen al toenemende digitalisering van de maatschappij werden de Bureaus Digitale Expertise (BDE) opgericht. In de loop der jaren is op dit terrein al heel wat bereikt. Wat begon als een pilotproject in de politieregio's Amsterdam, Oost- Nederland en Den Haag, is inmiddels uitgegroeid tot een netwerk van zo'n 7 bureaus in het land, centrale eenheden die onder de Korps Landelijke Politiediensten (KLPD) vallen en centrale expertise die voornamelijk bij het Nederlands Forensisch Instituut (NFI; voorheen Gerechtelijk Laboratorium) ligt. Hieronder wordt de organisatie van de digitale recherche gepresenteerd aan de hand van het zogenaamde 'kennislagenmodel'. Volgens dit model wordt de kennis binnen de politie georganiseerd in vier lagen, weergegeven in figuur 3.1:

Figuur 3.1 Kennislagenmodel digitale expertise politie



Binnen dit model bevind de meest specialistische kennis en kunde zich bovenin. Het NFI heeft voornamelijk hoog opgeleid personeel dat is gespecialiseerd op vele terreinen. Eén van deze terreinen is het digitale forensisch onderzoek. Zij ontwikkelen, vaak samen met praktijkmensen van de BDE's, nieuwe methoden en technieken en ondersteunen de BDE's in lopende onderzoeken. Hiernaast werkt het NFI samen met andere informatie- en veiligheidsdiensten.

Zoals gezegd kent ons land 7 BDE's. De grootte van de BDE's varieert. Afhankelijk van het aantal politieregio's dat 'bediend' wordt varieert de grootte van 3 tot 5 mensen bij de BDE zelf. Daarnaast werken tussen de 10 en 20 mensen per BDE verdeeld over de politieregio's of districten. De wijze waarop de mensen in de regio's worden aangestuurd verschilt sterk. In sommige regio's hebben de digitale rechercheurs de *functie* van digitaal rechercheur, in andere regio's bestaan alleen taakaccenthouders digitale recherche. Dit heeft verregaande consequenties voor de inzet van de digitale rechercheur. Waar taakaccenthouders nogal eens kunnen worden opgeslokt door hun andere werkzaamheden, houden 'fulltime' digitale rechercheurs zich alleen met digitale recherche bezig.
De medewerkers van de BDE's worden over het algemeen geworven onder 'gewone' rechercheur, met affiniteit op het gebied van computers. De nadruk ligt hierbij echter wel op de recherchevaardigheden van de medewerkers en bijzondere interesse in het vakgebied van de ICT. Naast deze interne werving worden ook mensen van buiten de politieorganisatie aangetrokken; vaak zijn dit IT-specialisten. De toekomstige BDE-medewerkers krijgen een standaard opleiding waaronder een cursus 'digitaal rechercheren' bij het LSOP. Eventuele vervolgopleidingen en terugkomcursussen kunnen worden gevolgd afhankelijk van de mogelijkheden binnen en behoeften van de regio.

Er wordt naar gestreefd om bij alle 26 politieregio's binnen Nederland een eigen Bureau Digitale Recherche (BDR) op te zetten. De rechercheurs die bij de BDR werkzaam zijn, doen het feitelijke werk van de opsporing van virtuele criminaliteit ('draaien zaken') of ondersteunen recherche teams die met de opsporing bezig zijn van een zaak waaraan een digitale component zit.
De onderste twee lagen van het model worden gevuld door de reguliere politiemedewerkers. Hierbij hebben veelal alleen de taakaccenthouders basiskennis over digitaal onderzoek.

3.1.1 Kennis

Het kennislagenmodel heeft een statisch en een dynamisch karakter. *Statisch* omdat de uitgangspunten van het model en de partijen die daarbij zijn betrokken nagenoeg vaststaat. *Dynamisch* omdat de inhoud van het model, te weten kennis, door het model heen beweegt. De ontwikkeling van kennis op het gebied van de informatica en de aanpak van virtuele criminaliteit gaat zeer snel. De innovaties die plaatsvinden bij het NFI en KLPD en worden direct bij de BDE's neergelegd. Wanneer deze technieken en methoden op grote schaal gebruikt worden, wordt de benodigde kennis en kunde bij de BDR's en de taakaccenthouders uitgezet. Uiteindelijk is het de bedoeling dat bepaalde zeer veel toegepaste technieken ook terechtkomen op het niveau van de executieve diensten. Een goed voorbeeld hiervan is het uitlezen van mobiele telefoons. Zo werden SIM kaarten van mobiel telefoons vroeger uitgelezen bij het NFI; tegenwoordig kunnen de BDE's of de digitale rechercheurs in de regio's dit veelal zelf, eventueel met hulp van de BDE's. Gezien de verspreiding van de GSM in al zijn toepassingen is het denkbaar dat in de (nabije) toekomst

deze taken, bijna geheel geautomatiseerd, neergelegd worden bij de executieve diensten van de politie.

Bij het grootste deel van de BDE's in het land is deze opzet al realiteit of zal dit binnenkort het geval zijn. De meest voorkomende werkzaamheden kunnen door de digitale rechercheurs in de districten of de regio's worden gedaan. Het uitlezen van SIM kaarten en 'huis-tuin-en-keuken harde schijven' moet voor deze rechercheurs geen problemen opleveren. Voor het meer specialistische werk wordt de expertise die aanwezig is op de BDE benut. Men kan hierbij denken aan meer exotische bestandssystemen op harde schijven die gebruikt worden door Linux en MacOS besturingssystemen of gesloten systemen als organisers. Soms komt een BDE bestanden of closed- systemen tegen die zodanig versleuteld, beveiligd of beschadigd zijn (een gecrashte harde schijf bijvoorbeeld) dat zij er zelf niets mee kunnen aanvangen. Deze zaken worden op hun beurt door het NFI aangenomen. Het NFI beschikt over drie groepen waar voor een groot deel ontwikkelwerk wordt gedaan, maar waar ook complexe zaken worden afgehandeld. In de groep Gesloten Systemen wordt onderzoek gedaan naar bijvoorbeeld organisers, auto-electronica, gokautomaten, taximeters, etc. De groep Open Systemen van het NFI houdt zich meer bezig met computers, netwerken, enzovoort . Hiernaast bestaat er nog een groep Beeldbewerking. Zij onderzoeken onder andere beeldmanipulatie, doen animatie van crimescènes, etc.
Zaken bewegen zich dynamisch door het kennislagenmodel op en neer afhankelijk van de kennis die nodig is om een specifiek probleem op te lossen. Hierbij moet worden opgemerkt dat de hier geschetste werking van het model niet voor alle zaken en binnen alle politieregio's onproblematisch verloopt. Niet altijd vinden zaken of collega's hun weg naar de politiemensen met de benodigde digitale expertise.

Hiervoor werd al kort gesproken over de wijze waarop met name de BDE's aan hun digitale rechercheurs komen. Wanneer we over kennismanagement spreken is het van belang te constateren dat een aantal BDE's en ook het NFI de laatste paar jaar te kampen heeft gehad met een groot verloop van personeel. Deze mensen stromen voornamelijk uit naar het bedrijfsleven. Ook andere overheidsdiensten hebben in de 'Internet- boom' van de laatste drie jaar veel van hun 'digitale specialisten' verloren. Men verwacht dat dit met het afkoelen van de economie steeds minder een probleem zal zijn. Hierbij komt dat vanuit overwegingen van maatschappelijke betrokkenheid voor een groot aantal mensen de politie altijd een aantrekkelijke werkgever zal zijn. Aan de andere kant is er ook in het bedrijfsleven nog steeds zeer veel vraag naar mensen met kennis en kunde van (computer)beveiliging, dus het werven van goed personeel zal moeilijk blijven voor de politie.
Voor het opbouwen van expertise en kunde is het uiteraard wenselijk, mensen geruime tijd werkzaam te laten zijn op het gebied van digitaal recherchëren. Daarnaast is het up-to-date houden van kennis door voldoende en tijdige bijscholing essentieel.

3.1.2 Werkzaamheden

De werkzaamheden van de digitale rechercheurs behelzen voornamelijk het op een forensisch verantwoorde manier veiligstellen van digitaal sporenmateriaal in 'gewone' strafzaken. Hierbij kan men denken aan de gegevens die staan opgeslagen op harde schijven van computers, SIM- kaarten (met belgegevens en telefoonboeken) van GSM- telefoon, adresboeken in elektronische organisers, maar ook 'gesloten systemen' als taximeters,

gokautomaten, etc. Het soort sporenmateriaal dat men tegenkomt hangt sterk af van de soort strafzaak: bij een fraudezaak kan het bijvoorbeeld gaan om het
veiligstellen van administratie die op de harde schijf van een computer ligt opgeslagen.
Bij een zaak tegen een drugsdealer kunnen weer grote hoeveelheid SIM- kaarten en mobiele telefoons worden aangetroffen. Ter illustratie een globaal overzicht van de aantallen en soorten zaken van het BDE Oost over het jaar 2001. Dit overzicht is redelijk representatief voor de verdelingen die wij bij andere BDE's hebben aangetroffen, zij het dat er geen standaard- systeem blijkt te bestaan bij de BDE's om zaken te classificeren. Zo hebben de BDE's ieder een eigen 'systeem' om hun zaken in te registreren. Hierbij is (nog) geen aandacht besteed aan een duidelijke definitie van bepaalde delictcategorieën, zodat deze tussen de BDE's verschillen.

Tabel 3.1 Verdeling soorten zaken BDE Oost 2001

Soort zaak	aantal	procent
diefstal/ heling/etc.	149	18
drugs	108	13
fraude	43	5
gewelddelicten	148	18
hacking	28	3
internetgerelateerd	73	9
kinderporno	56	7
milieu	2	0
oplichting	17	2
virus	10	1
overige	179	22
totaal	813	100

Bij deze tabel moet allereerst de opmerking worden geplaatst dat vergelijking met veel andere politiegegevens mank gaat. Het draaien van een zaak door een BDE of BDR is vaak een veel tijd, capaciteit en inspanning rovende zaak. De digitale onderzoeken die men doet, en de verslaglegging achteraf, kosten veel meer aan tijd en werkuren dan andere onderzoeken.

Uit deze tabel is meteen af te leiden dat het aandeel 'nieuwe criminaliteit', zijnde criminaliteit tegen en met behulp van computers (DoS[12]- aanvallen, hacking, etc.) relatief laag is. De meeste zaken betreffen 'traditionele criminaliteit', waarbij min of meer toevalligerwijze digitale aspecten een rol spelen.

De werkdruk van het personeel bij de BDE's wordt door de meeste geïnterviewden omschreven als hoog tot zeer hoog. Er ligt zowel op de medewerkers binnen de korpsen / districten als bij de BDE's zelf een constante druk om zeer veel 'zaken te draaien'. Zo blijft er minder tijd over voor het bijscholen van de medewerkers. Idealiter zouden de medewerkers van de BDE's zich tussen 10% en 30% van hun tijd moeten bezig kunnen houden met Research & Development (R&D) op allerlei gebied. Dit is door de werkdruk niet altijd mogelijk.

De hoge werkdruk is wellicht één van de redenen dat de inspanning die gepleegd wordt, of kan worden op 'nieuwe vormen van criminaliteit' door de

Noot 12 Een DoS aanval staat voor 'Denial of Service': een computer wordt platgelegd door er zoveel verzoeken tot informatie op af te sturen dat deze het niet meer aan kan en 'verstopt' raakt. Computers die webpagina's bevatten zijn nogal eens doelwit van een dergelijke aanval; de website kan dan door niemand meer bereikt worden.

BDE's op een laag pitje staat. Hierbij speelt ook een rol dat hack-zaken, bedreigingen via e-mail, etc. over het algemeen niet erg hoog scoren in het case-screeningmodel in termen van aantoonbare schade of gevolgen. Eén hoofd van een BDE verwoordde dit treffend door te stellen dat in sommige korpsen zelfs wel eens verkrachtingszaken blijven liggen door gebrek aan capaciteit. Dan wordt het moeilijk om een hacking-zaak door het case-screeningmodel te laten komen. De enige soort zaken waarbij de digitale component een belangrijke rol kan spelen en die ook vanuit de korpsleiding en politiek de nodige prioriteit hebben gekregen zijn de zaken waarbij kinderporno met behulp van computernetwerken wordt verspreid.

Toch geven een aantal BDE's aan soms wel hack-zaken op te volgen, ondanks dat deze niet door het case-screeningsmodel[13] zouden komen. De reden hiervoor is vooral dat het voor de betreffende rechercheurs vaak erg veel voldoening geeft een dergelijke zaak uit te voeren. Ook gebruikt men deze zaken om expertise te verkrijgen en te behouden.

De hoofden van de BDE's verwachten de komende jaren vooral een toename van het aantal hacking- en DoS- aanvallen en andere 'netwerkcriminaliteit'. Om een chef van een BDE te citeren: 'het wordt alleen maar meer'. Dit komt enerzijds door het feit dat er steeds meer mensen over een 'always-on' internetverbinding (Kabel, ADSL) beschikken; anderzijds, omdat de gemiddelde internetter nog weinig maatregelen neemt om zijn of haar computer en gegevens te beschermen tegen deze aanvallen. Er is hierover nog veel voorlichting aan 'het grote publiek' noodzakelijk. De overheid heeft inmiddels de eerste stappen gezet op dit gebied door middel van de 'surf op safe'-campagne.

Hiernaast werd door de hoofden BDE's de opkomst van Linux als besturingssysteem voor PC's, en de mogelijkheid van het inbreken op draadloze bedrijfsnetwerken (W-Lan's) als mogelijkheden voor zogenaamd 'drive-by hacking' genoemd als nieuwe trends voor de nabije toekomst.

3.1.3 Aangiften

Zoals wij al in het beginstadium van het onderzoek vermoedden is de aangiftebereidheid van vooral 'nieuwe vormen' van computercriminaliteit laag. In het bedrijfsleven is men na een hack-poging vaak bang voor mogelijk imagoschending als de zaak in de publiciteit komt. Ook zijn zij vaak niet bereid de regie van de vervolging af te staan aan de politie of het OM. De hoofden van de BDE's menen dat hierin de laatste tijd wel enige verbetering komt: vooral ISP's doen nu nogal eens aangifte van hack-zaken. Hoe meer kennis van de werking van de politie in dit soort zaken er bij deze organisaties is, hoe groter vaak de aangiftebereidheid.

Een ander knelpunt waar zowel particulieren als bedrijven bij het doen van aangifte tegen aan lopen is het feit dat veel medewerkers in de basis politiezorg soms niet goed weten waar zij met een aangifte van computercriminaliteit heen moeten. De kennis bij de mensen aan de balie of op straat op het gebied van computercriminaliteit is hiervoor gewoon te laag. Aangevers worden niet altijd verwezen naar de Bureau's Digitale Recherche (BDR) of de aangifte wordt eenvoudigweg niet opgenomen. Bij systeembeheerders van

Noot 13 Het cas-screeningsmodel is een set van criteria waarop binnen de politie prioriteit gegeven wordt aan de zaken die binnenkomen. Hoe hoger in dit model, hoe meer prioriteit en dus meer capaciteit aan een dergelijke zaak wordt gegeven binnen de politie.

organisaties komt daar nog eens bij dat zij idealiter willen spreken met een politieman met een zelfde (informatica)technische achtergrond of kennisniveau. Ook dit gebeurt lang niet altijd of is niet altijd mogelijk waardoor soms aangevers afhaken.

3.1.4 Registraties

Binnen dit onderzoek is onderzocht wat er bij de BDE's werd bijgehouden aan cijfers en statistieken over hun werkzaamheden. Het doel hiervan was om te inventariseren of deze cijfers geschikt zijn om een indruk te krijgen van de omvang van criminaliteit in de virtuele ruimte. Het blijkt echter dat de registraties van de BDE's totaal niet geschikt zijn voor dit doel. In de eerste plaats verschillen de registraties tussen de verschillende BDE's onderling te sterk. Er worden verschillende categorieseringen en methoden om te tellen gehanteerd. Hiernaast loopt de gedetailleerdheid van de rapportage van de BDE's onderling uiteen. Zo brengt BDE Oost al geruime tijd een jaarverslag uit, andere regio's kunnen een dergelijke rapportage in het geheel niet leveren.
Door de meeste BDE's wordt, gezien de aard van het werk, wel een registratie bijgehouden van de soorten voorwerpen die worden onderzocht (aantal PC's, SIM- kaarten, harde schijven, organisers, enzovoorts). Hiervan kunnen door een aantal BDE's ook vrij gemakkelijk overzichten worden gegenereerd. Een overzicht van de aantallen en soort zaken die wordt bijgehouden kan aan de hand van dergelijke overzichten echter niet gegenereerd worden.

Ook het feit dat cybercrime in BPS en HKS niet als zodanig wordt geregistreerd en niet kan worden onderscheiden, draagt bij aan het ontbreken van zicht op de aantallen zaken waarbij de politie te maken krijgt met criminaliteit met een digitaal aspect. Het eerder gesignaleerde feit dat het nogal eens ontbreekt aan kennis om aangiften van bijvoorbeeld hack-zaken op te nemen, levert ook geen positieve bijdrage aan de kwaliteit van de registratie van computercriminaliteit. Om deze reden is er, nog afgezien van het 'dark number' van de niet bij de politie bekende criminaliteit in de virtuele ruimte, geen reden om aan te nemen dat er aan de hand van politieregistraties een betrouwbaar beeld gevormd kan worden van de omvang van de criminaliteit in de virtuele ruimte.

3.1.5 Knelpunten, kansen en ontwikkelingen voor de BDE's

Het eerste grote knelpunt dat genoemd wordt is het feit de BDE's op veel terreinen nog een voorhoedefunctie vervullen. De digitale aspecten van de aanpak van criminaliteit zijn nog niet in de hele politieorganisatie doorgedrongen. Dit begint aan de basis bij de functionarissen van de basis politiezorg. Maar ook aan de top van de korpsen heeft men eenvoudigweg te weinig kennis van computers en digitale aspecten van criminaliteit. Hierdoor gaat er voor de hoofden BDE veel tijd zitten in het veiligstellen van budgetten, menskracht, etc. Ook wordt er gesignaleerd dat de vanuit of aan de politie opgelegde leuze voor 'meer blauw op straat' ten koste gaat van allerlei zaken die de korpsleiding ziet als ondersteuning. Ook de BDE's vallen hieronder. Een voorbeeld hiervan is te vinden bij de BDE Noord, waar het budget voor de afdeling sinds 1994 hetzelfde is gebleven.

Het andere grote knelpunt is de hoge werkdruk en de grote hoeveelheid tijd die men kwijt is aan de schriftelijke vastlegging van werkzaamheden. Hierdoor komt de ontwikkeling en (bij)scholing van de medewerkers van de

BDE's vaak in de knel. Zo komt er van het up-to-date houden van kennis van medewerkers te weinig terecht.
Daarnaast zijn de ideeën over de rol van bijvoorbeeld de taakaccenthouder versus de functie van digitale rechercheur nog niet overal goed uitgekristalliseerd. Ook hierbij komt vaak het uiteindelijke kennisniveau dat gewenst wordt voor een bepaalde positie in het kennislagenmodel in het gedrang.

3.2 De organisatie van de opsporing: andere opsporingsdiensten

Naast de politie is er een aantal andere organisaties die zich bezighoudt met opsporings en preventiewerkzaamheden met betrekking tot criminaliteit in de virtuele ruimte. In de eerste plaats worden hier de activiteiten van een aantal Bijzondere Opsporingsdiensten besproken te weten de Opsporingsdienst Buma Stemra (ODBS) en de Fiscale Inlichtingen en Opsporingsdienst (FIOD). Hiernaast zijn er binnen het bedrijfsleven nog een aantal partijen op dit gebied werkzaam. Wij zijn hiervoor te rade gegaan bij een aantal contactpersonen bij banken, creditcardmaatschappijen en de forensische accountancy. Er zal bij deze bespreking aandacht worden besteed aan de relatie die de private partijen hebben met het opsporingswerk van de politie. Hiernaast is in kaart gebracht in hoeverre het dagelijks werk van deze opsporingsdiensten verandert met betrekking tot de aspecten van digitalisering die zijn geschetst in hoofdstuk 2.

3.2.1 Opsporingsdienst Buma-Stemra (OBDS)

De OBDS is ontstaan als private organisatie met een specifieke opsporingstaak waarbij de activiteiten worden betaald door de branche zelf. De opsporingsactiviteiten van de Buma-Stemra richten zich hoofdzakelijk op schendingen van het auteursrecht en naburige rechten op het gebied van muziek, interactieve software, en video en filmbeelden. De opsporing is feitelijk georganiseerd in twee gedeelten. De stichting Brein, onderdeel van de OBDS, houdt zich bezig met de civiele opsporing en aanpak van schendingen van auteursrecht. De OBDS is belast met het strafrechtelijke traject onder verantwoordelijkheid en toezicht van het OM. Er wordt bij internetgerelateerde zaken meestal eerst een civielrechtelijk traject begonnen. Heeft dit niet genoeg effect dan wordt de OBDS ingeschakeld. De strafrechtelijke opsporing is een veel arbeidsintensiever traject. Hier worden veel minder zaken gedraaid. Bij de OBDS werken ongeveer 10 bijzondere opsporingsambtenaren en bij de Stichting Brein 3 internetspecialisten en juristen.

De OBDS wordt in feite geconfronteerd met twee verschillende vormen van piraterij waarvan er één op haar beurt op twee verschillende manieren wordt georganiseerd. De piraterij met betrekking tot de illegale verkoop en distributie van illegale dragers (CD's, CD Roms, DVD's en videobanden) is voor een deel in handen van professioneel georganiseerde bendes, die hun dragers onder valse voorwendselen laten vervaardigen in bona fide perserijen of zelf de nodige apparatuur hiervoor aanschaffen. Om problemen bij de grens te voorkomen vindt de productie vaak plaats in een Schengen-land. Bij deze bendes worden vaak grote hoeveelheden mobiele telefoons en andere communicatieapparatuur aangetroffen. De distributie van deze netwerken loopt over het algemeen 'via via'. Via allerlei tussenhandelaren komen de illegale gegevensdragers vaak terecht bij de spreekwoordelijke 'man met de achterbak vol Cd's op een parkeerplaats'. Op deze plaatsen en in cafés, op markten en via andere informele netwerken komen de gepirateerde dragers uiteindelijk bij de consument terecht.

De OBDS is nog geen zaken tegengekomen waar de bovengenoemde bendes op grote schaal gebruik maken van het internet om hun waren aan de man te brengen. Dit is ook wel logisch, het gaat immers voornamelijk om fysiek distributie. Wat wel voorkomt is dat de 'fijndistributeurs' van dergelijke dragers hun 'catalogi' op een (gratis) homepage zetten en op deze manier hun waren aan de man proberen te brengen. Deze mensen zijn vaak ook diegenen die in de tweede categorie van drager-piraterij actief zijn: de zogenaamde 'thuisbranders'. Ook deze piraten zijn voor een groot deel afhankelijk van hun informele netwerk voor hun klandizie. Zij produceren zelf de dragers. Deze categorie piraten gebruikt het internet veelvuldig (gratis websites, mailing lijsten, hosting in het buitenland) om klandizie te werven. Het internet fungeert voornamelijk als advertentiemedium. Wel is het voor de categorie thuisbranders door de jaren heen, met het goedkoper worden en makkelijk beschikbaar komen van apparatuur, in principe eenvoudiger en goedkoper geworden om de gepirateerde dragers te produceren. Bij deze categorie piraten wordt bij de opsporing vaak gebruikt gemaakt van het principe van 'follow the money'. De remboursrekeningen die worden gebruikt voor het innen van de opbrengsten van de dragers zijn in principe traceerbaar. De opbrengsten (en dus schade voor de industrie) kan ook bij deze 'kleine jongens' behoorlijk oplopen. Er worden vaak bedragen aangetroffen die de €100.000 te boven gaan.
Ook de advertentiemogelijkheden op internet kunnen worden aangepakt door een verzoek van de Stichting Brein of OBDS aan het hosting-bedrijf. De medewerking van deze netwerkbeheerders is wisselend. Eind 2000 zijn Brein/OBDS begonnen met het aanpakken van deze internetsites. In deze tijd heeft de stichting Brein ongeveer 300 van dergelijke websites aangepakt, de OBDS rond de 30. Het effect van deze aanpak is nu al zichtbaar. Men ziet een verschuiving naar veilingsites en mailinglijsten om de waren aan de man te brengen.

De andere vorm van piraterij waarbij nieuwe technologieën een rol spelen is de verspreiding van illegale bestanden. De grote bendes die bij de piraterij van dragers actief zijn, vindt men hier niet terug. Over het algemeen worden deze bestanden verspreid door individuele gebruikers zonder winstoogmerk. De prioriteit bij de aanpak van de aanbieders van illegale bestanden ligt bij personen of organisaties die wel proberen geld te verdienen met deze vorm van piraterij. Vormen hiervan zijn het doorlinken van een muziekbestanden na het aanklikken van een advertentie en (dit is in Nederland één maal voorgekomen) het verspreiden van illegale muziekbestanden op een inbelnetwerk via een 0900- betaalnummer.

In 2001 zijn er ongeveer 2.000 websites (http en ftp) waar illegale bestanden werden aangeboden afgesloten. Hiernaast zijn (wereldwijd) een aantal providers van de technologie om (potentieel) auteursrechtelijk beschermde bestanden uit wisselen (Napster, Kazaa) voor de rechter gebracht. Ook op dit gebied is de medewerking van de ISP's wisselend. Op dit moment zijn er een aantal afspraken gemaakt met de Vereniging van Internetproviders (het NLIP) maar deze afspraken zijn niet bindend voor de leden van de NLIP. Een ander probleem bij de aanpak van de verspreiding van illegaal verspreide bestanden is dat dit geen prioriteit heeft bij het OM. De bovengenoemde zaak met het betaalde inbelnummer vormt hierop een uitzondering. De samenwerking met de politie verloopt zonder problemen.

Uit het voorgaande wordt duidelijk dat de Buma-Stemra een begin heeft gemaakt met greep te krijgen op de piraterij in de virtuele ruimte. Zij beperkt zich daarbij tot op Nederland gerichte piraterij; haar zusterorganisaties in het buitenland doen dat in het eigen land.

De prioriteiten liggen doorgaans bij de piraten die geld verdienen aan de illegale verspreiding. De mogelijkheden die nieuwe technologieën bieden om over te gaan tot het verspreiden van illegale content worden ook door de OBDS gebruikt voor de opsporing. Zo wordt er anoniem door de stichting Brein op het internet 'gepatrouilleerd' op zoek naar illegale bestanden en aanbieders.

3.2.2 Fiscale Inlichtingen- en Opsporingsdienst (FIOD) / Economische Controle Dienst (ECD)

De Fiscale Inlichtingen- en Opsporingsdienst (FIOD) heeft tot taak:
a. het verzamelen van gegevens welke van belang zijn voor de heffing en de invordering van rijksbelastingen en
b. het opsporen van bij de belastingwet strafbaar gestelde feiten.

De FIOD heeft 11 vestigingen in Nederland en ongeveer 1.200 medewerkers. Deze medewerkers zitten over de gehele wereld verspreid; vaak verbonden aan ambassades.
Tot taak van de Economische Controle Dienst (ECD) behoort de controle op de naleving van wettelijke voorschriften en het opsporen van strafbare feiten op het gebied van economische criminaliteit.
Per 1 december 2001 werken deze twee diensten nauwer samen. Dit brengt onder andere met zich mee dat beide gebruik maken van de expertise en de ondersteunende diensten van de afdeling digitalisering van de FIOD. Deze afdeling bestaat uit een onderdeel dat zich bezig houdt met beleidsvorming en uit 6 digitale ondersteuningsteams (digiteams van ongeveer 6 personen) die de feitelijke opsporing ondersteunen. In deze teams zijn diverse specialisaties opgenomen als een IT-specialist en een medewerker Electronic Data Processing (EDP). Naast ondersteuning bij lopende onderzoeken, zowel intern bij onderzoeken van de FIOD en ECD als extern bij onder andere de politie, worden bij deze afdeling van de FIOD ook tools en methoden ontwikkeld.
De FIOD geeft aan zeer weinig zaken op het gebied van cybercrime te hebben. De meeste zaken die zij draaien, worden door de belastingdienst aangeleverd en betreffen 'old crimes' met 'old tools'. Deze conclusie wordt door een intern onderzoek, dat door de FIOD is verricht, ondersteund. Bij de ECD spelen met name zaken rond goederenstromen; ook hier gaat het om een gering aantal zaken in totaal.
Voor de toekomst verwacht de FIOD wel een stijging van het aantal zaken. De eerste e-commerce bedrijven zullen in het recente verleden of de nabije toekomst hun eerste belastingjaar achter de rug hebben. Mogelijk levert dit in de toekomst voor de FIOD meer cybercrime zaken op. Ook verwacht men in de toekomst zaken waarbij vervalste boekhoudingen of het zogenoemde 'undergroundbanking' een rol spelen. Men kan hier bijvoorbeeld denken aan een schaduwboekhouding, zoals die vermoed wordt te bestaan in de zogenaamde 'bouwfraudezaak'.

Aangegeven werd dat de digitalisering voor de FIOD vaak een positief effect sorteert. De overdaad aan informatie waar de FIOD mee te maken heeft laat zich makkelijker opslaan, vervoeren en onderzoeken in digitale vorm. In sommige onderzoeken hoeven nu niet meer vele ordners vol met papier te worden doorzocht. Hiermee is de transparantie van de te onderzoeken materie voor de FIOD toegenomen.
Het grootste probleem dat bij de FIOD wordt gesignaleerd is de moeite die men heeft om geschikte mensen te vinden voor dit soort werk en het voldoende opgeleid en bijgeschoold houden van de medewerkers. Een opmerking als "De gemiddelde speurneus kan niet digitaal denken" is in dit kader veelzeggend.

3.2.3 Banken en creditcardmaatschappijen

Banken en creditcardmaatschappijen hebben op een aantal manieren te maken met criminaliteit in de virtuele ruimte. In de eerste plaats kan men denken aan aanvallen op het bancaire netwerk waarmee onderlinge transacties, pinbetalingen en geldautomaten met elkaar verbonden zijn. Deze netwerken zijn over het algemeen fysiek gescheiden van openbare netwerken als het Internet en zijn om deze reden dan ook zeer weinig het doelwit van pogingen om binnen te dringen. Dit is in Nederland een enkele keer gebeurd in de afgelopen jaren zonder dat het netwerk werd binnengedrongen. Iets vaker (enkele keren per jaar) komt het voor dat banken of creditcardmaatschappijen worden afgeperst met de dreiging om dit netwerk te kraken. De banken zijn op dit front nog weinig 'echte' bedreigingen tegengekomen.

Op het openbare internet komt het wel geregeld voor (enkele gevallen per jaar) dat servers met betaalinformatie (in het bijzonder: creditcardnummers) van bedrijven die zaken doen op het internet, worden blootgelegd door kwaadwillende hackers. Ook wordt er bij banken nogal eens gefraudeerd met buitenlandse overboekingen. Dit zijn vrijwel altijd 'papieren fraudes': valse overboekingen die worden gedaan door formulieren te vervalsen. Door het internationale bankennetwerk zijn deze overboekingen vaak snel de wereld rond en moeilijk te achterhalen. Door de geïnterviewde securityspecialisten van de banken wordt hiernaast aangegeven dat men de combinatie van technologische kennis en criminele bendes voor de toekomst als een bedreiging voor de veiligheid van het bancaire netwerk ziet. Deze bedreiging is echter nog niet in de praktijk voorgekomen.

Een vaker voorkomende vorm van criminaliteit, waarbij gebruik wordt gemaakt van moderne (digitale) communicatiemiddelen, is de zogenaamde MO-TO- fraude (mail order, telephone order fraude). Hierbij worden artikelen besteld en betaald via de telefoon of via het internet. Hiervoor wordt gebruik gemaakt van een gestolen of niet-bestaand[14] creditcard nummer. In deze vorm van fraude zijn twee soorten te onderscheiden: aan de ene kant de fraude waarbij slecht niet-fysieke diensten (bellen naar het buitenland via de telefoon, software of andere diensten via het internet) worden besteld en geleverd en de fraude waarbij fysieke goederen worden besteld en geleverd. De aantallen van dergelijk fraude zijn moeilijk aan te geven. Bij de beveiligingsafdelingen van de banken komen meestal slechts de zaken terecht die 'het topje van de ijsberg' vormen. Het betreft hier tientallen meldingen per maand. Binnen dit aantal bevinden zich ook de gevallen van de gehackte webservers met creditcardinformatie. Een groot deel van de frauduleuze transacties wordt al afgevangen door automatische fraude-detectiesystemen. Bij creditcardmaatschappijen wordt het uitgavenpatroon in de gaten gehouden; bij bankrekeningen vaak de bedragen die op de rekening worden gestort. Komt dit systeem een opmerkelijke overboeking tegen dan gaat er een 'alarmbel' rinkelen. Nieuwe electronische betaalsystemen (I-Pay, pinnen, chippen) worden pas ingezet na een gedegen veiligheidsanalyse. Het kraken van de beveiliging van deze systemen is nog niet voorgekomen.

Een probleem bij het op het spoor komen van, registeren van en optreden tegen creditcardfraude is dat de schade uiteindelijk bij de leverancier van de producten of diensten terechtkomt. De creditcardmaatschappijen lijden de schade vaak zelf niet. Voor het behouden van vertrouwen in het betaalmiddel

Noot 14 Deze worden dan gegenereerd met behulp van speciale programmaatjes: zogenaamde 'credit card generators'

en de maatschappelijk functioneren van deze instellingen wordt deze fraude uiteraard wel zoveel mogelijk opgespoord. Dit is wellicht een verklaring voor het fenomeen dat door de politie wordt gesignaleerd: van deze vormen van fraude wordt niet vaak aangifte gedaan. Deze aangiften worden door bedrijven, als ze al overgaan tot aangifte, zeer versnipperd over het land gedaan. Hiernaast vormt de samenwerking met politie en justitie nogal eens een knelpunt. In de eerste plaats liggen de prioriteiten van het OM en politie en justitie niet altijd bij de MOTO fraude of de fraude naar het buitenland. Bij grensoverschrijdende fraudegevallen lopen de rechtshulpverzoeken om sommen geld te achterhalen in het buitenland vaak maanden achter op de geldstromen zelf. Banken en creditcardmaatschappijen moeten op zo'n moment vertrouwen op hun eigen (vaak informele) netwerken van collega beveiligingsspecialisten in het buitenland.

3.3 Aspecten van de digitalisering: gevolgen voor de opsporing

3.3.1 Plaats en Afstand

De vraag onder welke jurisdictie een bepaald delict valt dat gepleegd wordt in de virtuele ruimte, is vaak lastig te beantwoorden. Of de Nederlandse justitie wel rechtsmacht heeft, is een vraag die zich vele malen vaker voordoet bij criminaliteit in de virtuele ruimte dan bij andere vormen van criminaliteit.
De fysieke afstand tussen verdachten en opsporende instanties kan groot zijn. Hierbij vormen de traditionele indeling in arrondissementen, kantons en dergelijke een probleem; het potentieel aan mogelijke verdachten van buiten het 'eigen' gebied kan vele malen groter zijn dan bij traditionele vormen van criminaliteit.

Er zijn echter ook relevante gevolgen voor de daders van virtuele criminaliteit. De dader kent slechter de lokale omstandigheden (waaronder de expertise van de opsporingsinstanties en de juridische mogelijkheden) en de specifieke zwakheden van zijn slachtoffer. Dat was duidelijk het geval bij de Nederlander die naar de Verenigde Staten gelokt werd omdat hij seksuele intenties zou hebben met een minderjarige. Uitlokking van een misdrijf is niet toegestaan in Nederland maar hackers worden wel degelijk uitgelokt door zogenaamde honey-pots. Dit zijn aantrekkelijke en kwetsbaar ogende websites of computersystemen. Doel daarbij is om enerzijds de state-of-the-art aanvalsmethoden te achterhalen en anderzijds om de identiteit van de aanvallers te achterhalen. Indien het de aanvaller duidelijk had kunnen zijn dat de website of het computersysteem niet voor het publiek toegankelijk is, dan is strafrechtelijke vervolging toch mogelijk zonder dat van uitlokking sprake is.

Als de criminelen gebruik maken van de afstand en de grenzen van de jurisdictie dan is het zaak om delen van de opsporing effectiever en efficiënter te maken door waar nodig expertise te bundelen. Op deze wijze wordt ook de aanpak onafhankelijk gemaakt van de afstand en de grenzen van de jurisdicties.

3.3.2 Tijd en Frequentie

Digitale technieken geven criminelen de kans om bepaalde handelingen te automatiseren en daardoor in zeer korte tijd vele malen te herhalen. Een vele malen herhaald en/of tegelijkertijd uitgezet delict is zeer moeilijk te bewijzen. Wanneer ieder afzonderlijk klein delict in beeld moet worden gebracht, moet een buitenproportionele opsporingsinspanning worden geleverd.

De som van de vele kleine delicten levert echter het grote delict op. Men kan hierbij denken aan de bekende Nigeriaanse '419 fraude', waarbij op zeer grote schaal brieven of e-mails worden verstuurd met de bedoeling mensen op te lichten. Wellicht ook dat vaker gekeken kan worden naar de omvang van het totale bewijs, dan dat strenge eisen gesteld worden aan ieder individueel bewijsmiddel.

3.3.3 Anonimiteit

De mogelijkheden om anoniem te werken, maar ook de mogelijkheid om de informatie te versleutelen, maakt opsporing evident problematisch.
Wie de dader is, maar ook wie het slachtoffer is, blijft soms onbekend. Maatregelen om hetzij de anonimiteit, hetzij de versleuteling op te heffen kunnen steevast rekenen op groot verzet op privacy gronden. In het onlangs getekende verdrag European Convention on Crime in Cyberspace rime wordt hier echter een voorziening voor getroffen[15].

3.3.4 Kopieerbaarheid en Gemak van verspreiding

De kopieerbaarheid van informatie speelt bij criminaliteit omtrent auteursrechten en intellectuele eigendomsrechten.
De herkomst van informatie of software is door de zeer gemakkelijke verspreiding vaak lastig aan te tonen. Ook de locatie van een dader is hierdoor vaak moeilijk te achterhalen.

Het gemak van verspreiding werkt ook in de hand dat slachtoffers onderling informatie kunnen uitwisselen en krachtige allianties kunnen vormen om hun tegenacties te coördineren. De overheid maar ook bijvoorbeeld de consumentenbond stimuleert deze krachten bundeling door het inrichten van meldpunten. Waarschuwingen tegen aanvallen of malafide praktijken kunnen ook makkelijker verspreid worden.

3.3.5 Manipuleerbaarheid en Wissen van sporen

Het veranderen van bits is zeer eenvoudig. Zo kunnen bijvoorbeeld gemakkelijk debet of credit gegevens, opgeslagen in computerbestanden of bepaalde chipkaarten, worden gemanipuleerd.
Door deze manipuleerbaarheid kunnen sporen van eventueel criminele activiteiten gemakkelijker worden verwijderd. Wanneer dit vakkundig gebeurt, wat lang niet altijd zo eenvoudig is als de gemiddelde computergebruiker denkt, kunnen sporen onherstelbaar en onherleidbaar worden gewist.
Daarentegen kan essentiële informatie op meerdere plaatsen worden bijgehouden of kan een permanent archief worden bijgehouden van alle relevante datacommunicatie (loggen).

Noot 15 De volledige tekst van dit op 23 november 2001 gesloten verdrag kan men vinden op: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

3.3.6 Beschikbaarheid van informatie via Internet

De informatiekosten die een dader maakt om zijn daden voor te bereiden worden lager als gevolg van internet. Criminele kennis kan makkelijk worden uitgewisseld of worden ingewonnen.

De mogelijkheden van de overheid of van slachtoffers om te waarschuwen zijn ook groter. Dit is het middel dat de overheid het meest gebruikt bij de bestrijding van cybercrime: het verschaffen van informatie. Vooralsnog blijft de informatie afkomstig van de Nederlandse overheid achter bij de informatie die beschikbaar is in de Verenigde Staten of Engeland.
Vooralsnog is het beveiligen tegen cybercrime een zaak van de meer kundige gebruikers. De gemiddelde gebruiker kan met moeite de aanbevolen beveiligingsmaatregelen installeren (virusscanner, procedures telebankieren) en moet er maar op vertrouwen dat verder alles redelijk is afgedicht. Echter, het is aannemelijk dat PC-, softwareleveranciers en ISP's met de tijd gedegen en gebruikersvriendelijke beveiligingsoplossingen zullen ontwikkelen.

3.3.7 Beschikbaarheid van apparatuur

Kosten voor cybercrime kunnen beperkt blijven tot een PC en mogelijke enkele interface kaarten. Met deze vaak relatief goedkope en overal beschikbare apparatuur kunnen vele criminele activiteiten worden gepleegd of worden ondersteund.
Voor heel specialistische taken echter is soms zeer gesofisticeerde apparatuur nodig. Zeer krachtige, zeldzame of speciaal te ontwikkelen digitale apparaten kunnen zeer kostbaar zijn.

De kosten van de apparatuur zijn vaak laag maar ook de kosten van bijvoorbeeld krachtige encryptie middelen en middelen om de identiteit van computergebruikers te identificeren (vingerafdruk) nemen af. Het is goed denkbaar dat in combinatie met de diensten vanTrusted Third Parties, partijen die in vertouwen bepaalde informatie beheren of doorgeven, internet protocollen en procedures ontwikeld worden die veel van de huidige cybercrime dreigingen effectief tegengaan.

4 Conclusies en aanbevelingen

Binnen dit onderzoek stond de volgende probleemstelling centraal: *'Wat is de aard en omvang van criminaliteit in de virtuele ruimte?'*. Om een antwoord op deze vraag te kunnen geven, is een aantal activiteiten ondernomen. Door middel van een uitgebreide probleemanalyse zijn de voor de ontwikkeling van de criminaliteit relevante aspecten van de digitalisering van de samenleving in kaart gebracht. Hiernaast zijn de effecten van deze digitalisering op de huidige en toekomstige mogelijkheden voor bestrijding beschreven. Daarbij is ook de organisatie van de aanpak van deze vormen van criminaliteit aan bod gekomen. Dit onderzoek is uitgevoerd ten behoeve van de Nederlandse politie; de conclusies en aanbevelingen richten zich dan ook tot deze (omvangrijke) doelgroep.

4.1 Conclusies

Criminaliteit in de virtuele ruimte verschilt op een aantal aspecten van 'traditionele criminaliteit'. Om een kader te scheppen waarin de verschillen en overeenkomsten met traditionele criminaliteit te begrijpen zijn, is binnen dit onderzoek een *werkdefinitie* van de criminaliteit in de virtuele ruimte geformuleerd.
In de eerste plaats is er een onderscheid gemaakt tussen de begrippen 'new crimes' en 'old crimes' en 'new tools' en 'old tools'. De new crimes zijn de vormen van criminaliteit die als doelwit slechts de (gegevens in) moderne computer- en telecommunicatieapparatuur kunnen hebben (bijvoorbeeld hacking). Old crimes zijn alle andere, meer 'traditionele' vormen van criminaliteit zoals diefstal (bijvoorbeeld van computers).
De andere dimensie in deze afbakening heeft betrekking op de instrumenten waarmee de criminaliteit wordt gepleegd. 'New tools' zijn alle moderne elektronische digitale technieken met behulp waarvan criminaliteit wordt gepleegd.
Criminaliteit in de virtuele ruimte in brede zin heeft dus betrekking op die vormen van criminaliteit waarbij een 'digitale' component aanwezig is als instrument of als doelwit. Hierbij worden de 'new crimes, new tools' nog apart onderscheiden als 'criminaliteit in de virtuele ruimte in enge zin'.

Tabel 4.1 Crimes versus Tools

		Tools	
		Old	New
Crimes	Old	**1**- *old crimes, old tools*: - diefstal van geheugenchips uit computers door middel van braak-	**2**- *old crimes, new tools* - oplichting van consumenten door een nep website-
	New	**3**- *new crimes, old tools* - ontregelen van digitale meetapparatuur (gas, licht, elektra)-	**4**- *new crimes, new tools* - hacking[16] -

Noot 16 Onder 'hacking' wordt verstaan het zich zonder toestemming van de beheerder toegang verschaffen tot een computersysteem. Hiervoor is het vaak noodzakelijk dat deze door middel van een netwerk zijn verbonden met andere computersystemen.

Criminaliteit in de virtuele ruimte onderscheidt zich op een aantal specifieke kenmerken van 'traditionele' vormen van criminaliteit, omdat gebruik gemaakt wordt van een aantal aspecten van de digitalisering van de maatschappij. Er worden hiervoor de volgende zeven aspecten onderscheiden:

- Plaats en Afstand;
- Tijd en Frequentie;
- Anonimiteit;
- Kopieerbaarheid;
- Manipuleerbaarheid;
- Beschikbaarheid van informatie;
- Beschikbaarheid van apparatuur.

Louter het gebruik maken van digitale technieken is echter niet voldoende om binnen de definitie van criminaliteit in de virtuele ruimte te vallen. Voor de vraag of een specifieke verschijningsvorm van criminaliteit binnen de opgestelde definitie van criminaliteit in de virtuele ruimte valt, is het ook noodzakelijk dat gebruik gemaakt wordt van de specifiek aspecten van de digitalisering. Dit leidt tot de volgende definitie van criminaliteit in de virtuele ruimte.

Definitie Cybercrime

Cybercrime is criminaliteit waarbij gebruik wordt gemaakt van:
a. digitale dataopslag of datacommunicatie en
b. waarbij één of meerdere aspecten van de digitalisering van de criminaliteit bepalend zijn voor het gepleegde delict. Deze aspecten zijn: tijd en frequentie, anonimiteit, kopieerbaarheid, manipuleerbaarheid, beschikbaarheid van informatie en beschikbaarheid van apparatuur.

Met deze definitie kan de aard van de zeer diverse verschijningsvormen van criminaliteit in de virtuele ruimte worden geduid. In hoofdstuk 2 zijn vele vormen van cybercrime beschreven.

Omvang van criminaliteit in de virtuele ruimte
Het is onmogelijk gebleken om de omvang van criminaliteit in de virtuele ruimte te bepalen. De registratie van cybercrime vindt zeer versnipperd plaats binnen de politie. In bedrijfsprocessensystemen als X-Pol en BPS en een systeem als het herkenningsdienstsysteem (HKS) zijn gegevens over dit soort zaken niet terug te vinden. Ook slachtofferonderzoek over dit soort delicten (zoals de politiemonitor) is vrijwel niet voorhanden. De subjectieve indrukken over de omvang van dit type criminaliteit van diverse binnen het werkveld geïnterviewde personen lopen nogal uiteen. Moeilijkheden om tot een bepaling te komen van de omvang wordt mede veroorzaakt door het feit dat er tot nu toe geen sluitende definitie van deze vormen van criminaliteit was.
Op dit moment lijkt, binnen het hierboven gemaakte onderscheid naar 'crimes' en 'tools', de categorie met de '*old* crimes' wat betreft omvang groter te zijn dan de categorie met de 'new crimes'. Verwacht mag worden dat de categorie 'new crimes, new tools' sterker zal groeien dan de andere categorieën.

Mede door het ontbreken van een duidelijk definitie van cybercrime is er geen zicht op de omvang van deze problematiek. De politiecijfers die nu worden gegenereerd zijn voor het geven van een beeld volkomen ongeschikt.

Expertise binnen de politie
Binnen de Nederlandse politie is de expertise op het gebied van digitale aspecten van de opsporing verdeeld over zogenoemde 'kennislagen'. De diverse Bureau's Digitale Expertise (BDE's) verspreid over het land, zijn de schakel tussen het landelijk kennisniveau (het Nederlands Forensisch Instituut waar de meest specialistische kennis zich bevind) en de dagelijkse, lokale politiepraktijk. Zij kunnen worden ingeroepen als de zaken die de politie in haar dagelijkse werk tegenkomen een digitale component hebben.

De BDE's gaan de laatste jaren gebukt onder een steeds groter wordende 'caseload'. Dit zelfs ondanks het feit dat veel zaken die in aanmerking zouden kunnen komen voor behandeling niet verder onderzocht worden, omdat veel ze niet door het case-screeningsmodel van de Nederlandse politie heen komen. Daarnaast komt waarschijnlijk een aanzienlijk deel van de cybercrime niet bij de politie terecht omdat er geen aangifte wordt gedaan.

Een groot deel van de werkzaamheden van de digitale recherche bestaat uit het geven van technische ondersteuning op digitaal gebied voor de aanpak van 'traditionele' vormen van criminaliteit. De aanpak van pure 'new crimes, new tools'-criminaliteitsvormen als hacking komt veel minder vaak voor. De gemiddelde zaak van de digitale recherche vergt vaak meer werk dan een vergelijkbare traditionele recherchezaak. Een goed deel van de tijd gaat op aan verslaglegging en documentatie. Eén type zaak waarbij de digitale recherche vaak betrokken raakt en dat binnen alle korpsen hoge prioriteit heeft, is de bestrijding van kinderporno.

Door de toenemende werkdruk komt het opleiden van de medewerkers en het ontwikkelen van de kennis binnen de afdelingen nogal eens onder druk te staan. Meer algemeen geld dat de 'digitale kennis' zich langzaam door de politieorganisatie heen beweegt. Medewerkers aan de basis weten nog niet altijd de weg te vinden naar de deskundigen en wanneer zij deze weg zouden moeten bewandelen. Dit levert problemen op wanneer een partij aangifte wenst te doen van een strafbaar feit waarbij een digitale component een rol speelt.

De rol die de digitale recherche binnen Nederland speelt is tweeledig. Waar het de aanpak van 'old crimes' betreft *ondersteunen* zij de traditionele opsporing. Waar het echter de aanpak van 'new crimes' betreft, hebben zij in wezen hun eigen werkgebied. De aandacht voor dit eigen werkgebied van de digitale recherche moet worden vergroot.

De digitale recherche binnen de politie heeft, door de hoge werkdruk, niet genoeg tijd en capaciteit voor kennisopbouw en het uitwisselen van deze kennis. Hiervoor moet meer ruimte komen; naast basis scholing ook blijvend bijscholen.

Daarnaast moet in het werk van de digitale recherche meer aandacht komen voor het eigen werkgebied van de digitale recherche namelijk de 'new crimes'. Voor de aanpak van deze 'new crimes' moet een loketfunctie worden ontwikkeld (bijvoorbeeld bij de bureau's digitale recherche). Een voorbeeld van een al lopende ontwikkeling op dit gebied is het Hacking Emergency Respons Team (HERT – zie hieronder). Hierdoor moeten meer cybercrime zaken op de juiste plek terecht komen en deze moeten dan ook in behandeling worden genomen. Voor de 'old crimes' moet zoveel mogelijk worden aangesloten bij de bestaande loketten binnen de Nederlandse opsporingsketen.

Sleutelpersonen binnen de overige opsporingsinstanties (buiten de politie) en het bedrijfsleven rapporteren dat 'new crimes, new tools' nog niet vaak voorkomen. Wel vreest men voor een toename van de problematiek in de (nabije)

(nabije) toekomst. Een uitzondering hierop vormen schendingen van het auteursrecht. Dit komt op het publieke Internet zeer veel voor. De opsporing op dit gebied beperkt zich noodgedwongen tot de auteursrechtschenders die hiermee trachten geld te verdienen.

4.2 Aanbevelingen

Het in dit rapport neergelegde onderzoek heeft uiteindelijk een zeer brede scope gekregen. Dit komt doordat criminaliteit in de virtuele ruimte zoals hiervoor werd omschreven een gevolg is van een bredere maatschappelijke ontwikkeling, namelijk de digitalisering van de samenleving. De gevolgen van deze ontwikkeling voor de veiligheid zijn niet alleen een onderwerp voor de Nederlandse politie of de overheid. In feite is iedereen betrokken bij dit onderwerp.

Integraal Veiligheidsplan
Onze eerste aanbeveling is dan ook dat er een ***Integraal Veiligheidsplan*** voor criminaliteit in de virtuele ruimte moet worden gemaakt. Hierin worden de rollen en verantwoordelijkheden van de diverse partijen nader omschreven. Daarbij moet ook aandacht worden besteed aan de preventie van cybercrime; het onderwerp noopt daartoe.
Voor de uitwerking van dit plan moet op nationaal niveau een partij als spin in het web fungeren die in korte tijd tot een uitgewerkt plan kan komen. Een interdepartementale werkgroep waarin naast de Ministeries van Justitie en Binnenlandse Zaken en Koninkrijksrelaties ook vertegenwoordigers van bijvoorbeeld de Stuurgroep Informatietechnologie en Criminaliteit van het Nationaal Platform Criminaliteitsbeheersing zitting hebben is daarvoor een goede mogelijkheid.
Op operationeel niveau is een eerste stap tot verdergaande integrale samenwerking al gezet. Met het opzetten van een specifiek op new crimes, new tools gespitst team waarin overheid en bedrijfsleven samenwerken (een HERT: een Hacking Emergency Response Team) is een begin gemaakt.

De aanpak Criminaliteit en onveiligheid in de virtuele ruimte is geen taak van alleen de politieorganisatie. Er moet een Integraal Veiligheidsplan voor criminaliteit in de virtuele ruimte worden opgezet.

Betere samenwerking
De samenwerking tussen diverse overheidsinstanties moet verder worden bevorderd. Er is op dit gebied al veel kennis en expertise aanwezig binnen diverse takken van de overheid. Gezegd moet worden dat er al veel samengewerkt wordt. Met name op het gebied van concrete lopende onderzoeken wordt kennis en expertise, wanneer daar behoefte aan is, al vaak buiten de deur gezocht en gevonden. Op beleidsniveau en op het gebied van preventie echter moeten deze contacten zich intensiveren. Ook het OM moet meer betrokken worden bij de ontwikkeling van de aanpak van cybercrime, zij valt nu vaak nog buiten de boot.
Het benoemen en het aanspreken van deze bronnen op hun vaak specifieke en specialistische kennis en vaardigheden moet worden ingebed. Hiernaast kunnen ook overheidsinstanties en het ***bedrijfsleven*** meer samenwerken op het gebied van de aanpak van cybercrime.

Kennis algemeen
De aanpak van deze vorm van criminaliteit en onveiligheid alleen effectief kan plaatsvinden wanneer de partijen die hierbij betrokken zijn voldoende kennis in huis hebben en houden. Het vasthouden van kennis (in de vorm van mensen met ervaring) en het goed opgeleid en bijgeschoold houden van de betrokken medewerkers is daarbij van het grootste belang. Hier moet binnen de organisatie van de aanpak voortdurende aandacht voor worden gehouden.

Kennis politie en justitie
Binnen de keten van politie en justitie is het nodig om de kennisopbouw- en cumulatie te waarborgen. Door middel van het kennislagenmodel is daarvoor al een goede basis gelegd bij de politie. Omdat de aanpak van cybercrime vooral afhankelijk is van de aanwezige kennis, is het managen van deze kennis van groot belang. Het doorvoeren en praktisch uitwerken van deze gedachte binnen de politieorganisatie en het OM is dan ook noodzakelijk.

De verspreiding van kennis over moderne ICT- en communicatietechnologie en de invloed hiervan op de opsporing moet een speerpunt worden binnen de keten van politie en justitie.

Een ander aspect van deze kennisopbouw en –cumulatie is dat er kwantitatief onderzoek moet worden opgezet naar de omvang van de 'virtuele criminaliteit'. Men kan hierbij denken aan zowel dader- als slachtofferonderzoek. Voor de eerste vorm van onderzoek is dan wel een aanpassing, standaardisering en uniformering noodzakelijk van de registraties van de politie van deze delicten. De BDE's moeten hierin het voortouw nemen door hun eigen registraties onderling te standaardiseren. Op deze manier kunnen ook trends in de tijd in kaart worden gebracht en kan op een betere manier aan het management worden gerapporteerd over waar de huidige opsporingscapaciteit voor wordt ingezet. Door middel van het uitvoeren van slachtofferonderzoek, in de vorm van een aanvulling op de Politiemonitor of een geheel 'virtuele monitor' , moet een begin worden gemaakt met het in kaart brengen van slachtoffers van 'nieuwe' vormen van criminaliteit.

De BDE's moeten hun registraties standaardiseren en verbeteren. Er moet vanuit politie en justitie zowel dader- als slachtofferonderzoek worden geïnitieerd naar criminaliteit in de virtuele ruimte.

Het bijhouden van de laatste technische ontwikkelingen is een aandachtspunt dat binnen de bestrijding van cybercrime veel aandacht verdient. Dit onderwerp leent zich ook, meer dan nu gebruikelijk is, voor een pro-actieve aanpak. Dit zou kunnen plaatsvinden door:

- het in kaart brengen van criminele groepen met digitale expertise,
- het inventariseren van de markten voor bepaalde strategische goederen en
- het actief bestrijden van criminele informatie (criminele 'how-to's) op netwerken. Men mag hierbij niet de illusie koesteren dat deze informatie geheel uit het publiek domein verwijderd kan worden. Wel kan men de verspreiding van deze informatie tegengaan door regelgeving, opsporing en handhaving.

Politie en justitie: internationale samenwerking
Het grensoverschrijdende karakter van een deel van cybercrime maakt het voor de politie noodzakelijk om haar netwerk verder uit te breiden. Zowel nationaal als vooral ook internationaal. Daarbij volstaat het niet als op landelijk niveau een beperkt aantal mensen deze contacten onderhoud.

De medewerkers van de diverse bureau's digitale expertise en recherche zouden indien nodig en gewenst gemakkelijker en sneller informatie met buitenlandse collega's moeten kunnen uitwisselen. Verregaande samenwerking met opsporingsinstanties in het buitenland is de enige manier om effectief en snel tot de aanpak van sommige vormen van criminaliteit in de virtuele ruimte te komen. De procedures waarlangs informatie en rechtshulp kan worden gevraagd en geboden moeten worden geautomatiseerd en versneld. De politie in Nederland moet op haar beurt ook de nodige prioriteit geven aan zaken die vanuit het buitenland worden aangeleverd en rechtshulpverzoeken uit het buitenland.

De Nederlandse overheid en politie moeten het initiatief nemen om een vast samenwerkingsverband tussen internationale opsporingsinstanties op het gebied van criminaliteit in de virtuele ruimte op poten te zetten.

De mogelijkheden van het opzetten van een snel Europees elektronisch 'opsporingsnetwerk', met onder andere deze taken als doel, moet worden onderzocht. Daarnaast moeten de rollen van Europol en Interpol in deze verder worden uitgewerkt en mogelijk efficiënter worden benut.

Cybercrime en het case-screeningsmodel
Binnen het case-screeningsmodel dat de politie hanteert moet meer aandacht komen voor cybercrime. Er moet bijvoorbeeld rekening gehouden worden met 'microschades' die bij een groot aantal partijen kunnen ontstaan (bijvoorbeeld fraude via een groot aantal betalingen over een netwerk). Men kan hierbij denken aan de in hoofdstuk 3 geschetste creditcard fraude waarbij de slachtoffers, vaak in verschillende regio's, allemaal apart aangifte doen. Dit vaak zonder dat de diverse politieorganisaties en –korpsen weten wie er naast hen nog meer met deze zaak bezig zijn. Op dit moment zal een dergelijke fraude, zonder een groot aantal aangiften, niet door het case-screeningsmodel komen. Er liggen kansen om op dit gebied samenwerking te zoeken met banken en creditcardmaatschappijen. Deze kunnen eenvoudiger een overzicht genereren over de schade van deze afzonderlijke microdelicten. Voor de ontwikkeling van kennis en expertise binnen de 'digitale' tak van de opsporing, zou in het case-screeningsmodel ook een component voor de mate van technische vernieuwing moeten worden ingebracht. Op deze manier kunnen ook zaken worden gedraaid waarbij aan technische ontwikkeling en innovatie wordt gedaan.

Virtueel surveilleren
De politie zou zich nog meer dan zij nu al doet bezig kunnen gaan houden met het surveilleren en detecteren van verdachte 'bewegingen' op openbare netwerken. Er is hiermee al een begin gemaakt door de actieve 'patrouilles' van de KLPD. Uit het in dit onderzoek genoemde voorbeeld van de surveillances van de OBDS blijkt dat deze aanpak zoden aan de dijk zet. Het is hier ook net als met 'traditionele' criminaliteit: niet alles wordt door de opsporingsinstantie gedetecteerd, maar het besef dat er gepatrouilleerd wordt maakt dat mogelijke daders worden afgeschrikt.

Het case- screeningsmodel moet aangepast worden zodat meer rekening gehouden wordt met cybercrime.
Voor zowel preventie als repressie van delicten in de virtuele ruimte is het wenselijk dat de politie meer actief patrouilleert op openbaar toegankelijke netwerken, net als in de niet-virtuele ruimte (meer blauw in cyberspace).

De overheid als wetgever en beleidsmaker
De landelijke en Europese overheid moet de opsporing en bestrijding van criminaliteit in de virtuele ruimte op haar beurt op een aantal punten eenvoudiger maken. In de eerste plaats zal er met betrekking tot het aspect 'afstand' een traject in gang moeten worden gezet om rechtsmachtproblemen van criminaliteit in de virtuele ruimte te voorkomen. Hierbij kan gedacht worden aan het claimen van rechtsmacht bij delicten waarbij de ICT infrastructuur van het slachtoffer of zich in Nederland bevindt[17] of zelfs een verregaande stap als het claimen van rechtsmacht over het gehele met Nederland verbonden virtuele domein is niet ondenkbaar. In de European Convention on Crime in Cyberspace is een begin gemaakt met het oplossen van deze problematiek door in internationaal verband afspraken te maken over samenwerking op het gebied van vervolging van criminaliteit in de virtuele ruimte.

Hiernaast kan de Nederlandse overheid ook een rol spelen in het vergemakkelijken van de vervolging van virtuele criminaliteit die vanuit Nederland worden gepleegd. Denk bijvoorbeeld aan het opzetten van een 'netwerk' van Internationale rechtshulp. Hierbij moet uiteraard van moderne elektronische technieken gebruik worden gemaakt. Voor een deel is hiervoor een aanzet gegeven in de European Convention on Crime in Cyberspace. De effectiviteit van dit verdrag zal echter voor een groot deel afhangen van de uitwerking van de afspraken die in dit verdrag zijn vastgelegd; het is zaak daar serieus werk van te maken.

Ook kan de wetgever overwegen om aan netwerkbeheerders op te leggen dat zij de gebruikers van hun netwerk verplichten zich bekend te maken met hun NAW-gegevens. Samen met een verplichting om de verkeersgegevens van een bepaalde gebruiker (het gaat hier dus niet om de *inhoud* van de communicatie) bij te houden, wordt het voor iemand die een delict wil plegen door zich te verschuilen achter anonimiteit op bijvoorbeeld het openbare internet, minder aantrekkelijk om dat delict te plegen. Ook het probleem van SPAM (nu nog niet strafbaar) en hatemail en pest-SMSjes kan op deze manier zowel voorkomen als bestreden worden. Deze verplichting kan ook worden opgelegd in de vorm van een aansprakelijkheidsstelling. Kan de netwerkbeheerder geen NAW leveren (aanwijzingsplicht), dan wordt zij zelf aansprakelijk voor de bij haar netwerk originerende delicten[18]. Nederland zou op dit punt een voorbeeldfunctie kunnen hebben.

De overheid speelt naast het gebied van de wetgeving een belangrijke rol in het voorlichten van burgers over het 'veilig' om kunnen gaan met digitale technieken. De overheid heeft op dit gebied al een aantal goede voorbeelden laten zien (de campagne 'Surf op Safe' bijvoorbeeld), maar men kan ook denken aan bijvoorbeeld keurmerken voor ISP's die de gebruiker op een actieve manier beschermen tegen hacking-aanvallen en virussen (een provider met het Politiekeurmerk Veilig Surfen bijvoorbeeld). Hiernaast moet er meer aandacht besteed worden aan de bewustwording van burgers over hun veiligheid op elektronische netwerken.

Noot 17 Dit is in principe mogelijk: door de Hoge Raad werd in haar 'Singapore'-arrest rechtsmacht van Nederland aangenomen omdat het een bepaald bestanddeel van het delict in Nederland verwezenlijkt werd. (HR, 6 april 1954, NJ 1954, 368). Voor andere aspecten van rechtsmachtproblematiek met betrekking tot criminaliteit in de virtuele ruimte: zie Chr. H. van Dijk en J.M.J. Keltjens, *Computercriminaliteit*, hoofdstuk 3.

Noot 18 Vergelijk hiervoor de voor gestolen goederen bestaande aanwijsplicht in artikel 3:86 BW jo. 3:87 BW.

De overheid moet, zeker in Europees verband, snel een begin maken met het formuleren van veiligheidsnormen van digitale technologie en software. Vergelijkbare normen bestaan er immers voor vrijwel alle andere aspecten van de samenleving. Men kan daarbij denken aan voedselveiligheid, bouwbesluiten, veiligheidseisen voor auto's, enzovoort. Een dergelijke normering voor digitale techniek waar steeds meer mensen op vertrouwen en die een steeds grotere rol speelt in de economie, is echter nog nauwelijks ontwikkeld. Zoals de Leidse hoogleraar Franken in zijn afscheidsrede al uitdrukte: binnen computerprogramma's en computernetwerken is op dit moment de programmeur de 'wetgever'[19].

Andere partijen; zelfregulering
Zoals gezegd is de aanpak van criminaliteit in de virtuele ruimte niet alleen een taak van de overheid. Zeker op het openbare internet, met zijn geschiedenis van zelfregulatie, zijn er genoeg andere partijen die ook hun deel van deze aanpak ter hand kunnen nemen. Zo kan van de beheerders van netwerken (hierbij kan gedacht worden aan ISP's, maar ook aan (mobiele) telefoonmaatschappijen etc.) wellicht worden gevraagd om in de eerste plaats de Acceptable Use Policy (AUP) op hun eigen netwerk op een serieuze manier te handhaven en snel op te treden tegen mensen die het netwerk misbruiken. Hiernaast kan er een preventieve werking uitgaan van deze handhaving, evenals van het expliciet registeren van NAW- gegevens van de klanten van netwerkproviders. De netwerkbeheerders moeten op deze manier tegemoetkomen aan hun maatschappelijke verantwoordelijkheid. Vanuit dit punt belicht moeten zij ook een rol spelen bij het ontwikkelen van normen en waarden op hun eigen netwerk. Een goed voorbeeld van het ontwikkelen van eigen 'netwerknormen' is de mobiele telefonie provider Ben, die een campagne heeft gevoerd die haar gebruikers opriep om aan anderen geen overlast te veroorzaken bij het gebruik van de mobiele telefoon. Ook diverse ISP's proberen hun gebruikers 'op te voeden' door aan hen uitleg te geven over de normen die gelden op het openbare internet.

Ook gebruikers van moderne digitale apparatuur hebben dankzij de moderne digitale technieken de mogelijkheden om zich te beveiligen. Zo kunnen zij zich op de hoogte stellen van de manieren om hun apparatuur te beveiligen tegen (netwerk)aanvallen van buitenaf, deze te beveiligen tegen oneigenlijk gebruik (password etc.) en om de integriteit van de data die in hun apparatuur staat opgeslagen te behouden (encryptie). De burger moet zich wel op de hoogte stellen van deze mogelijkheden. Met de binnen de maatschappij steeds verder verspreidende kennis op het gebied van computers wordt dit naar verwachting steeds eenvoudiger.

Uiteraard heeft de telecom- en software-industrie op dit gebied ook een verantwoordelijkheid. In de eerste plaats door de nodige veiligheids- en identificatievoorzieningen in haar apparatuur in te bouwen. Maar ook door de gebruikers over deze voorzieningen te informeren. Het vertrouwen van de gebruikers in deze producten staat of valt met deze beveiliging.
Het is dus ook in het belang van de industrie. Zo kan zij de veiligheid van haar producten zelfs gebruiken als marketing argument.

Noot 19 *Nemo Plus*, pagina 7.

Bijlagen

Bijlage A De begeleidingscommissie en geïnterviewde personen

De begeleidingscommissie voor dit onderzoek bestond uit:

- Dhr. prof mr C.D. Schaap, SVB Forensic Accounting & Consulting (voorzitter);
- Mw. mr. W.M. de Jongste, Politie & Wetenschap;
- Dhr. drs. R.H.P. Vriesde, landelijk projectleider, Landelijk projectbureau Digitaal rechercheren;
- Dhr. G. C. Th. Wierda, hoofd afdeling Digitale Technologie Nederlands forensisch Instituut (NFI);
- Dhr. mr J.R. Klunder, Officier van Justitie, Arrondissementsparket Zwolle;
- Mw. drs. M. Wong, Directie Politie, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

De volgende personen zijn voor dit onderzoek geïnterviewd:

- Dhr. Cusiel, hoofd BDE Noord;
- Dhr. H. Dekkers, hoofd BDE Amsterdam-Amstelland;
- Dhr. D. Philippo, medewerker BDE Amsterdam-Amstelland;
- Dhr. A. Olie, hoofd BDE Rotterdam-Rijnmond;
- Dhr. G. Philips, medewerker BDE Rotterdam-Rijnmond;
- Dhr. F. Kolkman, hoofd BDE Oost;
- Dhr. B. Idema , hoofd BDE Utrecht;
- Dhr. Ir. J. van Oss, Coördinator opsporing, Divisie recherche, KLPD;
- Dhr. L. Lamers, Digitaal rechercheur, Divisie recherche, KLPD;
- Dhr Z. Geradts, Nederlands Forensisch Instituut (NFI);
- Dhr. H.G. den Dunnen, Implementatiemanager innovatie- en informatie-management, FIOD;
- Een tweetal veiligheidsexperts van banken/ cc- maatschappijen;
- Dhr. T. Kuik, Buma Stemra;
- Dhr. C. Cordeiro, SVB Forensic Accounting & Consultancy.

Bijlage B Zoeken op internet

Het zoekproces werd begonnen met het intypen van trefwoorden in zoekmachines op internet zoals altavista.com of google.nl. Het trefwoord cybercrime levert overwegend referenties op naar de categorie new crimes- new tools. Het spectrum van ernst van de criminaliteit varieert daarbij van zogenaamde script kiddies die zonder veel kennis van zaken vrij verkrijgbare scripts loslaten op de schoolserver, tot staten die elkaar dreigen met ontregeling van het economisch functioneren en het militair systeem.

"Fraud" en "scam", eventueel in combinatie met digital levert meer informatie op in het segment old crimes-new tools. Een buitengewone rijke site is de Ward Chipman Library, onderhouden door de University of New Brunswick Saint John (www.unbsj.ca/library/subject/crim1.htm) en dan het onderwerp Computer Crime. De verdere zoektocht vanuit dit vertrekpunt leverde de volgende belangrijke overzichts-sites op:

- Crimes of Persuasion (www.crimes-of-persuasion.com;
- Internet scams (www.ccmostwanted.com/scams.htm);
- The National Fraud Center (www.fraud.org);
- Consumer Protection (www.ftc.gov/ftc/consumer.htm);
- United Nations Manual on the prevention and control of computer-related crime (www.uncjin.org/Documents/EighthCongress.html);
- Office of Consumer and Business Affairs (www.ocba.sa.gov.au/scam_scamex.htm);
- A Report of the President's Working Group on Unlawful Conduct on the Internet(www.nctp.org/unlawful1.html). In deze referentie wordt een voorzet gegeven tot de systematisering van de zeven aspecten, zoals verder uitgewerkt in dit rapport.

Bij het aflopen van de diverse links is gekeken naar:
- wijze van systematisering van de verschijningsvormen van cyber criminaliteit;
- kwantitatieve informatie wat betreft frequentie, aantallen en gemiddelde schade;
- betere trefwoorden;
- onverwachte, bijzondere listige of potentieel grootschalige fraudeschema's;
- nieuwe links, met name ook naar andere landen dan de US en Canada.

Met de belangrijkere trefwoorden is hiernaast gezocht in het Nederlands-, Duits- en Franstalige domein. Dat leverde niet veel andere informatie op; vaak wordt toch weer gerefereerd aan de Engelstalige websites.

Bijlage C Bevindingen uit de hackers-scene

Van 9 tot en met 12 augustus werd in Enschede de conferentie Hackers At Large (HAL2001) gehouden. Deze conferentie was een vervolg van de HIP 97 (Hacking in Progress) bijeenkomst, die ook in Enschede werd gehouden.

In de media en in de 'popular opinion' worden Hackers nog wel eens verantwoordelijk gehouden voor veel computercriminaliteit die in de wereld voorkomt. Men kan daarbij denken aan DoS (Denial of Service) Attacks op computers, het 'defacen' van websites en het kraken van webwinkels om creditcardgegevens te stelen. Ook zouden zij toegang kunnen krijgen tot allerlei vertrouwelijke en gevoelige informatie die op de computersystemen van bedrijven en overheden aanwezig zijn. Voor de onderzoekers was deze beeldvorming een goede reden om te bestuderen waar deze hackers nu eigenlijk mee bezig zijn. De HAL bleek daarvoor een uitgelezen kans.

Wij hebben twee dagen op de camping gebivakkeerd, diverse workshops bijgewoond en geprobeerd met mensen uit de Hackers-scene in contact te komen. Dat laatste was niet eens eenvoudig. Veel aanwezigen op de conferentie waren slecht aanspreekbaar, zelfs voor een 'gewoon praatje'. Dat kon ook moeilijk anders, omdat de een groot deel van de bezoekers gedurende de conferentie de meeste tijd al turend naar het computerscherm doorbracht. Een andere factor die de deelnemers aan de conferentie weerhield van het openlijk spreken met onderzoekers was de gesignaleerde cultuur van 'anarchistische paranoia'. De deelnemers denken – soms ook terecht - dat zij, als specialisten op het gebied van computerbeveiliging, gezien worden als een bedreiging voor bedrijven en overheden. Ze zijn er van overtuigd dat ze dus ook door de politie en geheime dienst in de gaten worden gehouden. De T-shirts met het opschrift 'staatsgevaarlijke anarchisten' werd door een aantal deelnemers aan de conferentie dan ook met trots gedragen.

Activiteiten
Op de Hal werden verscheidene activiteiten georganiseerd. In de eerste plaats werden er een aantal workshops en lezingen gehouden met een groot aantal uiteenlopende onderwerpen, zoals:

- DDos: analysis, detection and mitigation techniques;
- oppurtunistic encryption in IP security;
- web searching techniques and avoiding advertisements;
- drugs and thought crime;
- wearable computers;
- tracking a hacker.

De nadruk bij de workshops en lezingen lagen voornamelijk op het gebied van computerbeveiliging en – protocollen. Buiten het hoofdprogramma werden er ook demonstraties gehouden van allerlei andere zaken – al dan niet jolige activiteiten als lockpicking (leden van de Vereniging voor Hang en Sluitsport), Ritual Microsoft Manual Burning, jongleren, etc., etc.
Ook werd er een presentatie gehouden van de mensen die in Nederland het hacking- magazine 'Klaphek' hebben opgezet. Hiernaast kwamen de meeste bezoekers ook simpelweg om hun laptop of desktopcomputer in het netwerk van de HAL te pluggen en met elkaar spelletjes te spelen, informatie uit te wisselen, te chatten en elkaar computer proberen te hacken.

Hiervoor werden ook verschillende wedstrijdjes georganiseerd. Overal op de camping zag men dan ook het blauwachtige licht van computermonitoren uit de tenten komen.

Hacking en criminaliteit
In de eerste plaats moeten wij vooropstellen dat op het terrein van de HAL zelf naar onze informatie weinig delicten zijn gepleegd. Overal op de camping lag de computerapparatuur hoog opgestapeld: laptops, routers, servers en dergelijke, slechts beschermd door tentdoek. Ook de campus was in het geheel niet afgesloten; iedereen die wilde kon er op en eraf. Desondanks zijn bij de politie en de organisatie van het festival nauwelijks meldingen binnengekomen van diefstal en dergelijke.

Voordat de HAL begon was men bezorgd over eventuele pogingen om computers buiten de HAL te hacken als er zoveel hackers bij elkaar komen. Op een eerdere hackersconferentie in de VS werd door een groep hackers in zeer korte tijd enkele honderden websites hadden 'defaced' (de homepage veranderd door in te breken op het systeem). Door de organisatoren van HAL werd dan ook nadrukkelijk opgeroepen om geen hackpogingen te ondernemen tijdens HAL. Wij hebben begrepen uit het interview met het hoofd van de BDE-Oost (en uitspraken van organisatoren onder elkaar die door ons werden opgevangen) dat deze oproep onder enige druk van de BDE op de website is terechtgekomen. Er zijn echter voor zover bekend tijdens de HAL geen hackpogingen vanuit het HAL-netwerk naar buiten toe gemeld.

Uit de uitingen en verklaringen van hackers die wij op de HAL zijn tegengekomen lijkt het er op dat men een enigszins ambivalente houding aanneemt ten opzichte van hacking en criminaliteit. Aan de ene kant doet men er alles aan om het imago van 'gevaarlijke hackers' in stand te houden. Denk hierbij aan de eerder genoemde T-shirts van de 'staatsgevaarlijke anarchisten'. Men lijkt het ergens wel 'stoer' te vinden zo gezien te worden. Dit wordt verwoord door Rop Gonggrijp, één van de organisatoren op de website van HAL:
'Hey, let's not kid each other: we weren't all that good when we were kids. But right now, powerful people all over the world would like to paint a picture of HAL2001 as a gathering of dangerous individuals out to destroy. While it may seem cool to have powerful people think of you as dangerous, you're only...'(.....)'Members of the dutch law enforcement community (yes: cops) are attending in large numbers. '(.....)'And if HAL is anything like its predecessors, intelligence people from internal security agencies of most industrialised nations are walking around, and will see if anyone from their country is sticking their head out doing naughty things.'

Uit dit stuk blijkt dat de organisatoren ruiterlijk toegeven dat zij zelf geen lieverdjes zijn (of waren). Ook worden in dit stuk twee van de drie verdedigingslijnen duidelijk die worden opgetrokken om de activiteiten van hackers te rechtvaardigen. Deze zijn eigenlijk drieledig. Aan de ene kant worden de activiteiten van hackers gebagatelliseerd: hacking wordt gezien als een spelletje, in het ergste geval als een dolletje, een 'prank'. Te vergelijken met belletje trek. ('We weren't all that good when we were kids '). Hackers als onschuldige knutselaars. Zoals één van de leden van de redactie van 't Klaphek magazine het uitdrukte tijdens een presentatie over het werk van hun 'hack en phreakclubje' 'Wij willen gewoon weten hoe iets werkt of in elkaar zit'. Min of meer onschuldige grapjes dus. Op dezelfde presentatie lieten zij echter weten nu op zoek zijn naar het algoritme van de KPN Hi-prepay opwaardeerkaarten voor pre-paid abonnementen op mobiele telefoons.

Zodra dit algoritme gevonden zou worden, dan kan iedereen de nummers op deze kaarten zelf genereren en voor niets zijn of haar beltegoed opladen.

De tweede legitimatie die Hackers gebruiken om hun 'onderzoekswerk' te rechtvaardigen is de politieke component: In het eerder aangehaalde stuk van Gongrijp wordt de politieke legitimatie van de hackers- beweging onderstreept:

> 'We feel there are important things going on in the world today. Things worth fighting against. Governments and large corporations are basically taking over and are in the process of building mechanisms of control.....'
> '..... Governments and large corporations are taking control of our world at alarming speed. Hackers are more likely to understand what's going on, and to do something about it. ' Dit is de verdedigingslijn die het meeste thuishoort in de politieke arena; voor het werk van de politie is dit minder interessant.

De derde legitimatie voor het rechtvaardigen van activiteiten van hackers, vooral van het openbreken van computersystemen is de 'klokkeluidersverdediging'. De groep mensen die weten hoe de zaken in elkaar zitten, kunnen ook het beste waarschuwen tegen beveiligingslekken en dergelijke. Hackers zijn door hun nieuwsgierigheid daarvoor de meest geëigende groep. Door beveiligingslekken in computersystemen aan te tonen helpen zij de producenten ervan hun software beter te beveiligen. Wat de 'hackers-wereld' hierbij nog wel eens uit het oog wil verliezen zijn de volgende twee zaken. Ten eerste wordt er door activiteiten van kwaadwillende hackers reële schade geleden. Hiernaast kan de hackers- gemeenschap door het beschikbaar stellen van 'tooltjes' om websites mee te defacen, in te breken op andere computers etc. de wel – criminele hackers de kans geven om deze misdrijven te plegen. De hackers-gemeenschap neemt hierin niet haar eigen verantwoordelijkheid.

Er doen zelfs complottheorieën de rondte dat beveiligingsbedrijven in de computerwereld belang hebben bij de activiteiten van deze hackers. Bij elke andere vorm van criminaliteit zou raar worden opgekeken als vanuit dezelfde groep mensen zowel criminaliteit wordt gepropageerd als bestreden. Ter vergelijking: er bestaat geen wereldwijd netwerk van slotenmakers die inbrekers opleiden. Wat wij ons daarbij moeten realiseren is dat dit niet noodzakelijkerwijze dezelfde mensen hoeven zijn: degenen die de scriptjes maken waardoor de script-kiddies webpagina's kunnen defacen zijn niet dezelfden als diegenen die nu voor beveiligingsbedrijven werken.

Kansen voor opsporingsinstanties
Het omgaan van de politie met de hackers- gemeenschap biedt een aantal kansen. In de eerste plaats bieden conferenties als de HAL de politie een uitgelezen kans om pro- actief aanwezig te zijn. De BDE Oost heeft dit met betrekking tot de HAL goed opgepakt. Waarschijnlijk heeft dit ertoe bijgedragen dat er vanuit de HAL geen hackpogingen buiten het eigen netwerk zijn ondernomen. Ook kan de politie zo op de hoogte blijven van wat er de actuele ontwikkelingen op technisch gebied zijn. Hiernaast kan de 'digitale politie' de ontwikkelingen in de 'hackers-scene' heel goed op het internet in de gaten houden. De meeste hackers vertellen maar wat graag aan de buitenwereld wat zij hebben 'gepresteerd'.

Hiernaast hebben de 'goedwillende' hackers en opsporingsinstanties gedeeltelijk ook een zelfde doel: de voorlichting over het beveiligen van computersystemen moet beter. End-users, de gewone gebruikers van hardware en

software, moeten ervan doordrongen zijn dat zij aandacht moeten besteden aan de beveiliging van hun computers. Die aandacht ziet men nu al doorbreken bij de ISP's, die als onderdeel van hun internet- abonnement antivirus software beschikbaar stellen. Een ander gezamenlijk doel is het voorlichten van beleidsmakers die zijn nog niet altijd geheel 'digitally aware'. Men kan zich daarbij bijvoorbeeld premier Kok herinneren, die dacht dat een computer te kunnen bedienen door een computermuis op het beeldscherm te richten als ware het een afstandbediening. Beleidsmakers binnen de politie met te weinig kennis van de technische kant van ICT kunnen beleid voorbereiden dat technisch niet uitvoerbaar is of zeer onwenselijk. Dit zelfde probleem doet zich voor bij wetgevers die onbeslagen ten ijs komen. Men kan hierbij denken aan de 'nummerportabiliteit' van IP- adressen voor als men van ISP wisselt of de onlangs voorgestelde opt-out regeling voor Spam die door het Europees parlement wordt voorgesteld.

Een schrijnend voorbeeld van het gebrek aan kennis bij beleidsmakers wordt gepresenteerd in de film 'Free Kevin'. Hierin wordt het de gevangengezette hacker Kevin Mitnik verboden de publieke telefoon in de gevangenis te gebruiken, omdat de gevangenisdirecteur bang zou zijn dat hij deze telefoon zou gebruiken om zich een 'weg naar buiten te hacken'. Uiteraard is dit een technische onmogelijkheid, maar de gevangenisdirecteur wist zo weinig van technologie dat hij dit voor mogelijk achtte. Meer verspreiding van technische kennis in de justitiële keten zou ook hier op zijn plaats zijn.

Bijlage D Literatuur

Voor dit rapport is, naast de al in het rapport genoemde informatie op het internet, de volgende literatuur bestudeerd.

- *Beveiliging van persoonsgegevens,* Registratiekamer, Den Haag, 2001
- *BreinInfo*, periodiek Stichting Brein, Haarlem/ Hoofddorp
- *Kinderpornografie en Internet in Nederland.* Stichting Profit for the World's Children, Heemstede
- *Causes and Implications of Disinhibited Behavior on the Internet*, Adam Joinson, Chapter 3: Psychology and the Internet: intrapersonal, interpersonal and transpersonal implications. Academic Press, 1998
- *Criminal threats to E-commerce*, Marc D. Goodman, Baltazar Rodrigues, Clive Blake, Robert Maierhofer, Alessandro Carini, Semih Dokurer, Kai Küllmer (European working party on information technology and crime, Interpol), Interpol, 2001.
- *Computercriminaliteit*, Chr. H. van Dijk en J.M.J. Keltjens, 1995 , W.E.J. Tjeenk Willink, Zwolle.
- *Criminaliteit in Cyberspace, een praktijkonderzoek naar aard, ernst en aanpak in Nederland*, W.Ph. Stol, R.J. van Treeck, A.E.B.M. van der Ven, In-pact Onderzoeksteam, 1999, Elsevier bedrijfsinformatie bv.
- *Cyberpayments and Money Laundering* , R.A Molander, L. A. Mussington, P. A. Wilson, Critical Technology Institute, Rand Institute Washington, 1998
- *Digitaal blauw..., aan de slag met digitaal rechercheren,* (folder) Landelijk Projectbureau Digitaal Rechercheren, december 2001.
- *Digitaal blauw..., Herijking nationaal actieprogramma,* Cees, Verschuur, Richard Vriesde, Frans Kolkman en Eric Loermans (Beleidsadviesgroep Digitaal Rechercheren), 2001.
- Dossier Computerbeveiliging, NRC Handelsblad, http://www.nrc.nl/W2/Lab/Beveliging/
- *Een digitaal dijkenplan,* in Tijdschrift over samenleving en criminaliteitspreventie, Januari 2002, 16e jaargang, nummer 1.
- *Goed werken in netwerken – Regels voor controle op e-mail en internetgebruik van werknemers,* Registratiekamer, Den Haag, 2001
- *Het KWICT- instituut, Advies van het 24-uurs ministerie kwetsbaarheid ICRT- infrastructuur*, denktank Infodrome (Ministerie van OCW), Amsterdam

- Jaarverslagen 1999 en 2000, Bureau Digitale Expertise Politie Oost Nederland, Nijmegen

- *In Total Self/Control,* Marcel Bullinga, Ten Hagen Stam, Den Haag 2002

- *Internet Investigations, case studies*, Paolo Abalada, Luc Beirens, Eric Freyssinet, Tuomas Lahmusmetsa (European working party on information technology and crime, Interpol), Interpol, 2001.

- *Internet misuse and elementary internet investigations,* Luc Beirens, Claudio G. Frigerio, Brian Gardner, Tom Erik Guttlusrod, Louis Maatman, Nicolas Dewhirst, Vittor Agostinho, Rogerio Bravo (European working party on information technology and crime, Interpol), Interpol, 1999.

- *Inzet van ICT bij fraudeonderzoek niet meer weg te denken,* in Security & Forensic news, Ernst & Young, November 2001, nummer 4.

- *Jaarbericht 2000*, InterPay Nederland, 2001.

- *Means, Motive and Opportunity,* Lawrence R. Rogers, Software Engineering Institute Carnegie Mellon University, 2001

- *Nemo Plus.* Prof. Mr. Franken, afscheidsrede uitgesproken aan de Universiteit Leiden op 14 september 2001

- *Opsporing locaties verzocht,* Casper van Nassau & Bert Bulder, Research voor Beleid, Leiden.

- *Six- Month Data Trends Rapport may- november 2001*, Internet Fraud Complaint Center, FBI

- *Sleutels van vertrouwen, TTP's digitale certificaten en privacy,* Registratiekamer, Den Haag, 2001

- *Trends in Denial of Service Attack Technology*, K.J. Houle & G.M. Weaver, CERT Coordination Center, 2001

- *Verslag expertmeeting Politie & Wetenschap deel 'Policing Cyberspace, politiele handhaving in de virtuele ruimte'*, Kurhaus, Scheveningen,

  25 januari 2001.