High-tech crime, soorten criminaliteit en hun daders

264

Onderzoek en beleid

High-tech crime, soorten criminaliteit en hun daders

Een literatuurinventarisatie

R.C. van der Hulst

R.J.M. Neve

BJu | Boom Juridische uitgevers

Justitie **Wetenschappelijk Onderzoek- en Documentatiecentrum**

Onderzoek en beleid

De reeks Onderzoek en beleid omvat de rapporten van onderzoek dat door en in opdracht van het WODC is verricht.
Opname in de reeks betekent niet dat de inhoud van de rapporten het standpunt van de Minister van Justitie weergeeft.

Exemplaren van dit rapport kunnen worden besteld bij het distributiecentrum van Boom Juridische uitgevers:
Boom distributiecentrum te Meppel
Tel. 0522-23 75 55
Fax 0522-25 38 64
E-mail bdc@bdc.boom.nl

Voor ambtenaren van het Ministerie van Justitie is een beperkt aantal gratis exemplaren beschikbaar.
Deze kunnen worden besteld bij:
Bibliotheek WODC
Postbus 20301, 2500 EH Den Haag
Deze gratis levering geldt echter slechts zolang de voorraad strekt.

De integrale tekst van de WODC-rapporten is gratis te downloaden van www.wodc.nl.
Op www.wodc.nl is ook nadere informatie te vinden over andere WODC-publicaties.

ISBN 978 90 5454 998 7
NUR 824

Voorwoord

In het digitale tijdperk worden kernprocessen in de samenleving veelvuldig aangestuurd vanuit Informatie- en Communicatie Technologie (ICT) en digitale technieken. High-tech crime vormt wereldwijd in toenemende mate een financieel en maatschappelijk probleem. Het gaat zowel om klassieke vormen van criminaliteit die door ICT worden gefaciliteerd (bijvoorbeeld kinderporno, fraude en oplichting) als om nieuwe criminele activiteiten waarbij ICT behalve middel ook expliciet doelwit is (bijvoorbeeld hacking, phishing en het manipuleren van computergestuurde data en systemen). De preventie en bestrijding van high-tech crime vormt dan ook één van de speerpunten in het Nederlandse en Europese veiligheidsbeleid. Echter, het ontbreken van een gemeenschappelijk begrippenkader en het gebrek aan kennis over (kenmerken van) daders van high-tech crime (waaronder de betrokkenheid van de georganiseerde criminaliteit) vormen een belangrijke lacune voor een efficiënte en effectieve aanpak.

Dit rapport doet – tegen die achtergrond – verslag van een een verkennend en inventariserend literatuuronderzoek over de verschillende verschijningsvormen, daders en georganiseerde netwerken van high-tech crime. Het rapport is rijk aan bevindingen maar toont ook waar kennislacunes zijn. De studie vormt daarmee tevens een belangrijke aanzet voor de programmering van onderzoek op dit terrein.

Prof. dr. Frans Leeuw
Directeur WODC

Dankwoord

Het Coalitieakkoord 2007 en het Beleidsprogramma 2007 benadrukken de noodzaak om de preventie en de bestrijding van high-tech crime in de komende jaren verder te versterken. Dit rapport is een verkennend en inventariserend literatuuronderzoek over de verschillende verschijningsvormen, daders en georganiseerde netwerken van high-tech crime. Het levert een belangrijke aanzet voor de nadere onderzoeksprogrammering en voor het ontwikkelen van meer toegesneden beleidsmaatregelen op het gebied van preventie, opsporing en handhaving van high-tech crime. Wij willen dan ook iedereen bedanken die een bijdrage heeft geleverd aan de totstandkoming van dit rapport. Verschillende Nederlandse deskundigen hebben hun expertise op het gebied van high-tech crime met ons gedeeld. Wij danken Jaap van Oss (KLPD/Europol), Gert Wabeke en Phons Bloemen (KPN Security), Raoul Bhoedjang (NFI), Henk Klap (NPI), Wouter Stol (Noordelijke Hogeschool Leeuwarden), John Remmerswaal en Ellen Rossieau (OM/Landelijk Parket Rotterdam) en Pascal Hetzscholdt voor hun coöperatieve samenwerking. Ook bedanken wij de leden van de begeleidingscommissie (zie bijlage 1) voor hun visie, nuttige aanwijzingen, adviezen, kennisuitwisseling en betrokkenheid.

Renée van der Hulst en Rudie Neve[1]

1 Rudie Neve heeft als onderzoeker van het WODC meegewerkt aan dit rapport. Op dit moment is hij werkzaam als onderzoeker bij de Dienst Nationale Recherche Informatie (DNRI) van het Korps Landelijke Politiediensten (KLPD) in Zoetermeer.

Inhoud

Afkortingen

AHTCC	Australian High Tech Crime Centre
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
BDE	Bureau Digitale Expertise
BREIN	Bescherming Rechten Entertainment Industrie Nederland
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CD	Compact disc
CITI	Critical Information Technology Insiders
CP	Cyberpunk hacker
CSV	Crimineel samenwerkingsverband
DNRI	Dienst Nationale Recherche Informatie
DOS	Denial of service
dDoS	Distributed denial of service
DRC	Directie Rechtshandhaving en Criminaliteitsbestrijding
DTN	Dreigingsbeeld Terrorisme Nederland
DVD	Digital video disc
EC	Europese Commissie
EK	Eerste Kamer der Staten-Generaal
EU	Europese Unie
Europol	European Police Office
EZ	Ministerie van Economische Zaken
FBI	Federal Bureau of Investigation
FIOD-ECD	Fiscale Inlichtingen- en Opsporingsdienst en de Economische Controle Dienst
HKS	Herkenningsdienstsysteem van het KLPD
HTC	High-tech crime
HT-CSV	High-tech crimineel samenwerkingsverband
HTCIA	High Technology Crime Investigation Association (Verenigde Staten)
ICT	Informatie- en Communicatie Technologie
IW	Information warrior hacker
IRC	Internet relay chat
IT-er	ICT'er
IT	Internal hacker
KKK	Ku Klux Klan
KLPD	Korps Landelijke Politiediensten
KPN	Koninklijke PTT Nederland
LP	Landelijk Parket
MBO	Middelbaar beroepsonderwijs
MCC	Meldpunt Cybercrime
MDI	Meldpunt Discriminatie Internet
MKB	Midden- en kleinbedrijf
MKI	Meldpunt Kinderporno op Internet
MPEG	Motion Pictures Experts Group
MSN	Microsoft Network Messenger
MvJ	Ministerie van Justitie

NCJRS	National Criminal Justice Reference Service
NCTb	Nationaal Coördinator Terrorismebestrijding
NDB	Nationaal Dreigingsbeeld
NFI	Nederlands Forensisch Instituut
NHTCC	Projectgroep National High Tech Crime Center (Nederland)
NHTCU	National Hi Tech Crime Unit (Verenigd Koninkrijk)
NIBC	Nationale Infrastructuur Bestrijding Cybercrime
NICC	Nationale Infrastructuur ter bestrijding van Cyber Crime
NPAC	NPC-project Aanpak Cybercrime
NPC	Nationaal Platform Criminaliteitsbestrijding
NIJ	National Institute of Justice (Verenigde Staten)
NPI	Nederlands Politie Instituut
NSA	National Security Agency (bureau nationale veiligheid Verenigde Staten)
NV	Novice hacker
OG	Old guard hacker OM Openbaar Ministerie
PA	Political activist hacker
PA	Politieacademie
PC	Professional criminal hacker
PCA	Parliament of the Commonwealth of Australia
PDA	Personal Digital Assistant
PGP	Pretty good privacy
PT	Petty thief hacker
P2P	Peer to peer
RFID	radio frequency identification
RIVM	Rijksinstituut voor Volksgezondheid en Milieu
SCADA	Supervisory Control and Data Acquisition
SMS	Short message service
SOCA	Serious Organised Crime Agency (Verenigd Koninkrijk)
THTC	Team High-Tech Crime
TK	Tweede Kamer der Staten-Generaal
V-NDB	Vervolgstudie NDB
VNO-NCW	Vereniging van het Verbond van Nederlandse Ondernemingen (VNO) en de Nederlandse Christelijke Werkgeversbond (NCW)
VoIP	Voice over IP
VW	Virus writer hacker
WED	Wet Economische Delicten
WLM	Windows Live Messenger
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum
WOG	Wet op de Geneesmiddelenvoorziening
Wok	Wet op de kansspelen
WWM	Wet Wapens en Munitie
XTC	Ecstasy
7KP	Zevende Kaderprogramma voor Onderzoek en Technologische Ontwikkeling

Samenvatting

In het digitale tijdperk waarin wij leven worden kernprocessen in de hele samenleving veelvuldig aangestuurd door ICT en digitale technieken. Wereldwijd neemt in het laatste decennium het gebruik van ICT en het internet, zowel door bedrijven als door particulieren, steeds verder toe. Onze samenleving is voor haar functioneren sterk afhankelijk geworden van een goed functionerend netwerk van digitale en interconnectieve systemen. Deze afhankelijkheid wordt gaandeweg groter naarmate meer overheden, bedrijven, organisaties en natuurlijke personen hiervan gebruik zullen maken. De specifieke omstandigheden die hiermee gepaard gaan, zoals het toenemende gebruik van netwerken met een open verbinding met het internet, maar ook de anonimiteit en brede bereik van het internet, bieden echter lucratieve mogelijkheden voor het criminele circuit (Van Amersfoort e.a., 2002). De mogelijkheden voor het plegen van allerlei criminele activiteiten, hier beschreven als 'high-tech crime', zijn de laatste jaren fors toegenomen (NHTCC/NPAC, 2006a: 6). De financiële, economische en maatschappelijke gevolgen van high-tech crime kunnen voor onze samenleving vérdragende consequenties hebben. Niet alleen is het zaak dat de kernprocessen in onze samenleving goed kunnen blijven functioneren en zich verder kunnen blijven ontwikkelen, ook het vertrouwen van de gebruiker in een veilige ICT-wereld is van cruciaal belang. De preventie en bestrijding van high-tech crime vormt dan ook één van de speerpunten in het Nederlandse en Europese veiligheidsbeleid. Het gebrek aan kennis over de daders van high-tech crime en over de betrokkenheid van de georganiseerde criminaliteit vormen een belangrijke lacune voor een efficiënte en effectieve aanpak. Dat was voor het Ministerie van Justitie aanleiding om een *literatuur*inventarisatie uit te laten voeren, waarin de stand van zaken en kennis op het gebied van high-tech crime en in het bijzonder kennis over de daders ervan (de georganiseerde misdaad inbegrepen) in kaart wordt gebracht. De volgende zes onderzoeksvragen staan centraal in deze studie:

- Wat verstaan we onder het begrip high-tech crime?
- Welke verschijningsvormen van high-tech crime kunnen worden onderscheiden?
- Hoe zijn de daders (of dadergroepen) van high-tech crime te karakteriseren?
- In hoeverre is de georganiseerde misdaad betrokken bij high-tech crime?
- Wat zijn de lacunes in de literatuur in kennis over daders van high-tech crime?
- Welke ontwikkelingen op het gebied van high-tech crime zijn de eerstkomende jaren te verwachten?

Per onderzoeksvraag worden de belangrijkste bevindingen samengevat en enkele aandachts- en discussiepunten worden geëvalueerd voor de nadere invulling van de onderzoeks- en beleidsprogrammering op het gebied van high-tech crime.

Wat is high-tech crime?

Uit de literatuur is gebleken dat het niet eenvoudig is om het criminaliteitsterrein van high-tech crime eenduidig te definiëren. Een gemeenschappelijk begrippenkader ontbreekt en verschillende definities worden door elkaar heen gebruikt. De grote verwevenheid tussen klassieke vormen van criminaliteit (zoals fraude en diefstal) met geavanceerde ICT- en digitale technieken en tegelijkertijd het ontstaan van nieuwe criminele markten, maakt het criminaliteitsterrein oneindig breed en moeilijk af te bakenen. Het resultaat is dat onderzoekers en beleidsmakers, maar ook mensen binnen de opsporing, bestrijding en vervolgingsketen geneigd zijn om langs elkaar heen te praten: identieke begrippen ter omschrijving van een fenomeen kunnen voor betrokkenen een andere betekenis hebben en omgekeerd (uiteenlopende begrippen worden gebruikt terwijl ze feitelijk refereren aan hetzelfde probleem) en sommigen hanteren een smaller definitiekader dan anderen. Het criminaliteitsterrein zelf wordt door verschillende mensen ook uiteenlopend bestempeld. Zo zien we dat begrippen als cybercrime (of cybercriminaliteit) en high-tech crime veelvuldig als equivalenten van elkaar worden gebruikt, maar ook andere terminologieën als ICT-, internet-, digitale, e- of informatiecriminaliteit zijn begrippen die geregeld opduiken. Dit gebrek aan overzicht en consistentie schept verwarring en komt de aanpak, kennisuitwisseling en samenwerking op het gebied van high-tech crime niet ten goede.

In dit rapport hanteren wij '*high-tech crime*' als overkoepelend containerbegrip dat verwijst naar een veelheid aan criminele activiteiten waarbij gebruik wordt gemaakt van ICT. De criminele activiteiten kunnen gericht zijn tegen personen, eigendommen en organisaties (waarbij ICT als middel wordt ingezet), of tegen elektronische communicatienetwerken en informatiesystemen (waarbij ICT zowel middel als doelwit is). Ten opzichte van de term cybercrime biedt high-tech crime een breder en meer dynamisch perspectief dat beter aansluit bij de snelle technologische ontwikkelingen in de tijd. Nieuwe criminaliteitsvormen die kunnen ontstaan door innovaties van ICT (en niet alleen het internet) worden door dit containerbegrip afgedekt, wat per definitie inhoudt dat high-tech crime geen statisch containerbegrip is. Voor een nader onderscheid tussen klassieke delicten en nieuwe criminaliteitsvormen die door ICT zijn ontstaan maken we in dit rapport nog onderscheid tussen twee subcategorieën van high-tech crime. Daar waar ICT expliciet als middel én doelwit kan worden aangemerkt, spreken we van *computercriminaliteit*. Bij alle overige aan ICT gerelateerde (vaak klassieke) delicten spreken we van *cybercriminaliteit*. Beide subcategorieën kennen verschillende verschijningsvormen die sterk met elkaar verweven zijn en veelal in combinatie met elkaar worden gepleegd. Kenmerkend aan de verschijningsvormen

van computercriminaliteit (bijvoorbeeld hacking en het verspreiden van virussen) is dat zij een sterk technisch, virtueel karakter hebben: zij zijn ontstaan door, en kunnen niet bestaan zonder ICT. De verschijningsvormen van cybercriminaliteit daarentegen zijn doorgaans traditionele delicten die ook zonder tussenkomst van ICT gepleegd kunnen worden (bijvoorbeeld kinderporno en afpersing) maar door het gebruik van ICT een nieuwe (efficiëntere) uitvoering hebben gekregen door de inzet van geavanceerde technische middelen.

Wat zijn de verschijningsvormen van high-tech crime?

In dit rapport wordt een holistisch perspectief gehanteerd om zoveel mogelijk kennis te inventariseren over daders van high-tech crime. Daartoe hebben we de verschillende verschijningsvormen van cyber- en computercriminaliteit aan de hand van de literatuur in acht themaclusters als volgt gecategoriseerd (zie ook schema 2 in hoofdstuk 2).

Cybercriminaliteit:
1. legale communicatie en afscherming;
2. illegale handel;
3. financieel-economische criminaliteit;
4. illegale communicatie.

Computercriminaliteit:
5. ongeautoriseerde toegang tot ICT;
6. ICT-storing door gegevensverkeer;
7. ICT-storing door manipulatie van data en systemen;
8. dienstverleners.

Deze indeling is een voorlopige inventarisatie en dient als kapstok voor de doorontwikkeling van een typologie van high-tech crime. Dit overzicht is nodig om een aanzet te kunnen geven voor de verdere kennisopbouw en beleidsvorming in de preventie en bestrijding van high-tech crime. De indeling kan echter te allen tijde worden aangepast en gevoed met nieuwe en aanvullende inzichten. Voor elk van bovengenoemd themacluster en de bijbehorende verschijningsvormen volgt hierna een korte beschrijving.

Cybercriminaliteit

Cybercriminaliteit refereert aan het gebruik van ICT als instrument voor het plegen van uiteenlopende delicten. In veel gevallen gaat het om de ondersteunde functie van ICT ten behoeve van communicatie (tussen daders onderling of tussen daders en slachtoffers), maar bijvoorbeeld ook

voor het verrichten van (vrijwillige of onvrijwillige) transacties met goederen en diensten en financiële transacties.

Legale communicatie en afscherming
ICT heeft een veelheid aan gebruiksfuncties. In het kader van criminaliteit fungeert het internet bijvoorbeeld als virtuele inspiratiebron, als virtuele ontmoetingsplaats en als platform voor kennisuitwisseling en (afgeschermde) communicatie. Wanneer deze gebruiksfuncties worden ingezet in het kader van *illegale* doelstellingen (bijvoorbeeld rekrutering van radicale jongeren), spreken we in dit rapport van cybercriminaliteit. We onderscheiden binnen dit cluster drie thema's: radicalisering en extremisme, terrorisme en ideologisch gemotiveerde misdaad, en innovatieve afscherming met behulp van ICT. Zowel bij radicalisering als bij terrorisme speelt het internet een prominente rol. Het internet leeft, vooral onder jongeren, en zij laten zich over en weer inspireren en motiveren tot extremistische uitingen. Ook wordt het internet gebruikt om kennis te vergaren (handboeken die worden geraadpleegd of andere operationele kennis) en mensen te mobiliseren. In de literatuur is een tendens waarneembaar van publicaties die gericht zijn op de invloed van het islamistisch radicalisme (en in mindere mate van andere radicale stromingen). Dit kan ten koste gaan van de kennisontwikkeling in brede zin en leiden tot tunnelvisie waardoor belangrijke trends en indicaties aan het bewustzijn voorbij gaan. Radicalen, terroristen en mensen in het criminele circuit maken gebruik van innovatieve technieken om de communicatie mee af te schermen voor onbevoegden (waaronder de opsporing). Dit varieert van slimme vindingen (zoals het voortdurend wisselen van niet-geregistreerde mobiele telefoons of het gebruik van 'dead letter boxes' waarbij concept-e-mailberichten door meerdere gebruikers kunnen worden ingezien en aangepast zonder dat berichten daadwerkelijk worden verzonden) tot geavanceerde technieken als encryptie (waarbij de inhoud van berichten wordt versleuteld met codes) en steganografie (waarbij het hele bestaan van een bericht wordt verhuld door deze bijvoorbeeld in een afbeelding of digitale clip te verwerken). In sommige gevallen worden hiervoor experts ingehuurd.

Illegale handel
Via het internet kan onbeperkt en zonder veel moeite een diversiteit aan handel worden gedreven. Dit is een groeimarkt in onze huidige economie, maar gaat net zo goed op voor illegale goederen en diensten die via digitale weg worden verhandeld. De (inter)nationale literatuur biedt weinig zicht op de illegale handel in drugs, vuurwapens en explosieven, en mensenhandel- en smokkel. Op grond van deze studie is niet te bepalen of dit indicatief is voor de *mate* waarin gebruik wordt gemaakt van het internet of dat er een gebrek is aan opsporing, onderzoek en publicaties waardoor de kennis ontbreekt. Vooralsnog lijkt ICT bij deze handelsvormen vooral

een ondersteunende *communicatieve* functie te hebben. De relatieve anonimiteit van internetgebruikers en het gebrek aan sociale controle en face-to-face contact kunnen voor deze criminele markten het gebruik van internet juist tegengaan. Er zijn echter verschijningsvormen waarvoor het internet wel een belangrijke economische marktplaats en distributiekanaal is voor het verhandelen van goederen en diensten. Zo worden er op grote schaal merkvervalste geneesmiddelen, geneesmiddelen zonder recept, kinderporno, gestolen goederen, illegale software (softwarepiraterij) en illegale kansspelen aangeboden. Met name de grote afzetmarkten en de relatief geringe pakkans voor deze handel maakt het internet een populair en veelgebruikt middel. Vooral de handel in kinderporno, waarbij ook het materiaal zelf in digitale vorm wordt aangeboden, wordt in toenemende mate afgeschermd met behulp van geavanceerde technieken.

Financieel-economische criminaliteit
Bij financieel-economische criminaliteit wordt onrechtmatig voordeel behaald door fraude, oplichting en bedrog. Met name internetfraude is een veelvoorkomend probleem en vormt een bedreiging voor de Nederlandse samenleving. Mensen wordt onder valse voorwendselen geld uit de zak geklopt (voorschotfraude) of met behulp van ICT wordt op slinkse wijze vertrouwelijke informatie verkregen (identiteitsfraude) waarmee vervolgens bank- en creditcardfraude kan worden gepleegd. Identiteitsfraude met behulp van phishing, dat eerder een crimineel middel dan doel is, wordt beschouwd als een van de snelst groeiende vormen van niet-gewelddadige criminaliteit. Van de andere thema's (oplichting door marktmanipulatie, afpersing en chantage, en witwassen) is in de literatuur minder informatie terug te vinden. Door de toenemende virtuele geldstromen in het maatschappelijk-economische verkeer (via online veilingsites, elektronische en mobiele commercie) zou witwassen met behulp van ICT in de toekomst een aanzienlijke vlucht kunnen gaan nemen. Ook afpersing van bedrijven die in hun bedrijfsvoering sterk afhankelijk zijn van het internet (e-commerce), of van bedrijven en burgers waarvan belangrijke bestanden en gegevens dreigen te worden beschadigd, openbaar gemaakt of misbruikt, vormt een potentiële bedreiging. Opvallend hier is de sterke verwevenheid tussen varianten van cyber- en computercriminaliteit. Zo kent internetfraude (cybercriminaliteit) een diversiteit aan werkwijzen en technieken zoals phishing, spamming, malware en pharming (zie computercriminaliteit), en de cybervorm van afpersing en chantage is vaak gerelateerd aan het hacken van systemen en het dreigen met een dDoS-aanval waarmee hele systemen kunnen worden gecorrumpeerd (zie computercriminaliteit).

Illegale communicatie
De veelheid aan gebruiksfuncties van ICT en het internet kunnen ook worden gebruikt om boodschappen van *illegale inhoud* uit te dragen.

Het gaat hier met name om activiteiten waarmee de publieke moraal of de persoonlijke levenssfeer van slachtoffers daadwerkelijk wordt aangetast (bijvoorbeeld stalking, discriminatie, of grooming). In dit rapport spreken we dan van illegale communicatie. Wat inhoud betreft verschillen deze digitale gedragsdelicten weinig van de varianten ervan in de 'fysieke wereld'. Vooral discriminatie (of haatzaaien) via het internet is een trend geworden, waarbij verschillende groeperingen elkaar voortdurend provoceren via discussiefora en chatboxen. Een toenemend probleem dat verontwaardiging binnen de samenleving oproept is grooming, waarbij kinderen via chatsites door volwassenen worden benaderd met oneerbare seksuele bedoelingen. In sommige gevallen leidt dit tot een fysieke ontmoeting waarbij daadwerkelijk sprake kan zijn van ontucht en verkrachting van minderjarigen. Van illegale communicatie is ook sprake wanneer op illegale wijze, zonder toestemming computer- en telefoongegevens van derden ongemerkt worden onderschept (spionage). Daarvoor worden methoden en middelen ingezet als hacking, spyware en malware, en kan gebruik worden gemaakt van dienstverleners (bijvoorbeeld corrupt personeel). Ook hier zien we weer de sterke verwevenheid terug tussen cyber- en computercriminaliteit, waarvan vooral het gebruik van spyware (ongemerkt op de computer geïnstalleerde software die gegevens verzamelt en doorstuurt naar een derde partij) en keyloggers (waarbij toetsaanslagen en muisklikken worden doorgestuurd naar een derde partij) in de toekomst zal kunnen gaan toenemen.

Computercriminaliteit

Met computercriminaliteit refereren we in dit rapport aan alle nieuwe vormen van criminaliteit die zonder het bestaan van ICT niet mogelijk waren geweest. Bij de criminele activiteiten wordt ICT niet alleen ingezet als instrument maar is de ICT zelf tevens expliciet doelwit. In de meeste gevallen gaat het om het inbreken, verstoren, manipuleren of wijzigen van systemen dan wel om het ontwikkelen en voorzien van instrumentele middelen die hierbij helpen. We onderscheiden vier themaclusters die hierna worden besproken.

Ongeautoriseerde toegang tot ICT
Voor het ongeautoriseerd toegang verschaffen tot ICT, feitelijk het inbreken op systemen, staan twee elementen centraal: hackers en botnets. Hackers hebben in toenemende mate criminele bedoelingen, zijn steeds vaker financieel gemotiveerd, en verrichten multifunctionele activiteiten die kunnen worden ingezet bij meerdere varianten van computercriminaliteit. Zij kunnen inbreken op (beveiligde) systemen, instrumenten ontwikkelen om ICT-storingen mee te veroorzaken, en verrichten maatwerk waar een grote mate van expertise en technische kennis voor nodig is.

Er is sprake van een 'ondergrondse' subcultuur die overeenkomsten vertoont met het ondergrondse criminele circuit: er is sprake van een eigen identiteit, status is een hoog goed, en er gelden eigen normen en waarden. In toenemende mate laten hackers zich inhuren door traditionele CSV's en in sommige gevallen maken ook Nederlanders deel uit van georganiseerde (Oost-Europese) criminele netwerken in de rol van dienstverlener. Een van de belangrijkste criminele instrumenten die door hackers kunnen worden opgezet zijn botnets. Dit zijn verzamelingen van op afstand bestuurbare computers die instrumenteel zijn voor het plegen van diverse varianten van high-tech crime, vooral spamming, phishing en (afpersing met behulp van) dDoS-aanvallen.

ICT-storing door gegevensverkeer
Het verstoren van de werking van systemen (bijvoorbeeld websites, e-maildiensten of computernetwerken) kan op verschillende manieren worden bereikt. Twee belangrijke varianten die wereldwijd enorm zijn toegenomen zijn (d)DoS-aanvallen en spamming. Bij een (distributed) Denial of Service of (d)DoS-aanval worden bewust massale hoeveelheden gegevens verzonden naar systemen waardoor deze overbelast raken en onbereikbaar worden. Het is een middel dat onder meer voor afpersing van bedrijven wordt ingezet, maar ook een uiting kan zijn van protest, wraak, concurrentie of vandalisme. Bij spamming kunnen ook storingen worden veroorzaakt door het versturen van massale e-mails, maar dit is eerder een neveneffect van digitale marketing en reclame (voor bijvoorbeeld life-style producten en geneesmiddelen zonder recept) dan een concreet doel. Bij internetfraude worden phishing e-mails massaal verzonden om vertrouwelijke informatie van mensen te ontlokken waarmee ze vervolgens worden opgelicht. Hackers bieden zowel bij dDoS-aanvallen als spamming ondersteuning of verrichten deeltaken bij het veroorzaken van doelgerichte storingen.

ICT-storing door manipulatie van data en systemen
Storingen kunnen ook direct worden veroorzaakt door het daadwerkelijk manipuleren (beschadigen, verwijderen, wijzigen of vernietigen) van gegevens en systemen. Malware is het bulkbegrip voor dubieuze '*…computerprogramma's die zonder toestemming van de eigenaar of beheerder draaien op een computer en het systeem iets laten doen naar de wens van een buitenstaander*' (KLPD, DNRI, 2007a: 15). Dergelijke programma's worden door specialisten op maat gemaakt en kunnen ongemerkt vertrouwelijke informatie van gebruikers verzamelen, data en systemen beschadigen (de bekende virussen), of externe toegang verlenen op computers (via de moderne virussen, zogenoemde Trojaanse paarden). Ook complete websites kunnen worden geblokkeerd of gewijzigd (defacing), onder meer als instrument om mensen mee op te lichten (bijvoorbeeld internetfraude door middel van nepwebsites), af te persen, of om uiting te

geven aan protest (hacktivisme). Wanneer ICT-systemen die vitale infrastructuren aansturen (bijvoorbeeld transportsystemen, besturingssystemen in de chemische sector of belangrijke crisis- en informatiediensten) om politieke redenen worden aangetast om grootschalige maatschappelijke ontwrichting te veroorzaken, spreken we in dit rapport van een cyberterroristische aanval. Hoewel er tot op heden nog geen concrete pogingen zijn geweest, vormen vooral de (wraakzuchtige) insiders met kennis en toegang tot de besturingssystemen een bedreiging (zie ook dienstverleners).

Dienstverleners
De inzet van ICT-dienstverleners staat in directe relatie tot de georganiseerde misdaad Niet alleen criminelen maar ook terroristen huren de kennis in van experts om bijvoorbeeld communicatie veilig te stellen voor de opsporing of om instrumenten te ontwikkelen waarmee criminele of terroristische activiteiten worden gefaciliteerd (zoals het opzettelijk vervaardigen, verkopen, verspreiden of ter beschikking stellen van een technisch hulpmiddel, wachtwoord of code waarmee toegang kan worden verkregen tot een geautomatiseerd systeem). In dit rapport onderscheiden we drie vormen van dienstverlening: corruptie van ICT-personeel, infiltratie van criminele ICT'ers, en het inhuren ICT-experts. Werknemers met ICT-bevoegdheden die toegang hebben tot gevoelige bedrijfsgegevens kunnen (door omkoping of bedreiging) hulp verlenen aan criminele partijen van binnenuit een organisatie. We spreken dan van corruptie en verwevenheid tussen boven- en onderwereld. Hoewel de dreiging van corrupte IT'ers in Nederland nog beperkt lijkt, vormen het infiltreren van criminelen als ICT-consultant en het inhuren van experts voor het verlenen van hand- en spandiensten (bijvoorbeeld hackers) een aanzienlijk veiligheidsrisico.

Wat is bekend over de daders?

Het systematisch in kaart brengen van daderkenmerken in de vorm van risico-indicatoren (het prototype daderprofiel) staat bekend als '*profiling*'. Profiling-technieken staan qua ontwikkeling en bruikbaarheid echter nog in de kinderschoenen. Deze techniek leidt niet direct tot het identificeren van de dader(s) van een delict maar geeft een omschrijving van *combinaties van kenmerken* waar dader(s) naar alle waarschijnlijkheid aan voldoen. De effectiviteit van het gebruik van risicoprofielen is tot op heden nog onvoldoende onderzocht (zie ook Van Donselaar en Rodrigues, 2006: 43, 58). Duidelijk is dat het moet gaan om een combinatie van algemene en specifieke kenmerken van daders die voldoende onderscheidend zijn.

Het nadeel van risicoprofielen is dat vooroordelen over bepaalde mensen en groepen worden bevestigd. Zowel in de preventie als in de opsporing zal er onevenredig veel aandacht uitgaan naar bekende risicogroepen. Dit kan leiden tot stigmatisering van onschuldige personen (die toevallig aan deze kenmerken voldoen) en tegelijkertijd tot criminelen die 'onzichtbaar' blijven en dus ten onrechte over het hoofd worden gezien wanneer zij toevalligerwijze niet aan het profiel voldoen. De profiling-techniek is dus beslist niet feilloos en het gebruik ervan vraagt om de nodige voorzichtigheid en nuances. Het gebruik van risicoprofielen als preventief en opsporingsinstrument verdient grote zorgvuldigheid en dient met terughoudendheid te worden gehanteerd. Dit neemt echter niet weg dat inzicht in daderkenmerken aanknopingspunten kan bieden in zowel de preventie als opsporing van high-tech crime. Nader onderzoek zal dit moeten uitwijzen. Omdat de inventarisatie van daderkenmerken in termen van profielen nog niet empirisch wordt ondersteund en gevalideerde instrumenten tot op heden ontbreken, spreken wij in dit rapport van inzicht in het soort daders van high-tech crime en niet van daderprofielen.

Het gebrek aan kennis over daders in een zogenoemde 'intelligence database' is een belangrijke reden voor het gebrek aan ontwikkeling van daderprofielen. Een van de doelstellingen van deze studie was dan ook om de kennis over daders van high-tech crime te inventariseren op basis van (inter)nationale literatuur. In hoofdstuk 3 zijn daderkenmerken in kaart gebracht voor een selectie van verschijningsvormen van high-tech crime waarvoor de dreiging en risico's voor de Nederlandse samenleving als meest urgent worden beschouwd:[2]

1. radicalisering en extremisme;
2. terrorisme en ideologisch gemotiveerde misdaad;
3. kinderporno;
4. grooming;
5. softwarepiraterij;
6. internetfraude;
7. witwassen;
8. cyberterrorisme;
9. hacking;
10. malware;
11. ICT-dienstverleners.

Uit deze inventarisatie bleek onder meer dat vooral *internetfraude* en *hacking* criminele verschijnselen zijn die veelal in combinatie met andere vormen van high-tech crime worden gepleegd. Bij terrorisme, kinderporno, grooming, softwarepiraterij en internetfraude zijn hoofdzakelijk

2 De daderkenmerken van de overige verschijningsvormen van high-tech crime staan in bijlage 6 beschreven.

mannelijke daders betrokken. Het gros van de zedendelicten (kinderporno en grooming) wordt gepleegd door blanke daders terwijl bij terrorisme en internetfraude vooral daders betrokken zijn van Afrikaanse en/of Aziatische afkomst. Hoewel een aanzienlijk deel van de high-tech crimes financieel gemotiveerd is, hebben vooral hackers en schrijvers van malware nogal uiteenlopende motieven voor hun criminele activiteiten (men doet het bijvoorbeeld ook voor de uitdaging, uit ideologie, macht, wraak of vandalisme). Opvallend is dat corrupte ICT'ers en criminelen die actief zijn op het gebied van terrorisme, internetfraude, kinderporno en hacking nogal eens over een strafblad blijken te beschikken. Door de variëteit aan verschijningsvormen en de (summiere) aanwijzingen over de daders, is duidelijk dat er niet kan worden gesproken van 'de' high-tech crimineel maar dat criminelen zich specialiseren op een bepaald vlak. Doordat sommige delicten echter door dezelfde digitale technieken worden gefaciliteerd, wordt het voor de crimineel echter makkelijker om grotere winsten te behalen door dezelfde technieken in te zetten voor meerdere delicten tegelijk.

We moeten echter constateren dat er betrekkelijk weinig bekend is in de literatuur over individuele daders van high-tech crime. De literatuurinventarisatie biedt slechts grove en onvolledige schetsen van daders op basis van een beperkt aantal kenmerken. Vergelijken we bijvoorbeeld de profielschets met indicatoren zoals die werden ontwikkeld voor de FBI (zie bijlage 7), dan ontbreekt het in de literatuur sterk aan specifieke daderkennis, zowel in termen van organisatie (zoals rekrutering), uitvoering (expertise), gedrag (waaronder persoonlijke kenmerken) als van de gebruikte resources. In zijn algemeenheid geldt voor de meeste verschijningsvormen bovendien dat het inzicht ontbreekt in de criminele carrières van daders en in de overlap tussen de verschillende verschijningsvormen van high-tech crime. De informatie die wel te vinden is in de literatuur is doorgaans oppervlakkig, ongestructureerd en summier, en in sommige gevallen deels gebaseerd op anekdotes en hypothesen waarvan de betrouwbaarheid en validiteit niet of nauwelijks te bepalen zijn. Het ontbreekt al met al aan empirisch-wetenschappelijk onderzoek naar daderkenmerken waarin duidelijk onderscheid wordt gemaakt tussen afzonderlijke verschijningsvormen van high-tech crime. Nader inzicht in daders kan worden verkregen door meer probleemgerichte onderzoeken (bijvoorbeeld casestudies). Een literatuurinventarisatie is niet afdoende om gefundeerd uitspraken over daders van high-tech crime te kunnen doen.

Is er sprake van georganiseerde high-tech crime?

Van sommige verschijningsvormen van high-tech crime zijn aanwijzingen dat er sprake is van georganiseerde criminaliteit. We spreken in dit rapport van georganiseerde criminaliteit als: '*…groepen primair gericht zijn op illegaal [financieel of materieel] gewin en systematisch misdaden plegen met ernstige gevolgen voor de samenleving*' (Parlementaire Enquêtecommissie Opsporingsmethoden, Bijlage VII, 1996; Fijnaut e.a., 1998; Kleemans e.a., 1998: 22-23). Hoewel er in de literatuur weinig bekend is over dadergroepen van high-tech crime (het zicht op daders is relatief beperkt), zijn er aanwijzingen dat zowel traditionele CSV's (zoals de Russische en Oost-Europese maffia) betrokken zijn die de benodigde expertise extern inhuren, als nieuwe fluïde HT-CSV's waarbinnen experts (zoals hackers en schrijvers van malware) deeltaken verrichten en hun krachten bundelen. Het KLPD (Boerman en Mooij, 2006) spreekt van een trend naar *diversificatie* waarbij verschillende criminaliteitsvormen in combinatie met elkaar worden gepleegd (bijvoorbeeld hacking, botnets, spamming, malware, pharming, dDoS-aanval, internetfraude, afpersing) en van een trend naar *taakspecialisatie* waarbij criminelen experts inzetten die verantwoordelijk zijn voor verschillende deeltaken voor het plegen van een delict (bijvoorbeeld het ontwikkelen van de instrumenten of het maken van bijvoorbeeld nepwebsites).

In hoofdstuk 4 is een inventarisatie gemaakt van de betrokkenheid van de georganiseerde criminaliteit voor de verschijningsvormen van high-tech crime die eerder als bedreiging voor de Nederlandse samenleving waren gekwalificeerd (zie paragraaf 5.3). Van de in hoofdstuk 3 geprioriteerde verschijningsvormen zijn vooral kinderporno, softwarepiraterij, internetfraude (voorschotfraude en identiteitsfraude), witwassen, hacking en malware financieel lucratieve werkterreinen voor CSV's en HT-CSV's. De opbrengsten zijn groot, zeker als deze worden afgezet tegen de geringe investeringen en risico's. Ook ICT-dienstverleners hebben in toenemende mate criminele bedoelingen en raken betrokken bij georganiseerde criminaliteit. Jongeren met kennis van ICT op universiteiten, computerclubs en via het internet gerekruteerd om te ondersteunen bij malafide praktijken van criminelen. Hetzelfde geldt voor afgestudeerden en computermedewerkers. Dit neemt echter niet weg dat er ook binnen het criminele circuit zelf inmiddels voldoende technische kennis aanwezig kan zijn om zonder hulp van buitenaf een grote slag te slaan. Vooral de handel in botnets is een belangrijke criminele markt binnen de georganiseerde misdaad In Nederland zijn HT-CSV's vooral actief op het gebied van internet- en voorschotfraude. Nederland is bovendien een belangrijke toeleverancier van botnets (die tegen forse betaling te huur worden aangeboden) en belangrijk doelwit van dDoS-aanvallen. Vooral virusschrijvers (van malware en Trojaanse paarden) spelen in dit kader een prominente rol om de

controle over andermans systemen te krijgen en deze te bespioneren. Ook het aanpassen of vernielen van websites (defacing) of het ontwikkelen van nepwebsites waarnaar mensen worden omgeleid (pharming) zijn in toenemende mate activiteiten waarmee grof geld kan worden verdiend.

Voor radicalisering en terrorisme geldt dat activiteiten weliswaar (lokaal) georganiseerd plaatsvinden, maar dat traditionele CSV's hierbij niet betrokken zijn. Van georganiseerde high-tech crime is ook geen sprake bij grooming (dat doorgaans individueel wordt gepleegd) en voor cyberterrorisme geldt dat tot op heden nog geen concrete activiteiten zijn waargenomen. Onderzoek van het KLPD heeft bovendien geen aanwijzingen opgeleverd van samenwerking tussen criminele en terroristische CSV's (Boerman en Mooij, 2006: 86). Overigens zijn terroristische CSV's wel betrokken bij diverse criminele activiteiten, onder meer op het gebied van high-tech crime, om het terrorisme mee te financieren.

Ook hier kunnen we echter niet anders dan constateren dat er over georganiseerde high-tech crime op basis van deze literatuurstudie nog te weinig kan worden gezegd. De inventarisatie biedt een globaal overzicht van de criminele activiteiten (die soms gecombineerd met elkaar worden gepleegd), van het niveau van expertise dat daarvoor nodig is, van de inhuur van experts en dienstverleners, en van het grensoverschrijdende karakter van high-tech crime met zijn internationale connecties. Naar verwachting zal high-tech crime steeds meer het werkterrein worden van de georganiseerde misdaad waarbij telkens nieuwe trends en innovatieve technieken zullen worden toegepast. Specifieke kennis over daders en samenwerkingsverbanden ontbreekt echter in de literatuur, en aanvullend onderzoek (bijvoorbeeld dossieronderzoek) is nodig om de georganiseerde misdaad op het gebied van high-tech crime beter in kaart te brengen.

Wat zijn de lacunes in kennis over daders?

Op basis van deze literatuurinventarisatie kunnen we vaststellen dat er over daders en criminele samenwerkingsverbanden weinig specifieke kennis voorhanden is. In het overzicht zijn de bevindingen op het gebied van inzichten in daders geclassificeerd van 1 (zeer beperkte kennis) tot 4 (zeer goede kennis), met de geprioriteerde thema's van high-tech crime vetgedrukt. In de rijen (van links naar rechts) staat de kennispositie over individuele daders weergegeven, en in de kolommen (van boven naar beneden) de kennis over georganiseerde high-tech crime. Uit het overzicht is voor iedere verschijningsvorm van high-tech crime dus direct af te lezen wat er in de literatuur bekend is over individuele daders en HT-CSV's.

Overzicht: Daderkennis van high-tech crime in de literatuur

	Individuele daderkenmerken			
HT-CSV's	Zeer beperkt	Redelijk	Goed	Zeer goed
Zeer beperkt	**Dierenrechtenactivisme** **Extreem-rechts terrorisme** **Softwarepiraterij** **Identiteitsfraude** **Pharming (internetfraude)** **Witwassen** **Grooming** **Cyberterrorisme** **Hacking** **Novice hacker** **Petty thief hacker** **Old guard hacker** **Virus writer hacker** **Professional criminal hacker** **Information warrior hacker** **Political activist hacker** **Malware** **ICT-dienstverleners** Handel in geneesmiddelen Handel vuurwapens/ explosieven Mensenhandel Drugshandel Heling Illegale kansspelen Marktmanipulatie Spionage Spamming dDoS-aanval Defacing	**Rechts-radicalisme** **Islamistisch radicalisme** **Islamistisch terrorisme** **Cyperpunk hacker** **Internal hacker** Cyberstalkers Discriminatie	-	-
Redelijk	Afscherming Afpersing en chantage	**Kinderporno** **Voorschotfraude**	-	-
Goed	-	-	-	-
Zeer goed	-	-	-	-

Uit het overzicht blijkt dat er *redelijk* wat zicht is op daders van kinderporno en voorschotfraude (zowel in termen van individuele daders als van HT-CSV's), dat er van extreem-rechts en islamistisch radicale en terroristische stromingen *redelijk* zicht is op individuele daderkenmerken (maar niet van HT-CSV's), en dat van enkele hackervarianten (cyberpunk en internal hacker) en gedragsdelicten (cyberstalking en discriminatie) eveneens *redelijk* zicht is op individuele daderkenmerken maar niet van HT-CSV's.[3] Van een aantal technieken (afscherming, afpersing, pharming)

3 In geval van cyberstalking zijn samenwerkingsverbanden door de aard van het delict ook niet aan de orde.

is weliswaar enig zicht op HT-CSV's maar zijn juist de individuele daders erachter relatief onzichtbaar.

Voor geen van de verschijningsvormen wordt de kennis over daders en HT-CSV's als goed of zeer goed gekwalificeerd. Opvallend is dat van het gros van de verschijningsvormen er zeer beperkte kennis in de literatuur te vinden is over daderkenmerken (de cel linksboven in het overzicht is het meest gevuld). En voor veel van de verschijningsvormen die zijn aangemerkt als dreiging voor de Nederlandse samenleving (dierenrechtenactivisme, extreem-rechts terrorisme, softwarepiraterij, identiteitsfraude, pharming, witwassen, grooming, een aantal typen hackers, schrijvers van malware en ICT-dienstverleners)[4] kunnen we concluderen dat er dus sprake is van een gebrek aan kennis. Dit impliceert niet direct dat dergelijke kennis ook binnen de opsporingsdiensten ontbreekt: de huidige conclusies uit dit rapport zijn immers gebaseerd op basis van bestudering van veelal openbare literatuur.

Verwachtingen voor de toekomst

Toename van high-tech crime
De verwachting voor de komende jaren op het gebied van high-tech crime is dat zowel het aantal slachtoffers als de criminele winsten verder zullen toenemen. Daders wisselen snel van werkwijze en de trend van diversificatie (waarbij criminelen zich richten op meerdere activiteiten tegelijk) en taakspecialisatie (waarbij specifieke expertise wordt ingezet voor criminele deeltaken) zal zich verder voortzetten (NHTCC, aangehaald door KLPD/DNRI, 2007a: 36). De criminele activiteiten zullen naar verwachting ook meer afgestemd worden op specifiek doelwitten (zijnde een individu of organisatie), en vooral slachtoffers die de technische kennis van digitale communicatiestructuren nagenoeg ontberen (bijvoorbeeld ouderen) en zich onvoldoende hebben beveiligd zullen hiervan de dupe worden (NHTCC, 2006b: 10-11).

Het internet als plaats delict
De illegale handel op en via het internet zal door het toenemende gebruik van het internet (waarmee de afzetmarkten alleen maar groeien) en de geringe pakkans mogelijk verder gaan toenemen. Door de toenemende virtuele geldstromen is de verwachting bovendien dat internetfraude (en identiteitsdiefstal) de komende jaren de grootste aantallen slachtoffers en financiële schade zullen aanrichten (Taylor en anderen, 2006: 357-383). Ook in het V-NDB2006 wordt identiteitsfraude met behulp van phishing

4 Dat er kennis ontbreekt over daders van cyberterrorisme is evident gegeven dat dergelijke aanslagen nog niet gepleegd zijn.

als stormachtige ontwikkeling beschreven (Boerman en Mooij, 2006: 21, 30). De hoge ADSL-dichtheid, waarbij computers vrijwel permanent in verbinding staan met het internet, maken vooral Nederland een zeer aantrekkelijk werkterrein voor phishers. Het gaat hierbij niet alleen om cybercriminaliteit maar ook om varianten van computercriminaliteit zoals spamming (Ianelli en Hackworth, 2005). Phishing op internet geschiedt recentelijk deels via botnets (netwerken van door malware geïnfecteerde computers die vervolgens door derden vanaf externe locaties worden gecontroleerd). Botnets spelen ook bij vele andere verschijningsvormen een belangrijke rol en vormen dus een aanzienlijke bedreiging (Europol, 15 juni 2006). Doordat botnets kleinschaliger worden gemaakt en gericht wordt op specifieke doelgroepen, worden zij bovendien moeilijker te traceren.[5]

De opkomst van hackers als dienstverleners
Als belangrijkste ontwikkeling op het gebied van georganiseerde misdaad en high-tech crime moet worden aangemerkt de inzet van ICT-dienstverleners en -experts. Er zijn indicaties dat vooral criminele netwerken uit Oost-Europa en Rusland hackers inhuren die veelal afkomstig zijn uit West-Europa. Hackers hebben in de loop van de jaren ontdekt dat er met hun deskundigheid snel en veel geld te verdienen is. Daardoor zijn hackers ook in de belangstelling gekomen van CSV's en in sommige gevallen behoren ze er (waarschijnlijk) ook toe. Een aanzienlijk deel van de criminelen met belangstelling voor high-tech crime heeft bijvoorbeeld belang bij botnets, en dat geeft de hackers die over deze zombienetwerken kunnen beschikken een bijzondere positie. Hackers zijn daarmee geworden tot belangrijke 'facilitators' voor criminele groeperingen. Zij leveren op bestelling allerlei technische hulpmiddelen zoals backdoors (om toegang tot systemen te krijgen), Trojaanse paarden en bots (om computers extern mee te besturen) en volledige botnets (legers aan zombiecomputers die op afstand bestuurbaar zijn). Met name de multifunctionele toepassingen van *malware* en *botnets* zijn sterk bepalend voor de criminele markt van high-tech crime: zij worden op maat gemaakt en faciliteren diverse criminele activiteiten zoals dDoS-aanvallen, phishing, spamming, internetfraude en verspreiding van kinderporno. Vooral de rekrutering van jonge studenten (die worden benaderd op universiteiten, computerclubs of online forums), corruptie van hoogopgeleid ICT-personeel,[6] en infiltratie van criminelen in ICT-bedrijven of de e-commerce is reden tot bezorgdheid. Door een gebrek aan kennis over daders en de manier waarop criminele groeperingen ICT inzetten bij hun activiteiten doen er zich op dit terrein aanzienlijke problemen voor bij de opsporing en vervolging zodat

5 Doordat vele botnets tegelijkertijd actief kunnen zijn, hoeft de impact ervan namelijk niet minder te worden.
6 Er zijn al enkele jaren discussies gaande over de introductie van een beroepscode voor ICT'ers (Rogers, 2001: 132-133).

de beheersbaarheid van het fenomeen als zorgelijk wordt gekwalificeerd (NDB2004, KLPD, DNRI).

Jongeren als risicogroep
Vooral de jongere generatie en studenten met goed onderlegde ICT-kennis en -vaardigheden en verstand van het internet kunnen als risicogroep voor high-tech crime worden aangemerkt. Dit geldt in het bijzonder voor de mogelijkheid om betrokken te raken bij de georganiseerde misdaad en niet alleen voor criminele maar ook voor terroristische samenwerkingsverbanden (Europol, 2003; McAfee, 2006; Neve, 2007). Uit onderzoek is gebleken dat daders van computercriminaliteit (en sommige aanverwante vormen van cybercriminaliteit) steeds jonger zijn en steeds complexere activiteiten uitvoeren (Europol, 2003: 116). Los van de spanning en de uitdaging levert high-tech crime veel geld op. Hierdoor kunnen jongeren, die aanvankelijk getypeerd kunnen worden als een soort 'jeugdbende', in een criminele spiraal terechtkomen waaruit moeilijk meer te ontsnappen is.

Corruptie binnen bedrijven
Een ander fenomeen dat aandacht verdient zijn de kwetsbaarheden binnen bedrijven die ontstaan wanneer werknemers onzorgvuldig met veiligheidsmaatregelen omgaan of deze juist doelbewust blokkeren of ontregelen. Doordat kernprocessen bij bedrijven en overheden in toenemende mate aangestuurd worden door ICT is men aangewezen op experts die de vaardigheden en technieken beheersen om systemen te ontwikkelen, te beheren en te beveiligen. Vooral personen met een hoog niveau aan ICT-bevoegdheden (programmeurs, systeem- en gegevensbeheerders), met toegang tot gevoelige en vertrouwelijke gegevens (bijvoorbeeld klanten- en betalingsbestanden), en werkzaam bij bedrijven of organisaties die verantwoordelijk zijn voor de vitale infrastructuren en veiligheid (SCADA-systemen, opsporingsdiensten) vormen een risico. Het betreft niet alleen mensen die gevoelig kunnen zijn voor corruptie, maar bijvoorbeeld ook wraakzuchtige (ex-)werknemers (internal hackers en CITI's) die in potentie grote schade kunnen aanrichten. Bedrijven huren ook steeds vaker IT-consultants extern in om systemen of software te bouwen. Wanneer dit mensen zijn met criminele bedoelingen of wanneer criminelen als zelfstandige ondernemers ICT-diensten op de markt aanbieden, kan er sprake van een aanmerkelijk veiligheidsrisico.

Subculturen
Bij een deel van de sociale activiteiten die zich voorheen in 'het fysieke' afspeelden, wordt tegenwoordig gebruikgemaakt van ICT en digitale technologie. Virtuele gemeenschappen die bijvoorbeeld gebruikmaken van discussiefora kunnen in sommige gevallen als subculturen worden aangemerkt (hackers, wetenschappers, jeugdbendes, pedofielen). Er is binnen deze gemeenschappen sprake van een eigen identiteit, eigen normen,

waarden en interesses, en in sommige gevallen ook een eigen 'taal' (het gebruik van afkortingen en tekens). Dit geldt bijvoorbeeld voor jongeren met een radicaal (islamistisch of extreem-rechts) gedachtegoed, maar ook voor jongeren die tot het ondergrondse van de hackergemeenschap zijn gaan behoren. Wat volgens Turgeman-Goldschmidt (2005) aanvankelijk begint als vorm van entertainment kan makkelijk uitmonden en escaleren tot een crimineel verschijnsel. De steeds verdergaande verschuiving naar een digitale samenleving betekent ook dat gedragingen vaker zullen leiden tot uitspattingen en excessen op bijvoorbeeld het internet. Het verdient aandacht om een aantal verschijningsvormen van high-tech crime waar jongeren bij zijn betrokken (radicalisering en extremisme, softwarepiraterij, discriminatie, hacking) te evalueren in relatie tot subculturen en jeugdcriminaliteit. Expliciete aandacht daarbij is vereist op het gebied van sociaal-psychologische factoren en groepsprocessen die zich afspelen via het internet (bijvoorbeeld morele ontwikkeling, gezinsproblematiek, sociale beïnvloeding en subculturele groepsvorming) (zie ook NCTb, 2006b: 10; Yar, 2005b).

1 Inleiding

1.1 De keerzijde van technische vooruitgang

'Het gemak dient de mens'. Deze uitdrukking heeft de afgelopen decennia een steeds hoger realiteitsgehalte gekregen. Door de voortschrijdende Informatie- en Communicatie Technologie (hierna ICT) zijn de mogelijkheden en toepassingen voor het vergaren en verspreiden van informatie en onderlinge communicatie een stuk eenvoudiger geworden. De wereld van elektronische communicatie laat zich daarbij kenmerken door een sterke dynamiek met snelle innovaties en een keur aan nieuwe gebruiksmogelijkheden voor zowel burgers, bedrijven als overheden. Waar het gebruik en de toepassingen van ICT zich aanvankelijk kenmerkte door interne (gesloten) bedrijfsnetwerken en 'stand-alone' computers, is sinds eind jaren negentig in toenemende mate sprake van convergerende technologieën en markten. Steeds meer zien we bijvoorbeeld dat netwerken een open verbinding hebben met het internet[7] en bovendien zijn allerlei maatschappelijke processen steeds meer ingericht op online communicatie en interconnectiviteit. Met zijn laagdrempelige toegang en wereldwijde bereik biedt het internet nagenoeg onbegrensde mogelijkheden tot het aanbieden en afnemen van allerlei diensten en producten (zoals verkoop via het internet of elektronisch bankieren). Ook de economische sector en bankinstellingen zijn dus steeds meer afhankelijk geworden van online zakenverkeer. ICT, en internet in het bijzonder, laat zich typeren als een alomtegenwoordige, vitale infrastructuur voor vrijwel alle maatschappelijke en economische processen (Helmus, Smulders en Van der Zee, 2006; KLPD, DNRI, 2004: 43-44).

De kennelijk onbegrensde mogelijkheden van ICT en het internet, alsook het intensieve gebruik ervan door burgers, bedrijven en organisaties hebben echter een belangrijke schaduwzijde. Ook in de criminele wereld is gaandeweg namelijk het besef ontstaan dat, met de nieuwe communicatiediensten en de toenemende interconnectiviteit, kwetsbaarheden ontstaan zijn die misbruikt kunnen worden voor criminele doeleinden en dat daarmee veel geld te verdienen valt (Helmus e.a., 2006; Molenaar, 2007; NHTCC/NPAC, 2006a: 14). Ten opzichte van de traditionele (fysieke) criminaliteitsvormen hebben de nieuwe (virtuele) varianten bovendien een aantal voordelen: (a) de barrières van tijd en ruimte zijn verdwenen waardoor binnen enkele seconden direct contact mogelijk is met personen overal ter wereld, (b) het bereik ten opzichte van potentiële slachtoffers is groot (tegen minimale investering), (c) men geniet een zekere vorm van anonimiteit (met de mogelijkheid om een andere identiteit aan te nemen) en (d) activiteiten kunnen relatief gemakkelijk en veelvuldig worden herhaald of gelijktijdig plaatsvinden waardoor zelfs kleine opbrengsten per delict tot grote winsten kunnen leiden (Van Amersfoort,

7 Een afkorting voor *inter*connected *net*works: een openbaar netwerk van computernetwerken.

Smit en Rietveld, 2002: 21-23). De geavanceerde ICT-mogelijkheden en toepassingen hebben in de loop der tijd tal van criminele activiteiten dan ook een nieuwe dynamiek gegeven. Behalve het faciliteren van bestaande criminaliteit (zoals diefstal, kinderporno, fraude, oplichting, spionage en terrorisme) zijn er ook geheel nieuwe verschijningsvormen van criminaliteit ontstaan (zoals *hacking*[8] en *phishing*[9]) (zie ook Europol, 2003: 8; Europol, 2007b: 18; Rogers, 2001: 2).

Cybercrime is een veelgehoorde en -gebruikte term die doorgaans verwijst naar de traditionele vormen van criminaliteit waarbij gebruik wordt gemaakt van computers en ICT (en in het bijzonder het internet). Het begrip heeft aan betekenis enigszins ingeboet doordat een deel van de problematiek op het gebied van ICT en criminaliteit, namelijk nieuwe vormen van criminaliteit waarbij ICT expliciet als doelwit kan worden aangemerkt, buiten de boot valt. Tot op de dag van vandaag bestaat er verwarring over de exacte betekenis van het begrip cybercrime. Het begrip wordt internationaal dan ook regelmatig vervangen door de meer overkoepelende term high-tech crime om te benadrukken dat het zowel gaat om traditionele criminaliteit waarbij ICT een belangrijke rol speelt (cybercrime) als om criminaliteit die exclusief in virtuele omgevingen plaatsvindt (dat bekend staat als computercriminaliteit) (Europol, 2003: 9; G8, 2004; PCA, 2004: 3). Dit neemt overigens niet weg dat de begrippen cybercrime en high-tech crime in de praktijk nog steeds door elkaar worden gebruikt en dat een standaard hiervoor ontbreekt. Op grond van (inter)nationale literatuurstudie en in navolging van vooraanstaande autoriteiten en internationale ontwikkelingen op het gebied van onderzoek en bestrijding van ICT-gerelateerde criminaliteit,[10] gebruiken we in dit rapport het *containerbegrip 'high-tech crime'*. Het gaat dan zowel om ICT die als middel wordt ingezet om (traditionele) criminaliteit mee te faciliteren, als om ICT die behalve als middel ook als expliciet doelwit van criminele activiteiten kan worden aangemerkt (zie hoofdstuk 2). In navolging van de 'terms of reference' van de strategische cybercrime intelligence groep (Europol, 2003: 130-131) en de 'mededeling ter bestrijding van cybercriminaliteit' die onlangs werd uitgebracht door de Europese

8 *Hacking* staat voor het ongeautoriseerd toegang verschaffen tot een computer, netwerk of systeem. Het hacken van telefoonsystemen wordt ook wel 'phreaken' genoemd (Mooij en Van der Werf, 2002: 9). Wanneer hacking expliciet wordt gepleegd voor criminele doeleinden, is er sprake van '*cracking*' (*cr*iminele h*acking*).

9 *Phishing* is een verzamelnaam voor 'spam e-mail' (het versturen van massale e-mailberichten) die afkomstig lijkt van een gerenommeerde bron maar waarmee persoonlijke informatie van mensen wordt ontfutseld (zoals sofi-nummers, geboortedata, bankgegevens) om hen op te lichten. De e-mail kan tekst bevatten waarin expliciet wordt gevraagd naar bijvoorbeeld bankgegevens, maar kan ook verwijzen naar een nagemaakte website van een bankinstelling met de vraag hier bankgegevens bij te werken en te actualiseren.

10 Zoals Australië (Australian High Tech Crime Centre, AHTCC), de Verenigde Staten (International High Technology Crime Investigation Association, HTCIA) en het Verenigd Koninkrijk (National Hi Tech Crime Unit, NHTCU, dat in 2006 is opgegaan als e-crime-unit binnen het Serious Organised Crime Agency), Europol (15 juni 2006) en Interpol (2007). Zie ook Krone (2005).

Commissie (22 mei 2007a) opteren we voor de volgende werkdefinitie van high-tech crime:[11]

High-tech crime is het gebruik van ICT voor het plegen van criminele activiteiten tegen personen, eigendommen, organisaties of elektronische communicatienetwerken en informatiesystemen.

1.2 Aanleiding en probleemstelling van het onderzoek

High-tech crime vormt in toenemende mate een financieel en maatschappelijk probleem in een samenleving die steeds meer is aangewezen op ICT. Hoewel de exacte omvang ervan moeilijk te bepalen is[12] (Europese Commissie, 22 mei 2007b: 6) wordt alleen al de financiële schade geschat in de miljarden euro's.[13] Vaststaat dat zowel het aantal slachtoffers als het aantal daders van high-tech crime de laatste jaren explosief is gestegen (Europol, 2003: 8, 59). Er is sprake van een toenemende professionalisering en er zijn aanwijzingen dat ook de georganiseerde criminaliteit in toenemende mate betrokken is (Europese Commissie, 22 mei 2007: 3). De laatste jaren zijn er dan ook verschillende (inter)nationale initiatieven tot stand gekomen in de aanpak en bestrijding van high-tech crime. Een belangrijke bijdrage hierin vormde het Cybercrimeverdrag die op initiatief van de Raad van Europa in november 2001 werd aangenomen en in werking trad in 2004. Het verdrag heeft tot doel de opsporing en wetgeving met betrekking tot high-tech crime zowel binnen als buiten Europa te harmoniseren (Govcert, 2006: 138). In Nederland zijn de bepalingen uit het verdrag in de Wet op de Computercriminaliteit II geïmplementeerd dat op 13 juli 2006 in werking is getreden (EK, 2007). De afgelopen jaren is in de bestrijding van high-tech crime ook het beleid geïntensiveerd. Dit heeft bijvoorbeeld geleid tot de komst van een Meldpunt Cybercrime, een

11 Wij benadrukken dat het begrip high-tech crime in dit rapport wordt gehanteerd op grond van de bevindingen uit de literatuur en ter bevordering van de consistentie en transparantie in het veld. Het gebruik van het begrip high-tech crime ten faveure van het begrip cybercrime is een keuze van de onderzoekers voor zover het dit rapport betreft (zie ook bijlage 4). Deze begripsdefinitie zal voor sommigen afwijken van de gewoonten en kan weerstand oproepen, temeer gewoonten zich niet makkelijk laten veranderen (zie ook Helmus e.a., 2006).

12 Dit heeft onder meer te maken met een gebrek aan aangiftebereidheid en problemen in de registratie (Van der Werf, 2003).

13 In de literatuur worden verschillende schattingen gegeven. De schade bij Nederlandse bedrijven als gevolg van *hacking* incidenten wordt geschat tussen de 185 miljoen en 1 miljard euro (NHTCC, 2006b: 20). De schade als gevolg van *identiteitsfraude* in de Verenigde Staten (VS) wordt (omgerekend) geschat op 38 miljard euro en in Australië op ruim 2 miljard euro (Computable, 2007). Als gevolg van *piraterij* is de schade voor de Amerikaanse filmindustrie ruim 15 miljard euro (Nu.nl, 2006), en over de gehele software-industrie wereldwijd 26 biljoen euro per jaar (Lau, 2006). De schade als gevolg van *dDoS-aanvallen* wereldwijd wordt geschat op minstens 1 miljard euro (Boerman en Mooij, 2006) en die van *internetfraude* in 2007 door de georganiseerde misdaad in het Verenigd Koninkrijk (VK) op bijna 3 biljoen (E-crime congress, 2007). In zijn totaliteit wordt de jaarlijkse schadeomvang van high-tech crime in de VS (omgerekend in euro's) geschat tussen de 7,5 en 290 biljoen (McAfee in Choo, 2007: 2; Taylor e.a., 2006: 4) en in het VK rond de 15 biljoen (Choo, 2007: 2).

High Tech Crime Team bij de Nederlandse politie, en een samenwerkingsverband tussen publieke en private partijen (zie voor een nadere toelichting ook bijlage 3).
Het Coalitieakkoord 2007 en het Beleidsprogramma 2007 benadrukken de noodzaak om de preventie en de bestrijding van high-tech crime verder te versterken. Daarvoor is allereerst nodig om de transparantie en de kennisontwikkeling over high-tech crime te verbeteren. Tot op heden is er nog te weinig bekend over de aard en omvang van high-tech crime en over de effectiviteit van opsporing en bestrijding. In het Nationaal Dreigingsbeeld (NDB) uit 2004 (hierna NDB2004) (KLPD, DNRI: 47), waarin ernstige criminele dreigingen voor de Nederlandse samenleving in kaart worden gebracht, werd onder meer geconstateerd dat er onvoldoende kennis bestaat over de daders van high-tech crime en over de betrokkenheid van de georganiseerde misdaad daarbij. Voor een gerichte probleemaanpak van high-tech crime is het dan ook van belang om hierover meer kennis en inzichten te vergaren. De Directie Rechtshandhaving en Criminaliteitsbestrijding (DRC) van het Ministerie van Justitie (MvJ) heeft het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) gevraagd om een verkennend en inventariserend literatuuronderzoek uit te voeren om de hiaten in de kennis over de daders van high-tech crime (waaronder de georganiseerde misdaad) zoveel mogelijk in te vullen. De uitkomsten van dat onderzoek zijn neergelegd in deze rapportage, die tevens dient als input voor de nadere onderzoeksprogrammering op het gebied van high-tech crime. Hiermee wordt beoogd de basis te leggen voor meer toegespitst onderzoek op dit terrein, waarmee meer toegesneden beleidsmaatregelen op het gebied van preventie, opsporing en handhaving van high-tech crime.[14] De probleemstelling van dit onderzoek luidt als volgt:[15]

Wat is er in de (inter)nationale literatuur bekend over daders van high-tech crime, en wat zijn naar verwachting de belangrijkste ontwikkelingen op dit gebied voor de eerstkomende jaren?

Meer specifiek staan de volgende zes onderzoeksvragen in dit onderzoek centraal:
- Wat verstaan we onder het begrip high-tech crime?
- Welke verschijningsvormen van high-tech crime kunnen worden onderscheiden?
- Hoe zijn de daders (of dadergroepen) van high-tech crime te karakteriseren?

14 Expliciet wordt gedacht aan het ontwikkelen van risicoprofielen van (potentiële) daders.
15 De omvang van high-tech crime en de maatschappelijke en financiële risico's vallen buiten de doelstelling van dit onderzoek. Voor zover hierover informatie voorhanden was in de literatuur wordt hiernaar ter zijde verwezen.

– In hoeverre is de georganiseerde misdaad betrokken bij high-tech crime?
– Wat zijn de lacunes in de literatuur in kennis over daders van high-tech crime?
– Welke ontwikkelingen op het gebied van high-tech crime zijn de eerstkomende jaren te verwachten?

1.3 Onderzoeksopzet

Na een korte verkenning op het thema zijn er in de startfase van het onderzoeksproject zeven interviews afgenomen met Nederlandse deskundigen[16] op het gebied van high-tech crime. Doel van deze gesprekken was om inzicht te krijgen in de problematiek zoals die in Nederland speelt. Naast de interviews is er een uitgebreid literatuuronderzoek verricht in diverse databases[17] zoals de National Criminal Justice Reference Service (NCJRS), de mediatheek van de Rechercheschool van de Politieacademie, Web of Science, Picarta en diverse open bronnen zoals beschikbaar via het internet. In aanvulling op de interviews en het raadplegen van databases zijn ook wetenschappelijke publicaties en praktijkgerichte onderzoeksrapportages geraadpleegd van onder meer het KLPD (DNRI), de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Nationaal Coördinator Terrorismebestrijding (NCTb) en de European Police Office (Europol). Behalve wetenschappelijke bijdragen en (beleids)notities en publicaties zijn in dit rapport ook diverse mediaverslagen in dit rapport verwerkt. In hoofdzaak zijn echter de wetenschappelijke publicaties en praktijkgerichte onderzoeksrapportages als bronmateriaal gebruikt (voor een overzicht verwijzen we naar de literatuurlijst).

1.4 Opbouw van dit rapport

De interviews en het literatuuronderzoek zijn gebruikt ter begripsbepaling van high-tech crime en voor het categoriseren van de verschillende verschijningsvormen ervan. De in het verantwoordingsrapport van het National High Tech Crime Center (NHTCC, 2006b) gepresenteerde

16 Experts van het Landelijk Parket (LP), het KLPD, de Koninklijke PTT Nederland (KPN), het Nederlands Forensisch Instituut (NFI), de Politieacademie (PA), het Nederlands Politie Instituut (NPI), en het Openbaar Ministerie (OM). Voor een belangrijk deel betreft het personen die door DRC werden geadviseerd waarvan sommige kandidaten weer naar elkaar hebben doorverwezen.

17 Er is gezocht met zowel Nederlandse als Engelse trefwoorden op het terrein van *high-tech crime* (met de bijbehorende synoniemen zoals cybercrime, computercriminaliteit, digitale criminaliteit, internet crime, netcrime, computer crime, en dergelijke) en *daders van high-tech crime* (met de bijbehorende synoniemen zoals daderkenmerken, offender profiles, behavioral typologies, profielanalyses, en dergelijke). Ook zijn zoektermen gecombineerd met concrete bewoordingen van afzonderlijke verschijningsvormen van high-tech crime (bijvoorbeeld hacking, kinderporno, *cyberterrorisme*, en dergelijke).

indeling heeft daarbij deels als uitgangspunt gediend en is op punten geactualiseerd. Binnen de overkoepelende werkdefinitie van high-tech crime zijn twee belangrijke subthema's onderscheiden (*cybercriminaliteit* en *computercriminaliteit*) waarvan de verschillende verschijningsvormen in het rapport worden afgebakend en toegelicht (hoofdstuk 2). Aan de hand van de maatschappelijke en economische dreiging en risico's zijn een aantal verschijningsvormen van high-tech crime onderscheiden waarvoor geldt dat kennis over daderkenmerken prioriteit op de onderzoeksagenda verdient. Voor zover daarover in de geraadpleegde bronnen en literatuur informatie beschikbaar was, is voor die geprioriteerde thema's een inventarisatie van daderkenmerken gemaakt (hoofdstuk 3[18]). Ook wordt expliciet aandacht besteed aan criminele (en terroristische) samenwerkingsverbanden (CSV's) en de eventuele overlap van high-tech crime met andere criminele activiteiten (hoofdstuk 4). In hoofdstuk 5 worden ten slotte de conclusies en aandachtspunten uit het rapport samengevat en volgt een aanzet tot discussie met richtlijnen voor toekomstig onderzoek op het gebied van high-tech crime.

18 Een inventarisatie van daderkenmerken van niet-geprioriteerde thema's is opgenomen in bijlage 7.

2 High-tech crime nader beschouwd

2.1 Een nieuwe en afzonderlijke categorie criminaliteit?

Uit de literatuur blijkt veelvuldig dat het niet eenvoudig is om het fenomeen high-tech crime eenduidig te definiëren en er een handzame indeling naar verschijningsvormen voor te maken (Drucker en Gumpert, 2000; Europese Commissie, 2007; Furnell, 2001; Gordon en Ford, 2006; Grabosky, 2004; McCusker, 2006; Mooij en Van der Werf, 2002; Speer, 2000; Van Amersfoort e.a., 2002; Yar, 2005). Een gemeenschappelijke definitie en consistent begrippenkader voor dit criminaliteitsterrein ontbreekt. Een heel arsenaal aan terminologie wordt gebruikt, al dan niet in combinatie met de voorvoegsels cyber, computer, e-, internet, digital of information (Parliament of the Commonwealth of Australia: PCA, 2004; Weimann, 2005). Begrippen worden te pas en te onpas overgenomen, willekeurig toegepast, vertonen inhoudelijke overlap of juist belangrijke lacunes (Furnell, 2001). Dit zorgt voor verwarring, onduidelijkheid en uiteenlopende gebruiken en interpretaties, zowel bij onderzoekers en beleidsmakers op dit terrein als bij mensen in de opsporing, bestrijding en vervolging. Vanzelfsprekend komt dit de aanpak van criminaliteit en de kennisuitwisseling en (inter)nationale samenwerking op dit terrein niet ten goede. Harmonisatie in het gebruik van definities, terminologie en wetgeving is dan ook geen overbodige luxe[19] (Furnell, 2001; Gordon en Ford, 2006). In Nederland worden de begrippen cybercrime (of cybercriminaliteit) en high-tech crime als equivalenten van elkaar gebruikt.[20] De term high-tech crime biedt echter een breder en meer dynamisch perspectief dat beter aansluit bij de snelle technologische ontwikkelingen (zie hoofdstuk 1). In dit rapport hanteren wij dan ook high-tech crime als overkoepelend begrip waarmee wij verwijzen naar het gebruik van ICT voor het plegen van criminele activiteiten tegen personen, eigendommen, organisaties of elektronische communicatienetwerken en informatiesystemen.

Een belangrijke vraag die opdoemt is of, en in hoeverre, high-tech crime een eigen criminaliteitsterrein bestrijkt. Er is feitelijk sprake van een grote verwevenheid van traditionele vormen van criminaliteit met wat wij

19 In de recent gepubliceerde nota van de Europese Commissie (22 mei 2007a) ter bestrijding van computercriminaliteit werd uit praktische overwegingen gekozen voor de term 'cybercrime'. Volgens de Commissie (22 mei 2007a: 8) is er weliswaar sprake van uiteenlopende begrippen en definities maar zou het nog te vroeg zijn om een consistent begrippenkader te definiëren (als reden hiervoor noemt men de grote verscheidenheid aan verschijningsvormen van high-tech crime). Onzes inziens is dit reden te meer om tot een overzichtelijk en eenduidig begrippenkader en indeling te komen, zeker gezien de noodzaak tot samenwerking in de bestrijding van high-tech crime en verdeling van taakverantwoordelijkheden tussen de betrokken (inter)nationale instanties.

20 Denk bijvoorbeeld aan het National *High Tech Crime* Center (NHTCC) maar ook aan de Nationale Infrastructuur ter bestrijding van *Cyber Crime* (NICC). In het adviesontwerp van de Nationale Infrastructuur Bestrijding Cybercrime (NHTCC/NPAC, 2006: 5) hanteert men de term cybercrime als allesomvattend verschijnsel waarbinnen ook computercriminaliteit valt. Het Team High Tech Crime van het KLPD (actief sinds 1 februari 2007) gebruikt de term cybercriminaliteit als overkoepelend begrip en 'high-tech crime' om te verwijzen naar opsporingszaken met een vitaal belang (nationale veiligheid en economie) en/of waarbij de georganiseerde misdaad is betrokken.

tegenwoordig high-tech crime noemen. Evenals velerlei legale activiteiten worden klassieke misdrijven (denk bijvoorbeeld aan fraude of diefstal) tegenwoordig veelal met behulp van moderne ICT[21] uitgevoerd. Dit maakt het begrip high-tech crime diffuus, zeker waar het de opsporing en registratie van daders betreft.[22] Wordt bijvoorbeeld een professionele oplichter die zijn werkwijze heeft verlegd van de straat naar het internet nu per definitie een 'high-tech crimineel'? Tot op heden bestaat hierover weinig consensus.

Criminelen die zich bezighouden met traditionele criminaliteit (zoals fraude) kunnen echter niet per definitie over één kam worden geschoren met criminelen die zich bezighouden met nieuwe vormen van criminaliteit (zoals het hacken van computersystemen). De verschillende verschijningsvormen van high-tech crime kennen in essentie immers evenzoveel verschillende soorten daders en werkwijzen. Voor de opspoorbaarheid van high-tech criminelen is een nadere differentiatie tussen daders van groot belang (waarmee wij overigens niet uitsluiten dat verwante of zelfs identieke daders betrokken zijn bij verschillende verschijningsvormen van high-tech crime). Alvorens kennis over daders in kaart te kunnen brengen (hoofdstuk 3) is het allereerst een vereiste om het scala aan verschijningsvormen van high-tech crime zo duidelijk mogelijk te definiëren en af te bakenen. Vanuit het perspectief van de rol van ICT voor het plegen van een misdrijf kunnen twee ideaaltypen van high-tech crime worden onderscheiden waartussen zich een zeker continuüm bevindt[23] (Casey, 2002: 566; zie ook Furnell, 2001; Gordon en Ford, 2006; Van Amersfoort e.a., 2002: 18). In dit rapport onderscheiden wij *cybercriminaliteit* en *computercriminaliteit* als subthema's van high-tech crime.

2.1.1 Cybercriminaliteit

Bij cybercriminaliteit[24] gaat het om traditionele criminaliteitsvormen die ook zonder tussenkomst van ICT gepleegd kunnen worden maar door het gebruik van ICT een nieuwe uitvoering hebben gekregen (Gordon en Ford,

21 Men maakt bijvoorbeeld gebruik van de computer, het internet, e-mail, de mobiele telefoon of de Personal Digital Assistant (PDA). De PDA is een klein draagbaar toestel dat computer-, telefonie-, fax- en netwerkfuncties combineert.

22 Dit komt onder meer tot uiting in de politieregistraties: moet een inbraak in een computersysteem waarbij privacygevoelige gegevens worden gestolen nu simpelweg worden beschouwd als een nieuwe vorm van 'inbraak en diefstal', of moeten we dit soort daden – gezien de rol van ICT in de uitvoering van het delict – toch beschouwen als high-tech crime?

23 Sommigen onderscheiden (daarnaast nog) andere vormen van high-tech crime (bijvoorbeeld Europese Commissie, 22 mei 2007: 2; Govcert, 2006: 10; Taylor e.a., 2006: 9-15). Wij zijn van mening dat de gehanteerde tweedeling in dit rapport echter volstaat voor het categoriseren van high-tech crime omdat andere categorieën inhoudelijk weinig toevoegen aan de gebruikte tweedeling. Zo evalueren wij bijvoorbeeld 'elektronische publicaties met illegale inhoud' (zoals kinderporno en rassenhaat via het internet) (EC, 2007) als traditionele delicten waarbij ICT als instrument wordt gebruikt (cybercriminaliteit).

24 Ook bekend als criminaliteit van het 'type II', 'computer-assisted crimes', oude criminaliteit, of computercriminaliteit in brede zin (Furnell, 2001; NHTCC/NPAC, 2006a: 5; Van Amersfoort e.a., 2003: 20).

2006; NHTCC, 2006b: 11). Feitelijk is er sprake van veelal klassieke criminaliteit waarbij nu digitale hulpmiddelen worden ingezet (Broadhurst, 2005). Voorbeelden zijn fraude en oplichting via het internet (zoals de *Nigeriaanse 419 scams*[25]), het illegaal en digitaal verspreiden van auteursrechtelijk beschermd muziek- en filmmateriaal (*softwarepiraterij*[26]), stalking via het internet (*cyberstalking*[27]), en het verspreiden van illegale inhoud op het internet (zoals kinderporno, *discriminatie*). We hanteren in dit rapport de volgende werkdefinitie:

Cybercriminaliteit omvat alle (traditionele) criminele activiteiten waarbij ICT als instrument wordt gebruikt zonder dat ICT expliciet doelwit is van de criminele activiteiten.

2.1.2 Computercriminaliteit

Bij computercriminaliteit[28] gaat het om nieuwe vormen van criminaliteit met een sterk technisch, virtueel karakter die zijn ontstaan door en niet kunnen bestaan zonder ICT (Broadhurst, 2005; Gordon en Ford, 2006). Behalve dat ICT wordt gebruikt als instrument zijn de digitale instrumenten, computersystemen en/of datagegevens dus ook expliciet doelwit van de activiteiten (NHTCC, 2006b: 6). Voorbeelden zijn aanvallen op ICT-infrastructuren door het verstoren van de werking van een computersysteem (het verspreiden van *spam*[29]), het vernielen of wijzigen van elektronische gegevens op een geautomatiseerd netwerk (via *malware*[30] of door *defacing*[31] van websites), het veroorzaken van een elektronische verkeersopstopping door het versturen van massale gegevens of verzoeken naar een website waarmee de toegang of gebruik van het systeem wordt belemmerd (distributed Denial of Service oftewel *dDoS-aanvallen*[32]), het

25 Bij de Nigeriaanse 'advance fee fraud' ofwel voorschotfraude (ook wel '419 fraude' genoemd naar het artikel uit het Nigeriaanse strafrecht) gaat het om grootschalige oplichtingspraktijken die veelal door Nigerianen worden gepleegd. Internetgebruikers worden met behulp van misleidende digitale informatie (vaak spam e-mail) overgehaald om een financieel voorschot te verlenen (zie hoofdstuk 2).

26 Softwarepiraterij is een vorm van cybercriminaliteit (zie NHTCC, 2006b: 13 en Post, 2006) en staat voor het illegaal en digitaal verspreiden van auteursrechtelijk beschermd materiaal zoals muziek en films.

27 Cyberstalking is de verzamelnaam voor het stelselmatig en op dwangmatige wijze online lastigvallen (en soms zelfs bedreigen) van een persoon door provocerende uitspraken te doen en/of berichten te plaatsen via online forums, bulletin boards en chatrooms, de ander via spyware te bespioneren, of door het voortdurend ongevraagd verzenden van e-mail en spam.

28 Ook bekend als criminaliteit van het 'type I', 'computer-focused crimes', nieuwe criminaliteit of computercriminaliteit in enge zin (Furnell, 2001; NHTCC/NPAC, 2006a: 5; Van Amersfoort e.a., 2003: 20).

29 Spam is het veelal massaal verzenden van ongewenste e-mail van commerciële, ideële of charitieve aard die verstuurd wordt zonder voorafgaande toestemming van de ontvanger (Govcert, 2006: 25).

30 Malware is een afkorting van 'malicious software' waarmee andermans computer zonder toestemming kan worden beschadigd (bijvoorbeeld virussen, wormen, Trojaanse paarden en/of spyware).

31 Bij defacing worden websites door hackers gewijzigd, beschadigd of vervangen.

32 Een distributed Denial of Service (dDoS)-aanval is een verstikkingsaanval gericht op een computer of netwerk waarbij met een leger aan besmette zombiecomputers (waarvan de besturing is overgenomen) wereldwijd vanaf meerdere plaatsen tegelijk zoveel verbindingsverzoeken naar de server van een website worden verstuurd dat de service door overbelasting tijdelijk niet beschikbaar is of de server zelfs crasht (Wikipedia, laatst geraadpleegd op 19 juli 2007).

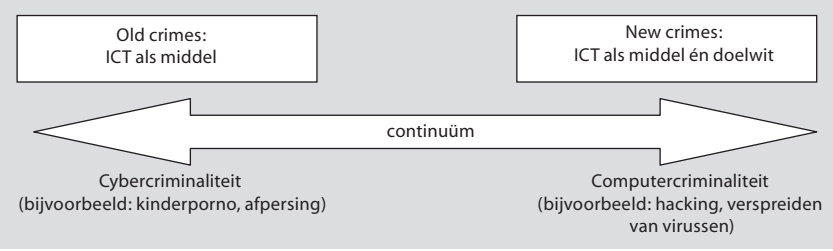
ongeautoriseerd inbreken in een computernetwerk (hacking) en het aftappen (sniffen) of opnemen van actieve en passieve gegevens in datacommunicatie (NHTCC, 2006b: 13). We hanteren in dit rapport de volgende werkdefinitie:

Computercriminaliteit omvat alle criminele activiteiten waarbij ICT als instrument wordt gebruikt én waarbij ICT expliciet doelwit is van de criminele activiteiten.

2.1.3 Ideaaltypen

Volgens de gehanteerde definities in dit rapport ligt het niet voor de hand om cybercriminaliteit als zelfstandig criminaliteitsterrein te bestempelen. Het betreft hier immers klassieke criminaliteitsvormen (zoals drugshandel, afpersing of fraude) waarvan de modus operandi door de jaren heen 'slechts' met ICT verweven is geraakt (Europol, 2003: 27; NHTCC/NPAC, 2006a: 10). Met betrekking tot computercriminaliteit moeten we vaststellen dat het hier wel een nieuw (en mogelijk zelfstandig) criminaliteitsterrein betreft.[33] Het gaat hierbij immers om handelingen die voorheen niet met andere middelen mogelijk waren en (deels) om eveneens nieuwe criminele doelen. Van belang is in ieder geval dat beide vormen als ideaaltypen worden beschouwd: als uiteinden van een continuüm, zoals weergegeven in schema 1, waarbinnen verschillende combinaties mogelijk zijn. Diverse verschijningsvormen van cyber- en computercriminaliteit lopen dus in elkaar over en worden veelal juist in combinatie toegepast (zie ook Europol, 2003: 9; Gordon en Ford, 2006: 16; Grabosky, 2000). Zo wordt de inzet van een dDoS-aanval (computercriminaliteit) gecombineerd met het afpersen van bedrijven (cybercriminaliteit) en worden vertrouwelijke gegevens voor het plegen van fraude (cybercriminaliteit) niet zelden verkregen door middel van hacking (computercriminaliteit). In het navolgende worden de diverse verschijningsvormen van cyber- en computercriminaliteit aan de hand van een clustering van thema's nader beschreven.

Schema 1 Cybercriminaliteit en computercriminaliteit als ideaaltypen van high-tech crime



33 Dit komt mede tot uiting in de bijzondere wetgeving op dit gebied (Wet op de Computercriminaliteit II).

2.2 Clustering van high-tech crime naar subthema's

Over de jaren heen blijkt het scala aan misdrijven dat tot high-tech crime wordt gerekend flink te zijn toegenomen en er komen steeds nieuwe vormen bij (Furnell, 2001). Een algemene indeling naar verschijningsvormen waarover (inter)nationaal consensus bestaat is er helaas nog niet. Om inzicht te geven in daderkenmerken van high-tech crime is een algemene indeling naar verschijningsvormen echter onontbeerlijk. Op grond van de (in de literatuur) meest voorkomende beschrijvingen van cyber- en computercriminaliteit worden deze verschijningsvormen in dit rapport geclusterd naar thema (zie ook Mooij en Van der Werf, 2002: 9; NHTCC/NPAC, 2006a; NHTCC, 2006b: 13). Hoewel het in detail beschrijven van alle mogelijke vormen van high-tech crime buiten het bestek ligt van dit rapport, is gekozen voor een zo breed mogelijke inventarisatie (zonder te streven naar volledigheid). Voor cybercriminaliteit (paragraaf 2.3) en voor computercriminaliteit (paragraaf 2.4) definiëren we vier thematische clusters.

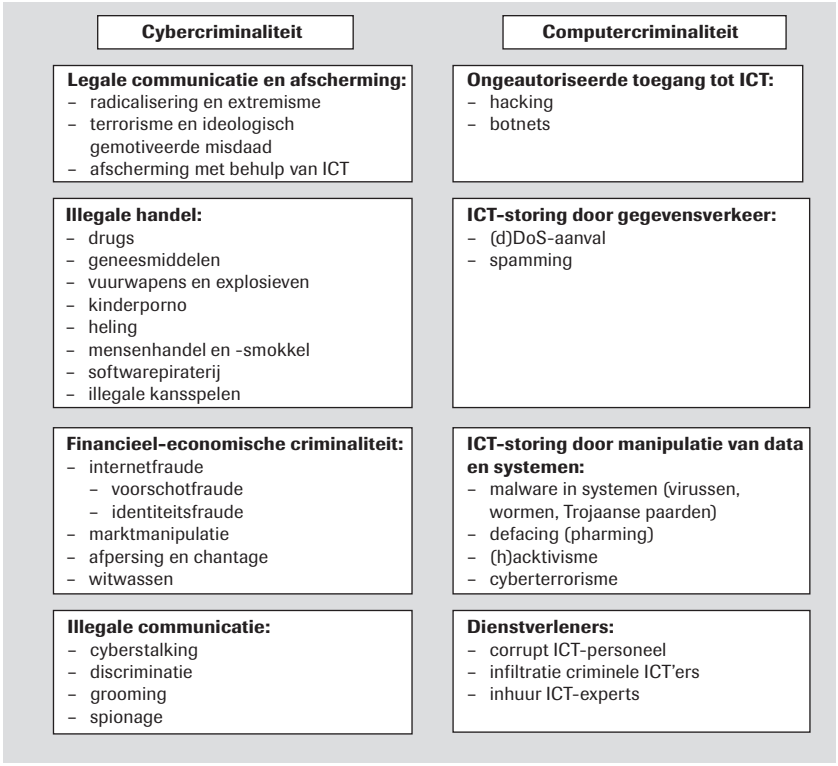
Cybercriminaliteit:
- legale communicatie en afscherming;
- illegale handel;
- financieel-economische criminaliteit;
- illegale communicatie.

Computercriminaliteit:
- ongeautoriseerde toegang tot ICT;
- ICT-storing door gegevensverkeer;
- ICT-storing door manipulatie van data en systemen;
- dienstverleners.

Per cluster worden verschillende verschijningsvormen onderscheiden die in schema 2 naar thema overzichtelijk staan gepresenteerd.[34] In de navolgende paragrafen (2.3 en 2.4) worden de verschijningsvormen afzonderlijk toegelicht. De gehanteerde indeling uit schema 2 dient nadrukkelijk voor het creëren van overzicht: een ruw, strategisch kader dat als kapstok *kan* dienen voor de verdere doorontwikkeling van een zogenoemde 'typologie van high-tech crime'.

34 Aan de hand van alternatieve criteria zijn andere indelingen mogelijk (zie bijvoorbeeld Drucker en Gumpert, 2000; Europol, 2003; Govcert, 2006: 139-142; NDB2004; NHTCC, 2006b: B25-B29; Raad van Europa, 2001; Speer, 2000; Van Amersfoort e.a., 2002; Wall, 2001; Yar, 2005). Voor dit rapport doet dat echter niet ter zake. Het gaat in beginsel om een overzicht van verschijningsvormen zodat daderkenmerken kunnen worden geïnventariseerd. Ook kan met een dergelijk overzicht beter sturing worden gegeven aan beleid(sonderzoek) en maatregelen op het gebied van high-tech crime.

Schema 2 Thematische clustering van high-tech crime naar subthema's



2.3 Cybercriminaliteit: ICT als instrument

Cybercriminaliteit betreft alle criminaliteitsvormen waarbij ICT wordt ingezet als instrument. Dit kan zijn het gebruik van ICT ten behoeve van communicatie en logistiek (tussen daders of tussen dader en slachtoffer), maar ook transacties van gelden en goederen (vrijwillige transacties tussen daders of onvrijwillige transacties tussen dader en slachtoffer) (zie ook Kortekaas, 2005). We hanteren de volgende clustering van thema's die in de navolgende secties nader uiteen worden gezet naar verschillende verschijningsvormen (zie ook schema 2):

– legale communicatie en afscherming (paragraaf 2.3.1)
– illegale handel (paragraaf 2.3.2)
– financieel-economische criminaliteit (paragraaf 2.3.3)
– illegale communicatie (paragraaf 2.3.4)

2.3.1 Legale communicatie en afscherming

Het internet biedt een bijna onuitputtelijke bron van informatie waarop kennis en ideeën van uiteenlopende aard kunnen worden uitgewisseld. Het is als het ware '*…een virtuele bibliotheek met een vrijwel oneindige hoeveelheid informatie die merendeels openlijk toegankelijk is*' (NCTb, 2006b: 76). Naast de belangrijke kennisfunctie heeft het internet ook een brede sociale communicatieve functie gekregen in onze samenleving. Mensen komen er online met elkaar in contact (of men elkaar nu kent of niet), wisselen er al dan niet gericht kennis uit en organiseren uiteenlopende activiteiten die in de 'fysieke wereld' worden voortgezet. Vooral *chatrooms*[35] zijn voor sommige groepen een probaat middel om gelijkgestemde anderen met verwante interesses te ontmoeten. Dergelijke 'virtuele bijeenkomsten' kunnen variëren van wetenschappelijke discussiefora tot radicaliserende jongerengroepen en criminele organisaties. De virtuele gemeenschappen die ontstaan kunnen ook als subculturen worden aangemerkt met eigen normen, waarden en gebruiken (Europol, 2003: 16).

Tot zover valt er in principe niets op af te dingen wanneer ICT wordt gebruikt voor het delen van informatie, het ondersteunen van communicatie (bijvoorbeeld propaganda) en/of het ontwikkelen van sociale contacten en groepsvorming (de virtuele gemeenschappen). Wanneer de activiteiten echter gericht zijn op illegale en criminele doelstellingen (zoals het rekruteren van radicaliserende jongeren of het beramen van een terroristische aanslag), wordt de reguliere ICT-functie van het internet aangemerkt als uitingsvorm van cybercriminaliteit (zie ook Molenaar, 2007). Kenmerkend aan deze activiteiten (legale communicatie en afscherming ten behoeve van illegale doeleinden) is dat zij meestal betrekking hebben op communicatie *tussen daders* (doorgaans ter logistieke ondersteuning van het criminele proces). We onderscheiden in dit rapport de volgende drie subthema's (zie ook schema 2):
– radicalisering en extremisme;
– terrorisme en ideologisch gemotiveerde misdaad;
– afscherming met behulp van ICT.

Radicalisering en extremisme
Radicalisme wordt door de AIVD (2004b: 15) omschreven als: '*…Het (actief) nastreven en/of ondersteunen van diep ingrijpende veranderingen in de samenleving, die een gevaar kunnen opleveren voor (het voortbestaan van) de democratische rechtsorde [doel], eventueel met het hanteren van ondemocratische methodes [middel], die afbreuk kunnen doen aan het functioneren van de democratische rechtsorde [effect]*'. Radicalisering is het proces dat hieraan ten grondslag ligt en zich kenmerkt door het uitdragen

35 Een chatroom is een virtuele ruimte op het internet waar mensen met elkaar communiceren.

van allesoverheersende gedachten en gedragingen die door een ideaal, geloof, doel of belang worden gestuurd (TK 2004-2005, 29 754, nr. 26: 5). Deze interpretaties veranderen vaak zeer plotseling en mensen ontwikkelen gaandeweg een (nieuw) zelfbeeld of identiteit. Onder invloed van de omgeving worden individuen aangezet zich te ontwikkelen in een gewelddadige richting waarbij men in toenemende mate (eventueel op ondemocratische wijze) ingrijpende veranderingen in de samenleving nastreeft (AIVD, 2004b; NCTb, 2007b). Van extremisme is sprake wanneer radicalisering overgaat in daadwerkelijke mobilisering van geweld (tegen bepaalde bevolkingsgroepen of tegen de overheid als geheel) (AIVD, 2004b: 16 en 2006a: 12).

De rol van het internet bij radicaliseringsprocessen is niet te onderschatten: behalve als ideologische inspiratiebron is het een belangrijke operationele kennisbron en een katalysator tot virtuele netwerkvorming. Het is in principe voor iedereen mogelijk om praktisch ongecensureerd en betrekkelijk anoniem allerlei radicale en extremistische boodschappen te verkondigen op en via het internet. Ook zijn op het internet diverse handboeken en trainingsmaterialen verkrijgbaar over professionele strijdmethoden en geweldsmiddelen (bijvoorbeeld het vervaardigen van explosieven maar ook richtlijnen voor het onopvallend voorbereiden van aanslagen in het buitenland) (AIVD, 2006a: 50-51). Volgens Al Qaeda zou in de voorbereiding van een terroristische aanslag 80% van de benodigde informatie over de vijand openlijk beschikbaar zijn via het internet[36] (NCTb, 2006: 62). Daarnaast is het betrekkelijk eenvoudig om in contact te komen met gelijkgestemden waardoor een virtuele gemeenschap kan ontstaan en allerlei vormen van logistieke ondersteuning bij de voorbereiding van aanslagen kunnen worden gemobiliseerd (AIVD, 2006a: 43, 49). De AIVD (2006b: 16) spreekt dan ook van een proces van 'virtualisering' waarmee men expliciet verwijst naar '…*De toenemende rol van het internet bij de verspreiding van extremistisch gedachtegoed en bij de netwerkvorming en onderlinge communicatie*'.

In Nederland kunnen drie vormen van radicalisme worden onderscheiden die een concrete bedreiging vormen voor de Nederlandse samenleving (AIVD, 2004, 2004b, 2004c; 2006a; 2006b; 2007; NCTb 2006a, 2007 en 2007c): (a) het dierenrechtenactivisme, (b) het rechts-extremisme, en (c) het islamistisch[37] radicalisme. In geval van het rechts-extremisme

36 Om die reden is onder andere door de Amerikaanse overheid na de aanslagen van 11 september 2001 besloten om veel informatie van het internet te verwijderen die voorheen vrij toegankelijk was (Neve e.a., 2006).

37 Het begrip islamitisch refereert aan alles betreffende de islam als religie, terwijl het begrip islamistisch verwijst naar een radicale stroming binnen de islam met een duidelijk politieke agenda. Islamisten streven ernaar om de samenleving een weerspiegeling te laten zijn van de 'zuivere' islam (gebaseerd op een conservatieve, letterlijke interpretatie van de Koran [het heilige boek van de moslims] en de Hadieth [islamitische overleveringen over de profeet Mohammed]). Het islamisme kent gewelddadige,

(neo-nazisme, fascisme, racisme) en het islamistisch radicalisme (extreem-puriteins, intolerant en sterk antiwesterse *dawa*-georiënteerde vormen van de radicale islam) heeft dit vooral te maken met de maatschappelijke onrust die wordt veroorzaakt door racistisch of religieus gelegitimeerde aanvallen (Gemeente Amsterdam, 2006: 7). Volgens het NCTb (2007c) is er sprake van een levendige internetcultuur, zowel onder jongeren met een extreem-rechts fascistisch gedachtegoed als onder jongeren met een radicaal islamistisch gedachtegoed. Naar verwachting zal de wederzijdse kruisbestuiving tussen (inter)nationale rekrutering enerzijds, en de spontane lokale netwerkvorming van jongeren anderzijds, onder invloed van het internet de komende jaren gaan toenemen[38] (AIVD, 2006a: 59-60). Er is dus een duidelijke virtuele component die als verlengstuk van de 'fysieke werkelijkheid' is gaan fungeren. Voor een achtergrond en toelichting op de drie stromingen verwijzen we naar bijlage 4.

Terrorisme en ideologisch gemotiveerde misdaad

Nauw verwant aan radicalisering en extremisme is wanneer deze processen uitmonden in een vorm van terrorisme en ideologisch gemotiveerde misdaad Van terrorisme is sprake als het expliciet gaat om het '*…plegen van, of dreigen met, op mensenlevens gericht geweld dan wel om het toebrengen van ernstige maatschappij ontwrichtende schade met als doel maatschappelijke veranderingen te bewerkstelligen of politieke besluitvorming te beïnvloeden*'[39] (NCTb, 2006b: 17). Terrorisme moet worden gezien als het uiterste einde van radicaliseringprocessen: alle terroristen zijn extremisten, maar niet alle extremisten zijn terroristen (AIVD, 2004b: 6; Europol, 2007a: 9). Uit een recent verschenen Europol-rapport (2007a) blijkt dat de meeste terroristische aanslagen binnen de Europese Unie (EU) in 2006 werden gepleegd door etno-nationalistisch, separatistisch terroristen[40] en door links-radicalistische terroristen.[41] Ondanks het geringe aantal islamistisch gemotiveerde aanslagen binnen de EU in 2006 had de helft van de aan terrorisme gerelateerde *arrestaties* wel te maken

niet-gewelddadige en democratische varianten (AIVD, 2006b: 13). In dit rapport wordt de term islamitisch gehanteerd voor verwijzing naar de islam als religie in het algemeen, en de term islamistisch als expliciete verwijzing naar (ultra-)orthodoxe islamieten met een conservatieve radicaal-islamitische ideologie (bekering tot de islam) en daarin politiek gemotiveerd zijn.

38 Gegeven de aanwas van relatief goed opgeleide jongeren met ICT-expertise bestaat ook de mogelijkheid dat islamistische en criminele netwerken zich gaan vermengen en op steeds professionelere wijze gebruik zullen maken van ICT (AIVD, 2006a: 64).

39 Cyberterrorisme (aanvallen op vitale infrastructuren) valt in dit rapport onder *computer*criminaliteit. Bij terrorisme als vorm van *cyber*criminaliteit gaat het om de ondersteunde ICT-functie voor bijvoorbeeld rekrutering, fondsenwerving en trainingsdoeleinden.

40 Zij worden gemotiveerd door gevoelens van nationalisme, etniciteit of religie (bijvoorbeeld IRA, ETA en PKK) en plegen aanslagen tegen bedrijven, overheidsinstellingen, privé-eigendommen van burgers (bijvoorbeeld vakantiehuizen) en kritieke infrastructuren (zoals de spoorwegen in Madrid). Verdere criminele activiteiten zijn witwassen en creditcardfraude (*skimming*) (Europol, 2007a).

41 Zij hebben een revolutionaire, antikapitalistische ideologie en willen het politieke, sociale en economische systeem omgooien naar linkse maatstaven. Aanslagen (veelal met explosieven) zijn gericht tegen bedrijven en overheidsinstellingen. Criminele activiteiten zijn gewelddadig (afpersing, gewapende bankovervallen, ontvoering) maar ook is men betrokken bij witwassen (Europol, 2007a).

met islamistisch terrorisme.[42,43] Het internet speelt daarbij volgens de AIVD (2006b: 40) een steeds prominentere rol. Naar schatting waren er begin 2006 ongeveer 4.800 websites (inclusief chatrooms en nieuwsforums) van terroristen en sympathisanten in de lucht (Weimann, 2006: 624).
Specifiek voor de Nederlandse samenleving wordt de internationale dreiging vanuit radicaal-islamistische hoek als meest ernstig ervaren (AIVD, 2004b: 5). Dit komt mede tot uiting in het aantal gepubliceerde artikelen en rapportages over dit onderwerp. Het rechts-extremisme wordt net als het dierenrechtenactivisme doorgaans niet als terroristische stroming onderzocht, hoewel het door Europol wel als toenemende dreiging wordt beschouwd (Europol, 2007a: 35). Voor een korte toelichting op de specifieke rol van het internet bij het islamistisch terrorisme verwijzen we naar bijlage 5.

Afscherming met behulp van ICT
Van afscherming is sprake wanneer ICT wordt gebruikt om de communicatie binnen het criminele circuit op innovatieve wijze af te schermen (bijvoorbeeld via *encryptie*[44]). Van de makers van kinderporno is bijvoorbeeld bekend dat zij beschikken over steeds meer expertise en gebruikmaken van afschermingsmethoden (zoals encryptie) om buiten het domein van de opsporing te kunnen blijven (Van der Werf, 2003). Ook in bepaalde publieke virtuele omgevingen (zoals chatrooms, veilingsites, peer-to-peer of *P2P-netwerken*[45]) is het mogelijk om afgeschermd met elkaar te communiceren (Morris, 2004: 4). Bepaalde *jihadistische* websites worden bijvoorbeeld beschermd met wachtwoorden en bezoekers worden geacht aan te kunnen tonen dat zij de Arabische taal beheersen (via het invullen van registratieformulieren) (NCTb, 2006b: 53). Bij de aanslagen van 11 september 2001 in de Verenigde Staten en in 2004 in Madrid bleken de daders veelvuldig gebruik te hebben gemaakt van zogenoemde e-mail 'dead letter boxes': hotmailaccounts waarop meerdere gebruikers toegang hadden en waar berichten werden achtergelaten in de 'draft- of concept-folder'. Berichten konden door meerdere gebruikers worden ingezien en aangepast zonder dat zij daadwerkelijk werden verzonden, waardoor ze moeilijker te traceren zijn (NCTb, 2006b: 21).

42 Samen met Spanje, Italië en Frankrijk hield Nederland het hoogste aantal verdachten aan (Europol, 2007: 3).
43 Specifiek voor de Nederlandse samenleving wordt de internationale dreiging vanuit radicaal-islamistische hoek als meest ernstig ervaren (AIVD, 2004b: 5). Dit komt mede tot uiting in het aantal gepubliceerde artikelen en rapportages over dit onderwerp. Het rechts-extremisme wordt net als het dierenrechtenactivisme doorgaans niet als terroristische stroming onderzocht, hoewel het door Europol wel als toenemende dreiging wordt beschouwd (Europol, 2007a: 35).
44 Bij encryptie wordt informatie omgezet in voor buitenstaanders (en onbevoegden) onleesbare taal en codes.
45 Dit is een technologie waarbij een groep internetgebruikers (peers) een deel van de eigen computer openstelt voor anderen (sharing files) en zo onder meer muziek- en videobestanden met elkaar uitwisselt zonder tussenkomst van een server (men heeft direct toegang tot andermans computer).

Afschermingstechnieken kunnen echter ook verder gevorderde technische vaardigheden vereisen. Zo is het niet alleen mogelijk om gegevens te coderen in een tekst (cryptografie) maar ook om codes en gegevens te verhullen in kennelijk onschuldige afbeeldingen (steganografie). Bij steganografie wordt niet alleen de inhoud van een boodschap afgeschermd met andere informatie (zoals bij versleuteling/cryptografie), maar het hele bestaan van de boodschap wordt afgeschermd (bijvoorbeeld door geheime informatie en instructies in de afbeelding van een familieportret of in een digitale muziekclip te verhullen) (Gordon e.a., 2002). Bij een bekende afpersingszaak in Nederland van zuivelbedrijf Campina (periode 2002-2004) werd op ingenieuze wijze gebruikgemaakt van steganografie. Onder dreiging van het vergiftigen van toetjes werd het bedrijf gechanteerd om geld over te maken op een bankrekening waarvoor de dader de pinpas zou produceren. Hoewel de communicatie met de afperser in eerste instantie schriftelijk verliep (via brieven en kranten), eiste de dader op een later moment dat de benodigde code van het pasje versleuteld zou worden via steganografie in een fotoadvertentie op het internet. De dader (een 45-jarige IT-deskundige) werd uiteindelijk met hulp van de FBI opgespoord (Gelderblom, 2004: 123; OM, oktober 2005). Hoewel het daadwerkelijke gebruik van deze technische innovaties als steganografie nog beperkt lijkt, is er volgens het KLPD/DNRI (2004: 121) wel sprake van groeipotentie. Volgens de NCTb (2006b: 89) zal bovendien het gebruik van telefonie via het internet (*VoIP*)[46] en andere moderne afschermingstechnieken toenemen (NCTb, 2006b: 89).

2.3.2 Illegale handel

Behalve als communicatiemiddel wordt ICT ook als instrument gebruikt om handel en transacties mee tot stand te brengen. Niet alleen legale maar ook illegale goederen en diensten kunnen onbeperkt en zonder veel moeite op en via het internet worden verhandeld (bijvoorbeeld via veilingwebsites zoals Marktplaats of eBay)[47] (Europol, 2003: 30; KLPD, DNRI, 2004: 116-117; Morris, 2004: 18). In de navolgende paragrafen beschrijven we enkele verschijningsvormen die zich laten kenmerken door (tweezijdige) vrijwillige transacties tussen daders onderling[48] (zie ook schema 2):
- drugs;
- geneesmiddelen;
- vuurwapens en explosieven;
- kinderporno.

46 Vooral het aftappen van kleinere meer gedecentraliseerde VoIP-diensten is lastiger.
47 De daadwerkelijke omvang van illegale internethandel in Nederland is onbekend (Europol, 2003: 30; KLPD, DNRI, 2004: 116-117).
48 Het gaat dus niet om transacties tussen dader en slachtoffer, zoals het geval is bij financieel-economische criminaliteit. Bij kinderporno en mensenhandel en -smokkel worden de slachtoffers overigens beschouwd als (onvrijwillige) handel.

– heling;
– mensenhandel- en smokkel;
– softwarepiraterij;
– illegale kansspelen.

Drugs
Het produceren, verhandelen en bezitten van drugs is volgens de Opiumwet in Nederland strafbaar. Hoewel op het internet veelvuldig informatie kan worden verkregen met betrekking tot de benodigde apparatuur, chemische grondstoffen en de productie van bijvoorbeeld cannabis en XTC en dergelijke, zijn er bij het KLPD slechts enkele zaken bekend waarin via het internet (synthetische) drugs werden aangeboden (KLPD, DNRI, 2004). Ook volgens Europol (2003: 32-33) is er in Nederland in geringe mate sprake van handel in (soft)drugs via veilingwebsites. Naar schatting waren er volgens Europol in het jaar 2000 binnen de EU rond de 1.000 websites in de lucht (het merendeel uit Nederland en Zwitserland) waarin daadwerkelijk drugs werden aangeboden[49] (zie bijvoorbeeld www.project420.com uit Gelderblom, 2004: 98). Kenmerkend voor de handel via het internet is dat aanbieders en afnemers transacties verrichten zonder elkaar daadwerkelijk te (hoeven) ontmoeten. Je loopt dan als crimineel gemakkelijk in het oog bij de opsporing. Volgens Kortekaas (2005) is juist face-to-face contact bij de illegale handel in drugs belangrijk en is het om die reden dan ook '*…onwaarschijnlijk dat iemand op een website of via e-mail een container drugs aanbiedt*'.

Geneesmiddelen
Naar schatting 60% van alle spam die wij ontvangen maakt reclame voor medicijnen en pillen (Security.nl, 5 maart 2007). En wie kent ze niet: de massale aanbiedingen via spammail voor stimulerende middelen zoals Viagra®? Volgens de Wet op de Geneesmiddelenvoorziening (WOG) en de Wet Economische Delicten (WED) is het verboden om zonder vergunning (ongeregistreerde) geneesmiddelen in te voeren, te bereiden en te verhandelen. Ook de handel in merkvervalste geneesmiddelen is bij wet verboden. Uit onderzoek van de Nederlandse Inspectie voor de Gezondheidszorg (2004) bleek dat het aanbod van geneesmiddelen via internet groot is. Hoewel de daadwerkelijke handel volgens de inspectie niet precies is vast te stellen, is het aanbod vooral groot op het gebied van zogenoemde lifestylemiddelen (zoals seksgerelateerde middelen, partydrugs, kalmeringsmiddelen, dopingmiddelen en middelen tegen roken, overgewicht en kaalheid). In het najaar van 2006 heeft de

49 In de VS bedienen drugsdealers vooral via lokaal georiënteerde websites en nieuwsforums hun afzetmarkten met behulp van gecrypte advertenties en door chemische middelen (psychedelische drugs) onder het mom van wetenschappelijk onderzoek en laboratoriumproducten aan te bieden voor menselijke consumptie. Afnemers van de producten gebruiken gewoon creditcards om de goederen via het internet af te rekenen (Wikipedia).

opsporingsdienst FIOD-ECD bij invallen in Amsterdam nog ongeveer 250.000 neppillen (onder meer namaak-erectiepillen en afslankpillen) in beslag genomen die werden verhandeld via internet (Nu.nl, 23 november 2006). Los van de lifestylemiddelen is er in Nederland bovendien sprake van een groei in de handel van geneesmiddelen zonder recept (Europol , 2003: 32).[50] Het kopen van geneesmiddelen zonder recept via het internet (en in sommige gevallen ook lifestylemiddelen) brengt gevaren met zich mee voor de volksgezondheid (Interpol, 2007). Enerzijds omdat mensen medicijnen kopen en gebruiken zonder medisch advies, anderzijds omdat er geen enkele garantie bestaat dat wat men koopt daadwerkelijk het product is waarvoor het verkocht wordt (zie Security.nl, 5 maart 2007).

De wereldgezondheidsorganisatie schat dat 60% van de pillen en geneesmiddelen die op het internet wordt aangeboden nep is. Uit onderzoek van het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) (Blok-Tip e.a., 2005) naar 400 monsters die door de overheidsinspecties waren ingezonden voor chemische analyse bleek dat slechts 3% van de illegaal verhandelde erectiepillen daadwerkelijk Viagra was. In 30% van de onderzochte monsters ging het om doelbewust nagemaakte producten (bijvoorbeeld met onjuiste doseringen van de werkzame stoffen of andere actieve farmaceutische ingrediënten zoals cafeïne of amfetamine), en in ruim 60% van de gevallen betrof het nepproducten waarvan de aangetroffen bestanddelen uit de producten ook niet op de verpakking vermeld stonden. Volgens het RIVM (Blok-Tip e.a., 2005) worden steeds vaker (onbekende) chemische verbindingen aan kruidenproducten toegevoegd. Doordat hiervan de werking en bijwerking niet bekend zijn en kruidenproducten vaak gezien worden als natuurlijk en dus ongevaarlijk, is het risico voor de volksgezondheid veel groter. Dat dit soms dodelijke gevolgen heeft, wordt geïllustreerd door een incident in Canada waar een 57-jarige vrouw overleed na het innemen van vergiftigde kalmeringstabletten die zij via een website had gekocht (Cops, 2007g).

Vuurwapens en explosieven

In Nederland is volgens de Wet Wapens en Munitie (WWM) in principe het bezit van alle vuurwapens verboden (met uitzonderingen voor bepaalde vergunninghouders). Uit onderzoek van Spapens en Bruinsma (2004) blijkt dat jaarlijks naar schatting 10 tot 15.000 illegale vuurwapens Nederland binnenkomen. Bij de grotere importeurs gaat het om wekelijkse partijen van 30 à 50 vuurwapens die weer worden verkocht via tussenhandelaren verspreid over Nederland, maar een deel daarvan wordt doorgevoerd naar andere landen (bijvoorbeeld Groot-Brittannië). De

50 De zogenoemde 'no prescription websites' (websites waarop geneesmiddelen zonder recept verkrijgbaar zijn) worden vooral gehost vanuit landen waar bepaalde stoffen van het product legaal zijn (bijvoorbeeld opiumpreparaten in Mexico) (Wikipedia: http://en.wikipedia.org/wiki/Drug_trafficking, laatst geraadpleegd op 19 juli 2007).

kleinere importeurs werken vaak op bestelling en halen een partij wapens op wanneer er kopers voor zijn. De wijze waarop vuurwapens Nederland worden ingevoerd en worden verhandeld verschilt sterk per type wapen (Bruinsma en Moors, 2005: 87). Over de daadwerkelijke *internet*handel in vuurwapens en explosieven is in de literatuur weinig bekend. Uit onderzoek komt wel naar voren dat imitatiewapens besteld worden via het internet (bijvoorbeeld in Groot-Brittannië) (Bruinsma en Moors, 2005). Volgens een expert (aangehaald door Bruinsma en Moors, 2005: 77) zou het echter ook steeds makkelijker zijn geworden om via het internet aan echte wapens te komen. Recent onderzoek van Dijkshoorn en anderen (2007) naar het aanbod van verboden wapens op het internet toont aan dat op vier van de 800 onderzochte websites sprake was van aanbod van nepvuurwapens. De auteurs spreken van een 'verrassend lage uitkomst' (p. 25), waarbij overigens aangetekend moet worden dat alleen websites werden onderzocht die op enige wijze aan Nederland gelieerd konden worden (websites met de extensie .nl, Nederlandstalige websites en websites die op Nederlandse servers worden gehost). De cijfers geven dus geen beeld van de (nep)vuurwapens die te verkrijgen zijn op buitenlandse websites en/of websites die in het buitenland worden gehost.

Kinderporno

Van alle high-tech crimes roept het produceren en verhandelen van kinderporno maatschappelijk gezien volgens Stol (2001) de meeste weerzin op. Bij zedenzaken en andere seksgerelateerde verschijningsvormen (zoals kinderporno en grooming) spelen sociaal-ethische en maatschappelijke opvattingen een belangrijke rol. Op grond van de morele afkeuring die het oproept bij mensen, is de grens tussen onfatsoenlijk en strafwaardig gedrag volgens Lunnemann en anderen (2006: 102-103) echter niet altijd meer eenduidig. Kinderpornografie is volgens het Wetboek van Strafrecht (artikel 240b) '*…iedere afbeelding – of gegevensdrager die een afbeelding bevat – van een seksuele gedraging waarbij iemand, die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt, is betrokken of schijnbaar betrokken is*'. Zowel het verspreiden, tentoonstellen, vervaardigen, invoeren, doorvoeren, uitvoeren als in bezit hebben ervan is in Nederland strafbaar[51] (zie ook Stol, 2001). Kenmerkend aan de handel in kinderporno is dat het (in tegenstelling tot bijvoorbeeld de handel in verdovende middelen) volledig via de digitale snelweg kan verlopen doordat het materiaal zelf

51 Recentelijk is ook virtuele kinderporno onderwerp van aandacht: pornografisch materiaal dat door manipulatie tot stand is gekomen zonder dat daarbij kinderen zijn misbruikt of überhaupt zijn betrokken (denk bijvoorbeeld aan Second Life). Het OM heeft in februari 2007 aangekondigd proefprocessen te willen gaan voeren over virtuele kinderporno (AD, 24 april 2007). Ook het vervaardigen, bezitten en verspreiden van beeldmateriaal met dierenporno (of bestialiteit) heeft de laatste tijd meer aandacht gekregen. In Nederland is seks met dieren tot op heden alleen strafbaar als kan worden aangetoond dat het dier eronder lijdt. Onlangs werd echter een initiatief wetsontwerp ingediend in de Tweede Kamer voor het strafbaar stellen van het plegen van seksuele handelingen met dieren en pornografie met dieren (Cops, 2007f; TK 2006-2007, 31 009, nr. 1).

digitaal is. Stol (2001) spreekt daarom ook wel van '…*handel in criminele informatie*'.

Sinds de komst van het internet is het beeldmateriaal van kinderporno gewelddadiger geworden en worden daarvoor steeds jongere kinderen gebruikt. Afbeeldingen van baby's van een paar maanden oud die worden verkracht zijn daarbij geen uitzondering (Cops, 2007h; Lunnemann e.a., 2006: 109). Het materiaal lijkt voor de verzamelaar een 'verslavende' werking te hebben. Niet alleen wordt er obsessief 'verzameld' maar men wil ook steeds verdergaande plaatjes hebben (Van der Werf, 2003: 47). Met betrekking tot het soort plaatjes onderscheidt Sullivan (2007) drie soorten kinderporno: (1) seksueel getinte plaatjes van kinderen, (2) vernederende plaatjes van kinderen en volwassenen in relatie tot seks (bijvoorbeeld urine en uitwerpselen) maar ook bestialiteit (seks met dieren), en (3) gewelddadige plaatjes in relatie tot seks waarin zowel kinderen als volwassenen worden gemarteld. Hoewel de helft van de daders zich beperkt tot materiaal van de eerste categorie, richt een klein deel zich ook op materiaal van de andere categorieën (Sullivan, 2007).

Hoewel kinderporno aanvankelijk aangeboden werd op voor iedereen toegankelijke websites (waarvan de eigenaar gemakkelijk te achterhalen was), wordt in de verspreiding van het materiaal tegenwoordig steeds meer gebruikgemaakt van afschermingstechnieken. Foto's worden bijvoorbeeld in delen op verschillende servers gezet waardoor het complete plaatje moeilijk te vinden is. Pas als een klant een foto downloadt, komen de losse deeltjes op de computer van de klant samen (Metro, 18 april 2007). De verzamelaars van kinderporno maken meestal deel uit van min of meer georganiseerde netwerken[52] of nieuwsgroepen die gebruikmaken van afgeschermde delen van het internet (Stol, 2001; Van der Werf, 2003). Binnen deze virtuele 'pedofiele' netwerken gebruikt men bijvoorbeeld versleutelde e-mail en bestanden (door middel van *PGP-codes*[53]), groepsgewijze communicatie via *Internet Relay Chat (IRC)*[54] en *Microsoft Network Messenger (MSN*[55]), en peer-to-peer (P2P) uitwisselingsprogramma's[56] (waarbij documenten nooit werkelijk op het net komen te staan en dus moeilijker te traceren zijn) (Cops, 2007f; Lunnemann e.a., 2006: 105-108;

52 Meerdere personen werken om praktische redenen samen om gewin te behalen (dat niet per definitie financieel gewin hoeft te zijn) met ernstige gevolgen voor de Nederlandse samenleving (zie ook Boerman en Mooij, 2006: 13-15; Kleemans e.a., 2002; Van de Bunt en Kleemans, 2007).

53 Pretty Good Privacy (PGP) is een vercijferingsmethode (vorm van cryptografie) die veel wordt gebruikt op het internet (zie ook http://nl.wikipedia.org/wiki/Pretty_Good_Privacy).

54 Internet Relay Chat (IRC) is 'de elektronische babbelbox van het internet' (Govcert, 2007: 14): het stelt een gebruiker in staat om met meerdere mensen tegelijk, of juist met één gebruiker apart, te communiceren via getypte boodschappen. Vaak zijn IRC-kanalen ingericht op onderwerp zodat discussies zich concentreren op specifieke thema's voor belangstellenden.

55 Microsoft Network Messenger (MSN) is een chatprogramma dat als relatief veilig wordt beschouwd. Adressen van gebruikers zijn eenvoudig te blokkeren en gebruikers moeten expliciet aangeven of contactpersonen kunnen zien dat men online is.

56 Behalve eindgebruiker is men dan ook verspreider van het illegale materiaal.

Sullivan, 2005). Ook kan men onder alias een e-mail naar zichzelf sturen, het bericht zelf nooit openen maar wel aan anderen openstellen (een variant op de 'dead letter box').

Volgens het NDB2004 bestond er in Nederland nog geen directe relatie tussen kinderporno en seksueel misbruik van kinderen. Om die reden werd de dreiging niet als hoog ingeschat (KLPD/DNRI, 2004). Het aantal meldingen van kinderporno neemt echter nog altijd toe (KLPD, 2007). Recentelijk worden bovendien steeds meer video's aangeboden en foto's gebruikt als reclame waarmee klanten via spam e-mail en chatboxen naar websites worden gelokt (Lunnemann e.a., 2006: 104; Stol, 2004). Burgers kunnen meldingen van kinderporno doen bij het particuliere Meldpunt Kinderporno op Internet (MKI)[57] en bij het Meldpunt Cybercrime (MCC)[58] van het KLPD dat sinds 2006 is ingericht. Websites en nieuwsgroepen vormen het grootste deel van de meldingen die binnenkomen bij het Meldpunt Kinderporno op Internet (MKI). Het team van het KLPD dat zich bezighoudt met de bestrijding van kinderporno in Nederland behandelt tussen de 600 en 800 zaken per jaar (Cops, 2007h). In 2006 zijn er in Nederland rond de 2.600 aangiftes gedaan van kinderpornosites (waarvan het merendeel overigens in het buitenland werd gehost) en 71 aangiftes van verspreiding van kinderporno (Metro, 1 mei 2007: 4).

Heling

Wie zijn fiets kwijt is of andere duurzame goederen die bijvoorbeeld via een woninginbraak zijn buitgemaakt, doet er tegenwoordig goed aan om eens een zoektocht te houden op het internet. Het is niet denkbeeldig dat de spullen daar weer te koop worden aangeboden. Het kopen of verkopen van gestolen goederen staat bekend als heling en is volgens het Wetboek van Strafrecht (artikel 416) strafbaar in Nederland. Uit recent onderzoek naar helingpraktijken in Nederland (Van de Mheen e.a., 2007) bleek dat het voor de helft van de geregistreerde helingzaken gaat om auto's, fietsen en geld (witwassen) en voor de helft om goederen als elektronica, kleding, sieraden, genotsmiddelen en voeding. Populaire distributiekanalen zijn markten (zoals de Zwarte Markt in Beverwijk) en het internet. Als belangrijkste redenen voor het internetgebruik worden de grootte van de afzetmarkt genoemd en het feit dat het relatief veilig is (de pakkans is gering) om spullen langs deze weg te verkopen. Uit onderzoek van het KLPD blijkt ook dat steeds vaker gestolen goederen via websites als Marktplaats[59] en eBay worden aangeboden (computers, mobiele telefoons, auto's, sieraden, fietsen, brommers en dergelijke). Kopers en verkopers handelen meestal

57 Het meldpunt (www.meldpunt-kinderporno.nl) is sinds 1996 actief in Nederland.
58 Via het MCC (KLPD, 2007) kan tevens aangifte worden gedaan van het seksueel benaderen van kinderen (grooming) en van radicale en terroristische uitingen op en via het internet (zie ook bijlage 3).
59 Marktplaats.nl (een Nederlandse advertentiesite) schat dat 1% van de aangeboden advertenties verdacht is.

niet openlijk via het internet maar maken gebruik van *bulletin boards*[60] en chatrooms.

Mensenhandel en -smokkel
Mensenhandel is in Nederland strafbaar gesteld volgens het Wetboek van Strafrecht. Van mensenhandel is sprake wanneer iemand door dwang, (bedreiging met) geweld, afpersing, fraude, machtsmisbruik of misleiding wordt uitgebuit. Het gaat bijvoorbeeld om prostitutie, seksuele uitbuiting, gedwongen arbeid en slavernij[61] (Smit en Boot, 2007; TK 2005-2006, 29 911 nr. 4: 7). In Nederland heeft mensenhandel vooral betrekking op prostitutie en seksuele uitbuiting (met name van vrouwen uit Bulgarije, Nigeria, Roemenië en Rusland). Vrouwen worden vaak tegen hun wil in ontvoerd en vervolgens ingezet in de prostitutie. Criminelen die zich met deze praktijken bezighouden, veranderen hun ronselpraktijken en werkwijzen voortdurend. Zij verplaatsen bijvoorbeeld regelmatig hun werkterrein, wisselen om de zoveel tijd de werkplek van hun slachtoffers, en trekken zich steeds minder aan van landsgrenzen. Het internet wordt onder andere gebruikt voor het ronselen van potentiële slachtoffers (TK 2004-2005, 28 638, nr. 13: 14) en daders maken gebruik van chatrooms om met elkaar te communiceren (Europol, 2003: 32-33). Met de introductie van de webcam is een nieuwe vorm van seksindustrie aangeboord die mogelijk miljoenen omzet kan genereren (De Volkskrant, 23 augustus 2006). In hoeverre de meisjes achter de webcam vrijwillig seksuele handelingen verrichten en in hoeverre sprake is van bijvoorbeeld mensenhandel is vooralsnog onduidelijk[62] (Cops, 2007i).

Softwarepiraterij
Er zijn globaal vijf verschillende vormen van softwarepiraterij te onderscheiden (Business Software Alliance, 2007):
1. eindgebruikers (die bijvoorbeeld software zonder toestemming kopiëren of één licentie op meerdere computers installeren);
2. overgebruik van de client-server (waarbij meer gebruikers van een programma op een netwerk actief zijn dan de licentie toestaat);
3. internetpiraterij (het downloaden van software van het internet waarvoor geen licentie is verkregen, het onbevoegd uitwisselen van auteursrechtelijk beschermde programma's via P2P-netwerken, alsook internetveilingen die namaaksoftware aanbieden);
4. het laden van de harde schijf (het verkopen van nieuwe computers met illegale exemplaren van software op de harde schijf), en

60 Een *bulletin board* is een virtueel prikbordsysteem waarop mensen berichten kunnen achterlaten.
61 Ook werving, vervoer, huisvesting en ontvoering vallen hieronder, evenals het laten verwijderen van organen.
62 Een prostitutieteam van politie Brabant-Zuidoost heeft onlangs een actie gehouden waarbij negen illegale internetprostituees werden opgepakt. Zij werkten zonder vergunning maar waren wel meerderjarig en beweerden vrijwillig aan de internetactiviteiten mee te werken (Cops, 2007i).

5. het regelrecht vervalsen van software (het illegaal verveelvoudigen en verkopen van materiaal waarop auteursrecht rust met de bedoeling om het product te imiteren).

Bij piraterij gaat het feitelijk om illegale handel van allerhande '*cd's, dvd's, films, software en andere producten waarvoor auteursrechten gelden*' (KLPD, DNRI, 2004: 75). De nadruk ligt volgens de definitie van het KLPD echter veelal bij eindgebruikers (ad 1), internetpiraten (ad 3) en vervalsers (ad 5), en in mindere mate bij overgebruikers van licenties (bijvoorbeeld bedrijven) (ad 2) en computerverkopers (ad 4). In alle gevallen is piraterij echter strafbaar en valt het onder meer onder het Wetboek van Strafrecht, de Auteurswet en de Merkenwet.

Als de beveiliging van software, cd's en dvd's afwezig of gekraakt is, kan het produceren van illegale kopieën gemakkelijk op touw worden gezet. Vaak zijn de nieuwste uitgaven van bijvoorbeeld films en muziek eerder op het internet verkrijgbaar dan dat ze in de winkel liggen (Gelderblom, 2004: 104). Softwarepiraterij biedt bovendien grote winsten en in combinatie met een kleine pakkans maakt deze vorm van criminaliteit zich bijzonder aantrekkelijk voor criminelen (Europol, 2003: 27). Ook in het NDB2004 werd piraterij beschouwd als een dreiging voor de komende jaren (KLPD, DNRI, 2004: 75).

De stichting BREIN (Bescherming Rechten Entertainment Industrie Nederland) houdt zich sinds 1998 bezig met het bestrijden van intellectuele-eigendomsfraude (Molenaar, 2007). Volgens de Stichting Brein (2007) is er de laatste jaren een afname te zien in de omvang van illegale, vervalste software die wordt verkocht op markten, beurzen en advertentiesites (ad 5). Daar staat tegenover dat consumenten steeds vaker illegale software zelf produceren. Het betreft hier enerzijds eindgebruikers (met eigen cd- of dvd-branders) (ad 1) en anderzijds internetpiraten die downloaden van het internet (bijvoorbeeld via de P2P-uitwisselingssites) (ad 3). Door deze 'consumenten' wordt het illegaal kopiëren van muziek, films en games en het downloaden van bestanden met behulp van P2P-netwerken (zoals Napster, Gnutella, Kazaa, eDonkey) bijna als vanzelfsprekend ervaren. De illegale producten die zelf worden gebrand worden onderling cadeau gedaan, geruild of 'via via' verkocht in bijvoorbeeld sportkantines, op scholen en onder collega's. In sommige gevallen blijft echter sprake van 'bedrijfsmatige' piraterij, waarbij illegale cd's en dvd's bijvoorbeeld in platen- en cd-winkels gewoon in de schappen liggen ten behoeve van de verkoop.[63]

63 In februari 2007 arresteerde de Politie Haaglanden nog een 48-jarige verdachte (Brein, 2007b).

Illegale kansspelen
Volgens de Wet op de kansspelen (Wok) is er in Nederland een verbod op het aanbieden, propageren en gebruikmaken van kansspelen waarvoor geen vergunning is verleend. Illegale kansspelen en gokken op het internet (bijvoorbeeld het online casino[64]) is echter één van de groei-industrieën op internet en kan worden beschouwd als een specifieke vorm van illegale handel. Het risico voor consumenten van online gokken is (behalve het verslavingsgevoelige element) dat men niet weet wat de winkansen zijn en maar moet afwachten of de winsten ook daadwerkelijk worden uitgekeerd (NRC, 11 maart 1999). De grote bedragen die met de illegale exploitatie van kansspelen gepaard gaan maakt de sector uiterst aantrekkelijk voor criminelen (MvJ, 2007). Hoewel het in Nederland verboden is om kansspelen aan te bieden of te bevorderen zonder vergunning, is het niet verboden om mee te doen aan *buitenlandse* kansspelen en loterijen. Een knelpunt in de opsporing en vervolging van aanbieders van online kansspelen is dan ook dat aanbieders van goksites veelal gevestigd zijn in landen waar het organiseren van kansspelen niet strafbaar is of waar nauwelijks regulering of toezicht op kansspelen plaatsvindt. Veel internetcasino's zijn fysiek gevestigd in belastingparadijzen zoals de Dominicaanse Republiek (MvJ). In februari 2006 zei de toenmalig Minister Donner hierover (aangehaald door Planet internet, 16 februari 2006): '*…internet is het enige terrein waar je aanbod uit het buitenland nauwelijks kunt tegenhouden. Want internet is per definitie een ongeregelde massa. Nederlanders kunnen nu dus ook al meespelen op buitenlandse sites. Ik heb daar wel een probleem mee, maar ik kan er juridisch moeilijk tegen optreden*'. In een eerder verschenen rapport over de bestrijding van kansspelen via internet (KLPD, 2003) werd geconcludeerd dat er ondanks het staatsmonopolie talrijke internetsites bestaan met kansspelaanbod.[65] Een voorstel tot wijziging van de Wok dat voorziet in het proef aanbieden van kansspelen via internet is op 20 september 2006 aangenomen door de Tweede Kamer (MvJ, 2007; TK 2005-2006, 30 362 nr. 2). Holland Casino heeft als enige een tijdelijke vergunning gekregen en zal naar verwachting rond de zomer van 2007 met een goksite online gaan (Cops, 2007h).

2.3.3 Financieel-economische criminaliteit

ICT vormt tegenwoordig ook een belangrijk instrument voor plegers van financieel-economische (of witteboorden)criminaliteit. Het gaat hier om alle vormen van criminaliteit die als oogmerk hebben economisch of financieel voordeel te behalen door het wekken van enige vorm van valse schijn (Politieacademie, 2007). De Fiscale Inlichtingen- en

64 Variërend van blackjack tot fruitmachines en men betaalt per creditcard (Woodruff en Gregory, 2005).
65 Er werden 780 overtredingen van illegale kansspelen aangetroffen (in 86% virtuele casino's) die zich (mede) richtten op de Nederlandse markt (Planet internet, 19 september 2005).

Opsporingsdienst en de Economische Controle Dienst (FIOD-ECD) is verantwoordelijk voor de opsporing ervan (Molenaar, 2007). In tegenstelling tot illegale handel, waarbij sprake is van vrijwillige transacties tussen daders (vorige paragraaf), gaat het bij financieel-economische criminaliteit veelal om traditionele delicten waarbij de criminele activiteiten eenzijdig gericht zijn van dader naar slachtoffer.[66] Kenmerkend is dat ICT als instrument wordt gebruikt om anderen te bedriegen met geld (zoals fraude en oplichting). We beschrijven de volgende verschijningsvormen (zie ook schema 2):

– internetfraude (voorschotfraude en identiteitsfraude);
– marktmanipulatie;
– afpersing en chantage;
– witwassen.

Internetfraude

Internetfraude is een bulkbegrip van allerlei soorten fraude en oplichtingspraktijken waarbij gebruik wordt gemaakt van 'online services' (zoals chatrooms, e-mail, *message boards*, internetveilingen of websites).[67] Bij deze vorm van fraude wordt het internet gebruikt om op oneigenlijke wijze gelden, goederen en diensten te verkrijgen zonder daarvoor te betalen of tegenprestaties te leveren (Morris, 2004: 14). In veel gevallen gaat het om online veilingfraude. Hiervan is sprake als mensen goederen of diensten kopen via het internet (bijvoorbeeld valse online reisbureaus en valse mode- en fotobureausites) en vooruit betalen voor te leveren diensten maar deze niet krijgen (of van veel slechtere kwaliteit dan waarvoor men heeft betaald), of als de prijs van een artikel door de eigenaar kunstmatig wordt opgehoogd (Cops, 2007h; Europol, 2003; Taylor e.a., 2006: 112). Behalve het feit dat oplichting op zich in Nederland strafbaar is, gaat dit ook vaak gepaard met andere strafbare feiten (zoals documentvervalsing, valsheid in geschrifte en witwassen). In toenemende mate wordt internetfraude bovendien als middel gezien voor fondsenwerving van terroristen (NCTb, 2007: 80). In het NDB2004 (pp. 77-78) werd internetfraude[68] (in het bijzonder voorschotfraude en creditcardfraude) beschouwd als dreiging voor de Nederlandse samenleving. De meest voorkomende en beruchte vormen van internetfraude zijn de voorschotfraude en de identiteitsfraude. Beide varianten lichten we afzonderlijk toe.

66 Witwassen vormt wellicht een uitzondering omdat in principe niet direct een slachtoffer is aan te wijzen.

67 Ook clickfraude en *telecomfraude* kunnen als vormen van internetfraude worden bestempeld. Bij *clickfraude* worden internetgebruikers zonder het te weten omgeleid naar websites met dure inbelkosten, of worden adverteerders op kosten gejaagd doordat online advertenties massaal worden aangeklikt via geautomatiseerde commando's (botnets) (zie Ianelli en Hackworth, 2005: 10). Bij *telecomfraude* worden telecomgebruikers en de telecomsector de dupe van oplichting. Voorbeelden zijn *PBX-fraude* (op kosten van een bedrijf dure gesprekken voeren) en de *0900-fraude* (het inbelnummer van internetgebruikers wordt automatisch naar websites omgeleid tegen dure gesprekskosten) (zie ook Boerman en Mooij, 2006; Kerkdijk e.a., 2006; KLPD, DNRI, 2004: 88; Stratix, 2007).

68 In de V-NDB2006 (Boerman en Mooij, 2006) zijn alleen criminele verschijnselen onderzocht waarover in het NDB2004 onvoldoende informatie beschikbaar was om te spreken van een dreiging. Dit betrof tevens identiteitsfraude met behulp van phishing.

Voorschotfraude

De voorschotfraude (of 'advance fee fraud') wordt veelal in verband gebracht met Nigeriaanse oplichters. Zo'n 90% van de internetoplichters is Nigeriaan, en het aantal ongebruikelijke 'moneytransfers' (snelle betalingen van en naar het buitenland zonder tussenkomst van een bank) (zie ook Ernst & Young, 2006) van Nederland naar Nigeria is in 2005 bijna verdubbeld naar 10.500 transacties (Cops, 2007e). Het staat daarom ook bekend als de 'Nigerian scam' of '419-fraude' (naar artikel 4.1.9 van het Nigeriaanse wetboek van Strafrecht).[69] Bij de voorschotfraude is sprake van grootschalige oplichtingspraktijken waarbij mensen geld uit de zak wordt geklopt door voor dingen vooruit te betalen. Doorgaans wordt de slachtoffers een groot geldbedrag in het vooruitzicht gesteld (bijvoorbeeld van een erfenis, loterij of een investering) maar om dat te krijgen moet het slachtoffer wel eerst een geldbedrag (voorschot) betalen. Populaire scams[70] (zie Holt en Graves, 2007) zijn die waarin de afzender zich voordoet als publieke functionaris of ambtenaar die kans heeft gezien om geld af te romen van een bedrijfs- of overheidscontract (maar het geld alleen nog even kwijt moet op een bankrekening waarvoor men de hulp van het slachtoffer inroept). Ook zijn er varianten waarbij de afzender zich voordoet als bankier die een bankrekening wil opheffen van een overleden cliënt, maar dat geld elders wil parkeren om onopgemerkt te blijven. Populaire trucs zijn ook berichten waarin de ontvanger te horen krijgt een grote geldprijs uit een internationale loterij te hebben gewonnen. Hoewel de meeste slachtoffers zich bevinden in de Verenigde Staten komt het ook in Nederland kennelijk nogal eens voor dat men reageert op dergelijke 'winnende loterijen' (Neve, 2007). De nieuwste trend is dat internetoplichters gedupeerden (die eerder al grote geldbedragen zijn ontfutseld) opnieuw benaderen maar ditmaal door zich voor te doen als politieambtenaar die het slachtoffer wil helpen het verloren geld terug te krijgen. Het slachtoffer wordt onder het mom van 'onkostenvergoeding' wel weer verzocht een voorschot te betalen (Cops, 2007e). De schade per slachtoffer varieert tussen de 8.500 euro en 2,5 miljoen euro (Internetoplichting.nl, 2007).

In zijn traditionele vorm vielen dergelijke lucratieve voorstellen en bedelbrieven voorheen per post bij mensen op de deurmat. Tegenwoordig maken de oplichters intensief gebruik van (spam) e-mail.[71] Kenmerkend voor de meeste scams is dat de afzender (de

69 De bovenregionale recherche (van Noordwest en Midden Nederland, Rotterdam-Rijnmond, Haaglanden, Amsterdam-Amstelland), de Koninklijke Marechaussee en de DNRI van het KLPD hebben in het kader van deze oplichtingpraktijken het Apollo-onderzoek gestart naar West-Afrikaanse criminele netwerken. Het onderzoek wordt gecoördineerd door het OM Haarlem en richt zich op valsheid in geschrifte, valse reisdocumenten, valse betaalmiddelen, oplichting en witwassen. Tussen oktober 2006 en april 2007 werden al 63 arrestaties verricht (internetOplichting.nl, 2007).

70 De term 'scam' is een algemene aanduiding die verwijst naar allerlei soorten frauduleuze handelingen gericht op het afhandig maken van geld van anderen (Govcert, 2007: 15).

71 Gelderblom (2004: 198) beschrijft een aantal van deze zogenoemde Nigeriaanse bedelbrieven.

oplichter) zich ogenschijnlijk enigszins op het illegale vlak begeeft en het potentiële slachtoffer wordt aangesproken om te helpen (tegen een vaak onwaarschijnlijk hoge vergoeding, zoals een deel van de winst). De e-mailberichten waarvan gebruik wordt gemaakt, hebben de volgende kenmerken (Holt en Graves, 2007):

– er wordt de indruk gewekt dat het om een professionele afzender gaat (men gebruikt officiële symbolen en logo's);
– er wordt een verhaal verkondigd dat nauw aansluit bij recente gebeurtenissen in het land van de geadresseerde (het potentiële slachtoffer);
– er worden vaak religieus getinte en emotioneel geladen woorden gebruikt;
– er spreekt een algemene belofte uit dat de geadresseerde op een snelle en makkelijke manier geld kan verdienen.

Op het moment dat het slachtoffer reageert op een dergelijke uitnodiging, zijn er vervolgens drie opties. Het slachtoffer kan door de oplichters worden gevraagd:

– af te reizen naar het land waar zij zich bevinden voor nader overleg en ondersteuning (in sommige gevallen met ontvoering en moord tot gevolg) (zie Holt en Graves, 2007);
– een financieel voorschot te verlenen (door zogenoemde 'complicaties' in het proces zijn daarna echter telkens opnieuw betalingen van het slachtoffer nodig);
– of allerlei persoonlijke informatie te verstrekken (zoals naam, adres, werkgever, bankgegevens en dergelijke) waarmee de oplichters vervolgens hun slag slaan door bijvoorbeeld volledige bankrekeningen te plunderen (zie ook identiteitsfraude).

Bij deze vormen van misleiding en oplichting wordt vaak gebruikgemaakt van wat men noemt '*social engineering*'. Social engineering staat voor het onder valse voorwendselen verkrijgen van vertrouwelijke informatie (of ongeoorloofd een bedrijf binnenkomen) en benadrukt de menselijke betrokkenheid (tactieken) bij het verkrijgen van deze toegang of gevoelige informatie[72] (bijvoorbeeld door werknemers binnen een bedrijf te bespelen) (NCTb, 2007: 40). Vaak is het succes van deze werkwijze gebaseerd op (een combinatie van) overtuigingskracht en charisma van de dader maar ook hebzucht en naïviteit van het slachtoffer.

72 De term 'social engineering' werd oorspronkelijk gebruikt door fisofoof Karl Popper. Popper verwees hiermee naar een sociale en politieke hervorming waarbij de overheid niet meer dan randvoorwaarden zou moeten scheppen (een blauwdruk van concrete maatregelen en praktische wetsvoorstellen) voor een samenleving waarin het individu maximale vrijheid en kansen zou kunnen benutten (zie ook Bolkestein, 2001).

Identiteitsfraude

Van identiteitsfraude is sprake wanneer persoonlijke identificerende gegevens of vertrouwelijke informatie van mensen wordt misbruikt om hen vervolgens mee op te lichten (zie voor een uitgebreide omschrijving De Vries e.a., 2007). Het verkrijgen van de identiteitsgegevens is meestal geen doel op zich maar dient om andere criminele delicten mee mogelijk te maken (variërend van het plunderen van rekeningen tot het onder valse naam aanvragen van creditcards, bankrekeningen en hypotheken, of inbraak in bedrijfssystemen) (Europese Commissie, 2007; KLPD, DNRI, 2007a: 2). In Nederland is over de eerste twee maanden van 2007 de identiteitsfraude met maar liefst 200% toegenomen (Cops, 2007e). In de meeste gevallen gaat het om misbruik van verkregen creditcardgegevens waarmee online aankopen worden gedaan op andermans kosten (creditcardfraude) en om bankrekeningen die worden geplunderd (Molenaar, 2007). Doorgaans zijn de slachtoffers zelf betrokken bij het afstaan van informatie, maar niet altijd: gegevens worden ook verkregen via het hacken van bedrijfssystemen (bijvoorbeeld creditcardmaatschappijen) of omkoping van personeel. Onderstaand beschrijven we de meest voorkomende technieken die door de oplichters worden gebruikt om mensen zelf via digitale weg vertrouwelijke informatie te ontfutselen (NHTCC, 2006b: 33):

– Een veelgebruikte techniek is het versturen van *informatieverzoeken* per (spam) e-mail[73] waarin mensen op geraffineerde wijze wordt verzocht een (nagemaakte) bedrijvenwebsite te bezoeken (van bijvoorbeeld bankinstellingen) om persoonsgegevens in te vullen (Boerman en Mooij, 2006: 19; Stratix, 2007: 20). De informatieverzoeken lijken vaak officiële berichten afkomstig van een betrouwbare partij (bijvoorbeeld de bank of een collega) (KLPD, DNRI, 2004: 76; MessageLabs, 2005). Deze vorm van misleiding wordt ook wel '*phishing*' genoemd (Govcert, 2006: 65; Interpol, 2007; NHTCC, 2006b: 33). Er wordt als het ware 'gevist' naar gegevens (zoals creditcardnummers, sofi-nummers, geboortedata, bankgegevens of wachtwoorden voor bankrekeningen) en goedgelovige ontvangers van een dergelijk bericht geven deze informatie ook. Potentiële slachtoffers worden steeds vaker bewust uitgezocht en gericht aangeschreven. Zo worden e-mailberichten soms verstuurd alsof ze van een collega afkomstig zijn (van de IT- of HR-afdeling) en wordt gevraagd om bevestiging van beveiligingscodes en wachtwoorden. Medewerkers kunnen op die manier op achteloze wijze zeer vertrouwelijke informatie van een bedrijf bloot geven (MessageLabs, 2005). Identiteitsfraude met behulp van phishing wordt beschouwd als een van de snelst groeiende vormen van niet-gewelddadige criminaliteit

73 Volgens onderzoek van McAfee (aangehaald in Choo, 2007: 4) zou wereldwijd naar schatting 75 tot 150 miljoen phishing e-mails per dag worden verzonden.

(Rogers, 2006) en werd ook in het NDB2004 en de V-NDB2006 (Boerman en Mooij, 2006: 31) als voorwaardelijke dreiging gekwalificeerd. Criminelen gebruiken het internet om ervaringen, advies, werkwijzen en technieken met elkaar uit te wisselen (onder andere via IRC en openbare internetforums). Hele *phishing kits* met uitgebreide instructies en technieken om internetgebruikers op te lichten (inclusief kant-en-klare e-mailberichten, e-maillijsten en nepwebsites) zijn tegen betaling online verkrijgbaar (KLPD, DNRI, 2007a: 22). Opvallend is dat Nederland een prominente 10e plaats inneemt op de wereldranglijst van bronlanden van phishing (Molenaar, 2007). Stratix (2007: 24-25) voorziet dan ook het plan van de Nederlandse regering om één centrale digitale kluis te ontwikkelen (het Burger Service Nummer) als een lucratief doelwit van criminelen.

– Phishers maken (in aanvulling op bovenbeschreven techniek) ook intensief gebruik van de bestaande *sociale netwerksites* waarop persoonlijke informatie van mensen vrij verkrijgbaar is, zo vertelde de 18-jarige 'Lithium'. Hij zou naar eigen zeggen 20 miljoen identiteiten hebben gestolen via het internet en deze vervolgens hebben verkocht aan oplichters. Met zijn activiteiten verdiende hij ongeveer 3.000 tot 4.000 Amerikaanse dollar per dag (Cops, 2007j).
– Ook wordt in toenemende mate gebruikgemaakt van malware (malicious software)[74] waardoor slachtoffers die online contact opnemen met een legitieme instelling worden omgeleid naar een namaakwebsite zonder dat zij zich daarvan bewust zijn (het *omleiden naar een nepwebsite* staat ook bekend als '*pharming*')[75] (KLPD, DNRI, 2007a: 7). Banken en financiële instellingen hebben als beveiliging een dubbel authenticatieproces[76] ingevoerd maar ook daar hebben criminelen iets op gevonden. Zo werd een nieuw *Trojaans paard*[77] ontwikkeld dat via spam e-mail wordt verspreid. Dit programma zorgt ervoor dat klanten nadat zij de dubbele authenticatie hebben doorlopen alsnog worden omgeleid naar een nepvenster, terwijl oplichters via de originele ingelogde website van de bank ongestoord hun gang kunnen gaan door bijvoorbeeld rekeningen te plunderen (MessageLabs, 2005). In Nederland werden klanten van de ABN AMRO per

74 In de VS wisten hackers in december 2006 door middel van malware in het computersysteem van een grootwinkelbedrijf tientallen miljoenen gegevens buit te maken zoals creditcards, bankgegevens, rijbewijzen en identiteitsbewijzen (MKB-net, 2007).

75 Ook mensen die gebruikmaken van zogenoemde wifi-hotspots (toegangspunten waarop mensen een draadloze internetverbinding kunnen maken) kunnen slachtoffer worden van een nepwifi-hotspot. Deze frauduleuze netwerken worden ook wel 'evil twin attack' of 'man in the middle attack' genoemd: de communicatie tussen zender en ontvanger wordt onderschept door een oplichter en al dan niet aangepast doorgezonden (Cops, 2007j; KLPD, DNRI, 2007a: 18).

76 De tweefase-authenticatie is een beveiligde manier van inloggen met behulp van drie van de volgende aspecten: (1) kennis van de gebruiker (wachtwoord of pincode), (2) bezit van de gebruiker (bijvoorbeeld een codegenerator), of (3) fysieke kenmerken van de gebruiker (bijvoorbeeld irisscan) (Govcert, 2007).

77 Een *Trojaans paard* is een programma dat ongewenst meekomt met een ander programma dat door de computergebruiker wordt geïnstalleerd. Het nestelt zich op de harde schijf en zorgt ervoor dat computers worden opengezet voor andere gebruikers en de besmette computer kan ook worden ingezet bij een dDoS-aanval (Wikipedia, laatst geraadpleegd op 19 juli 2007).

e-mail benaderd via het zogenoemde supportcentrum van de bank om een .exe programma op hun computer te installeren. In werkelijkheid bleek het bericht afkomstig van oplichters en betrof het een kwaadaardig programma (Trojaans paard) dat wachtwoorden en informatie ingevuld op webformulieren opslaat. De oplichters in deze zaak waren overigens niet succesvol in hun onderneming (Govcert, 2007).

Marktmanipulatie

Een andere vorm van cybercriminaliteit, in de vorm van handel met voorkennis, betreft het manipuleren van aandelenprijzen door het verspreiden van (onjuiste) informatie en geruchten (bijvoorbeeld van mogelijke overnames of interne problemen binnen organisaties) in chatrooms, internetforums en via e-mail (spamming) (Van Amersfoort e.a., 2002). Het manipuleren van aandelenkoersen staat ook wel bekend als 'pump 'n dump' of 'trash and cash'[78] oplichting (Morris, 2004: 17). Door het verspreiden van dergelijke informatie kan via aandelen- en optiehandel met voorkennis veel winst worden behaald, soms ook door afpersing. In Nederland is bijvoorbeeld een zaak bekend van een Nederlandse man die in 2006 op beleggersforums allerlei informatie over een Brits bedrijf verspreidde waarmee hij koersdalingen veroorzaakte. Vervolgens heeft hij onder dreiging van het voortzetten van zijn lastercampagne via internet het bedrijf via e-mail, fax en telefoongesprekken afgeperst. De man eiste onder andere aandelen van het bedrijf (Netkwesties, 8 mei 2006).

Afpersing en chantage

Bedreiging en afpersing is volgens het Wetboek van Strafrecht strafbaar in Nederland. Afpersing is het op illegale wijze verkrijgen van geld of goederen van een persoon of organisatie door middel van dreiging en/of geweld (Morris, 2004: 15). De cybervorm van afpersing is meestal gelegen in het dreigen met: een dDoS-aanval[79] (waardoor klanten niet meer bij een website van een bedrijf kunnen komen), het beschadigen van essentiële gegevens (zoals klant- en productenbestanden), het verstoren of beschadigen van industriële productiesystemen, het publiekelijk maken van gevoelige informatie (bijvoorbeeld via hacking verkregen), geruchten (zoals bij marktmanipulatie), of geweld. Zo zijn er gevallen bekend waarbij ontvangers van e-mailberichten (veelal mensen met een hoog inkomen, zoals artsen, advocaten en ondernemers) wordt verteld dat zij op een zwarte lijst staan om geliquideerd te worden maar dat de moordenaar

78 Bij positieve manipulatie worden aandelen direct na het stijgen van de aandelenprijzen verkocht met grote winst (pump 'n dump), of omgekeerd worden aandelen bij negatieve manipulatie direct na het zakken van de aandelenprijzen gekocht en na stabilisatie van het aandeel weer verkocht met grote winst (short-selling).

79 Het KLPD/DNRI (2007b: 2) geeft aan een dDoS-aanval gericht op afpersing de volgende definitie: '…het door middel van (dreiging met) een dDoS-aanval op computers, computernetwerken, servers of sites met als doel een persoon of organisatie te dwingen tot afgifte van geld of goederen'.

voor een kleine financiële vergoeding (bijvoorbeeld 30.000 dollar) de aanslag niet zal uitvoeren (Cops, 2007i). Een fenomeen dat recentelijk vaker de kop opsteekt is dat slachtoffers via het internet naar een locatie worden gelokt voor een seksuele ontmoeting (bijvoorbeeld via een seks-chatbox) waar zij worden overmeesterd, ontvoerd en onder bedreiging van geweld worden afgeperst (pinpas en pincodes worden afgegeven waarna geld van de rekening van het slachtoffer wordt gestolen) (Cops, 2007g; Webwereld, 2006). Met name afpersing met behulp van een dDoS-aanval werd in het NDB2004 als potentiële dreiging voor de Nederlandse samenleving aangemerkt. Vaak worden onder dreiging van een dDoS-aanval geld of goederen geëist van bedrijven die voor de bedrijfsvoering sterk afhankelijk zijn van het internet (bijvoorbeeld online casino's of goksites van bijvoorbeeld paardenraces). Als niet wordt betaald, gaat de website uit de lucht met alle gevolgen (financiële schade) van dien. Molenaar (2007) ziet overeenkomst met '*…het klassieke beschermingsgeld dat de maffia eist van winkeliers en horecaondernemers*'.

Er bestaat vooralsnog geen goed beeld van het aantal afpersingspogingen op en via het internet in Nederland. Dit heeft mede te maken met registratieproblemen (het betreft immers digitale varianten van traditionele misdaden), met een gebrek aan aangiftes (bedrijven zijn bang voor imagoschade en willen anderen niet op een idee brengen), en met het feit dat een deel van de dDoS-aanvallen gericht is tegen illegale bedrijven die zelf niet met de politie in aanraking willen komen (Europol, 2003: 12; KLPD, DNRI, 2007b: 6; Van der Werf, 2003). In het V-NDB2006 (Boerman en Mooij, 2006: 35; zie ook KLPD, DNRI, 2007b) werd afpersing met behulp van een dDoS-aanval door het geringe aantal (bekende) afpersingsgevallen niet meer als concrete dreiging gezien.

Witwassen

Ook witwassen is strafbaar volgens het Wetboek van Strafrecht in Nederland (artikel 420bis). Van witwassen is sprake wanneer misdaadgeld met zoveel mogelijk discretie in het legale financieel-economische circuit wordt ingebracht (bijvoorbeeld in onroerend goed): illegaal verkregen geld wordt dus op legale wijze belegd of geïnvesteerd, zodat zwart geld wit wordt gemaakt (Morris, 2004: 13). Dit is een strafbaar feit in Nederland (Wetboek van Strafrecht, artikel 420bis). Criminelen proberen de werkelijke oorsprong van grote geldbedragen te verhullen door legale economische transacties als dekmantel te gebruiken. Hiermee wordt het vermogen uit handen van de opsporingsdiensten gehouden en worden sporen gewist die leiden naar de dader van het misdrijf (Verrest, 2006: 41). Witwassen is in de fysieke wereld niet zelden gerelateerd aan casino's (waar ook in de virtuele wereld casino's gebruikt worden als dekmantel voor crimineel geld) (Cops, 2007h). Volgens Europol (2003: 40) zijn er bovendien redenen

om aan te nemen dat *e-commerce*[80] (elektronisch), *m-commerce*[81] (mobiel) en online veilingsites gerelateerd zijn aan witwaspraktijken door de grote virtuele betalingsstromen die hierin omgaan.

2.3.4 llegale communicatie

Eerder in dit rapport is aandacht besteed aan de ondersteunende functies van ICT ten behoeve van communicatie voor illegale doeleinden (radicalisering, terrorisme, afscherming van criminele activiteiten). Wanneer ICT wordt gebruikt (of misbruikt) om boodschappen van *illegale inhoud* uit te dragen, spreken we van illegale communicatie. Het betreft hier vooral strafbare digitale vormen van gedragsdelicten[82] waarbij de persoonlijke levenssfeer of publieke moraal wordt aangetast (stalking, discriminatie, kinderlokken/grooming) (NHTCC/NPAC, 2006a), maar ook het op illegale wijze verkrijgen van andermans gegevens en informatie (spionage). Qua inhoud verschillen deze vormen nauwelijks van de varianten ervan in de fysieke wereld (Van der Werf, 2003: 37). Kenmerkend is dat daders gebruikmaken van ICT als (eenzijdig) communicatiemiddel richting het slachtoffer. In de volgende paragrafen lichten we de volgende verschijningsvormen nader toe (zie ook schema 2):

– cyberstalking;
– discriminatie;
– grooming;
– spionage.

Cyberstalking

De definitie van stalking is het stelselmatig en op dwangmatige wijze lastigvallen van een persoon door die ander te achtervolgen, steeds op hinderlijke wijze contact op te nemen, en soms te bedreigen. Volgens het Wetboek van Strafrecht zijn dergelijke handelingen (belaging) pas strafbaar wanneer het slachtoffer dat hiervan inbreuk ondervindt op zijn of haar persoonlijke levenssfeer aangifte doet bij de politie. Als digitale variant is cyberstalking de verzamelnaam voor het stelselmatig lastigvallen van een persoon door provocerende uitspraken te doen en/of berichten te plaatsen via online forums, *bulletin boards* en chatrooms, of de ander als het ware via *spyware* te bespioneren dan wel voortdurend ongevraagd e-mail en spam te sturen. Het gaat in feite om een variant van huisvredebreuk waarbij sprake is van een verregaande inbreuk op de privacy van het slachtoffer (Benschop, 2007b; D'Ovidio en Doyle, 2003).

80 E-commerce verwijst naar bedrijven en organisaties die voor hun functioneren gebruikmaken van digitale communicatie en transacties (Europol, 2003: 65).
81 M-commerce is de mobiele variant van e-commerce (handel via het internet) waarbij handel wordt gedreven via draadloze mobiele media en klanten betalingen verrichten via de mobiele telefoon (Interpay, 2007).
82 Bij gedragsdelicten is het verrichten van de strafbare gedragingen op zichzelf strafbaar, zonder dat voor de strafbaarheid een bepaald gevolg moet intreden.

Sommige cyberstalkers gebruiken speciale programma's om op gezette of willekeurige tijdstippen bedreigende en intimiderende boodschappen te versturen zonder zelf fysiek aanwezig te zijn bij een computer. Ook kunnen beledigende pagina's met foto's en gegevens van het slachtoffer op het internet geplaatst worden. Bovendien kunnen ook andere internetgebruikers worden oproepen om het slachtoffer lastig te vallen of te bedreigen. Dat het niet alleen om onschuldige pesterijtjes gaat, illustreert de zaak Dellapenta uit de Verenigde Staten (1999, Los Angeles). Een 50-jarige beveiligingsbeambte deed zich op het internet voor als het slachtoffer (een 28-jarige vrouw) die een heimelijke seksuele fantasie zou hebben om verkracht te worden. In diverse seksueel getinte chatboxen liet de man informatie achter op het internet met uitgebreide beschrijvingen van het uiterlijk van de vrouw, haar adres, telefoonnummer, en zelfs aanwijzingen hoe het alarmsysteem van haar woning moest worden uitgeschakeld. De man wilde op deze manier wraak nemen omdat het slachtoffer niet was ingegaan op zijn avances. Behalve diverse telefoontjes van geïnteresseerden kreeg de vrouw in die periode zes mannen aan de deur, midden in de nacht, die 'bereid' waren haar te verkrachten (Samut, 2000).

Discriminatie

Negatieve gedragingen in de richting van andere personen (of groepen) zoals we die in de fysieke wereld kennen hebben ook hun uitingsvormen gekregen via het internet. Te denken valt aan belediging, smaad, laster, discriminatie, oproepen tot geweld en bedreiging. Een belediging is een opmerking, geschrift of afbeelding die door anderen als negatief en kwetsend wordt ervaren. Smaad is het opzettelijk aantasten van iemands eer of goede naam door verspreiding van een bepaald feit (of dat nu waar is of niet) en laster is het opzettelijk verspreiden van informatie waarvan de dader weet dat het een leugen is (Iusmentis, 27 oktober 2006). Discriminatie moet worden opgevat als een algemene uitingsvorm van onverdraagzaamheid jegens anderen waarbij ongegrond onderscheid wordt gemaakt tussen mensen (bijvoorbeeld op grond van godsdienst, levensovertuiging of geslacht). Volgens artikel 1 uit de Nederlandse Grondwet is discriminatie wegens godsdienst, levensovertuiging, politieke gezindheid, etniciteit, geslacht of op welke grond dan ook, niet toegestaan. Het zich in het *openbaar* opzettelijk beledigend uitlaten over een groep mensen wegens hun etnische achtergrond, godsdienst of levensovertuiging of seksuele gerichtheid is in Nederland dan ook strafbaar volgens het Wetboek van Strafrecht (artikel 137c). Dit staat min of meer op gespannen voet met het recht op de vrijheid van meningsuiting (artikel 7 van de Grondwet). Wanneer het uiten van een mening te ver gaat is dan ook niet altijd eenvoudig aan te geven. Bij het Meldpunt Discriminatie Internet (MDI)[83] kan men melding doen van uitingen op het internet van

83 Zie ook www.meldpunt.nl.

discriminatie. Behalve de vijandige houding ten opzichte van joden is er in Nederlands sprake van een toename in het aantal meldingen van discriminatie van moslims (Cops, 2007j; Van Stokkom e.a., 2007: 190-195).

Oproepen tot discriminatie en/of geweld wordt ook wel haatzaaien (of hate speech) genoemd.[84] Uitingsvormen hiervan hebben vaak de vorm van opruiende discussies op virtuele ontmoetingsplaatsen of discussiefora, teksten die worden gepubliceerd, maar ook afbeeldingen (bijvoorbeeld cartoons). Er is een onderscheid tussen georganiseerde haatgroepen zoals het islamistisch radicalisme en het rechts-extremisme (zie paragraaf 2.3.1: radicalisering en bijlage 4) en informele netwerken waarin individuen op discussiefora elkaar uitschelden, beledigen, belasteren, discrimineren, aanzetten tot haat en anderen soms zelf met de dood bedreigen. Op dergelijke discussiefora kan men relatief anoniem in discussie gaan met andere deelnemers. Hierdoor veroorloven mensen zich uitspraken die zij zich in het dagelijkse leven (vermoedelijk) niet zouden permitteren. Door de anonimiteit van het internet is sprake van een verharding en het aantal haatuitingen op internet is de laatste jaren flink toegenomen. Van Stokkom e.a. (2007) spreken wel van een haatepidemie op het internet. Onderzoek van Mann e.a. (2003) naar racistische haatgroepen op het internet wees uit dat een relatief kleine kern een groot gedeelte van de discussies op de webforums domineert: 1% van de bezoekers is verantwoordelijk voor maar liefst 45% van alle berichten (en 10% van de bezoekers zelfs voor 83% van alle berichten). Ook is er sprake van vele zogenoemde 'crossposting's' waarbij voortdurend berichten van de ene nieuwsgroep naar de andere nieuwsgroep worden verstuurd. Meer recentelijk worden innovatieve methoden en technieken toegepast om de communicatie tussen (leden van) haatgroepen te kunnen identificeren en analyseren (zie Chau en Xu, 2007). Met behulp van bijvoorbeeld 'web mining' (analyse van informatie uit tekst-, beeld- of audiomateriaal), sociale netwerkanalyse (analyse van structuren waarbij belangrijke knooppunten en interacties kunnen worden aangewezen), en 'usage mining' (analyse van gebruikersprofielen) kunnen bepaalde groepen op het internet worden geïdentificeerd die een bedreiging vormen voor de samenleving.

Grooming

Ontucht met minderjarigen is volgens het Wetboek van Strafrecht in Nederland strafbaar. Met de introductie van het internet is het voor volwassenen echter makkelijker geworden om zich op chatsites en MSN anders voor te doen (bijvoorbeeld als kinderen of als eigenaar van een modellenbureau[85]) met het doel om seksueel getinte contacten te leggen met kinderen. Deze onheuse benadering van volwassenen richting min-

84 Schafer (2003) beschrijft in stappen hoe een dergelijk 'haatproces' verloopt.

85 Recentelijk komen er meer meldingen binnen van mannen die doen alsof ze van een modellenbureau zijn en bijvoorbeeld aan jonge meisjes vragen voor de webcam te bewegen (Cops, 2007m).

derjarigen op het internet wordt ook wel '*grooming*' genoemd. Het contact kan een erotische kant opgestuurd worden, virtueel (bijvoor-beeld door seksuele handelingen te laten verrichten voor de webcam) maar ook fysiek (waarbij een ontmoeting plaats heeft en het kind daadwerkelijk seksueel misbruikt wordt) (Cops, 2007h; Lunnemann e.a., 2006: 107; Metro, 20 maart 2007; Metro, 9 mei 2007b). Ook in Nederland zijn er kinderlokkers op het internet actief en zij gebruiken internetfora onder meer om onderling tips en trucs uit te wisselen (bijvoorbeeld over hoe ze het beste het vertrouwen kunnen winnen van kinderen).[86] Volgens KLPD'er Groeneveld (aangehaald in Metro, 20 maart 2007: 8) gaan de daders geroutineerd te werk: '*…De mannen weten heel precies hoe ze het vertrouwen van een kind moeten winnen. Vaak maken ze ook deel uit van een heel netwerk. Zo gauw één van de mannen met een kind in gesprek is, gaan de anderen gemene berichtjes sturen en het kind pesten. De eerste man komt dan voor het kind op en zo wekt hij het vertrouwen. Het einddoel is natuurlijk altijd een afspraakje met seks.*' In tegenstelling tot andere Europese landen, zoals Engeland, is grooming in Nederland nog niet verboden (Cops, 2007f). Minister Hirsch Ballin van Justitie heeft op 9 september 2007 in het tv-programma Buitenhof wel kenbaar gemaakt preventief te willen gaan optreden en grooming te willen gaan verbieden: volwassenen die via internet onder een valse naam contact zoeken met kinderen (of zich op chatsites voordoen als een kind), met als doel om hen seksueel te misbruiken, worden strafbaar.

Spionage

Spionage is het op illegale wijze, zonder toestemming verkrijgen van informatie door het gebruik van spionnen of andere middelen[87] (Morris, 2004: 16). Met behulp van ogenschijnlijk onschuldige softwareapplicaties (spyware) kunnen computer- en telefoongegevens ongemerkt worden onderschept, afgeluisterd of bespioneerd.[88] Methoden die hiertoe worden ingezet zijn volgens Van Amersfoort e.a. (2002: 26):

– aanvallen van buitenaf (hacking);
– het gebruik van *spyware* (*keyloggers*) en *malware* (Trojaanse paarden);[89]

86 Uit onderzoek blijkt dat jongeren tijdens het chatten snel vertrouwen hebben in de chatpartner en erg openhartig zijn (Cops, 2007d). Dit geldt niet alleen voor contacten met volwassenen maar ook tussen jongeren onderling. Zo blijkt uit onderzoek van het Kenniscentrum Seksualiteit dat maar liefst 40% van de jongens en 57% van de meisjes wel eens een verzoek om cyberseks heeft gehad, en dat 25% van de jongens en 20% van de meisjes hier daadwerkelijk aan heeft toegegeven (Spits, 9 mei 2007).

87 Bijvoorbeeld bedrijfsspionage, politieke of militaire spionage waarbij toegang wordt verkregen tot geheime informatie.

88 Ook wel bekend als *sniffing* (Govcert, 2006: 60).

89 *Spyware* staat voor (onderdelen van) vaak gratis aangeboden en te downloaden software waarbij ongemerkt gegevens en informatie van een computer (of gebruiker) wordt verzameld en doorgestuurd naar een derde partij (bijvoorbeeld surfgedrag op het internet). Meestal wordt de verkregen informatie gebruikt voor marketing- en reclamedoeleinden. Keystroke logging (of *keylogging*) is een instrument dat bijhoudt wat er via het toetsenbord en aan muiskliks wordt ingetypt (bijvoorbeeld passwords) en ook deze gegevens worden doorgestuurd naar een derde partij (KLPD, DNRI, 2007a: 15; Wikipedia, laatst geraadpleegd op 19 juli 2007: http://nl.wikipedia.org/wiki/Spyware). Spyware kan met een virus worden verspreid of via een Trojaans paard (als aanhangsel van een programma dat wordt geïnstalleerd)

– hulp van binnenuit (corrupte medewerkers);
– interceptie (taps op dataverkeer).

Volgens Govcert (2007: 13) waren in 2006 de meeste pogingen om spyware op andermans computer te installeren afkomstig uit China, de Verenigde Staten, Nederland en Frankrijk. Verwacht wordt dat het gebruik van keyloggers en spyware om toegang te krijgen tot geheime informatie (spionage) een lucratieve misdaad wordt die in de toekomst op grotere schaal door criminelen zal worden ontdekt (McAfee, 2006: 18-19). Volgens experts neemt de kans toe dat criminelen gaan proberen gebruik te maken van corruptie en infiltratie (KLPD, DNRI, 2004: 115, 121).

2.4 Computercriminaliteit: ICT als instrument én doelwit

Computercriminaliteit betreft alle criminaliteitsvormen waarbij ICT behalve instrument ook expliciet doelwit is van de criminele activiteiten. Dit kan zijn het gebruik van ICT om in te breken op netwerken en systemen, om de functionaliteiten van ICT te verstoren, of om geautomatiseerd opgeslagen gegevens te manipuleren (beschadigen, wijzigen, vernietigen). Deze 'nieuwe vormen van criminaliteit' die zonder het bestaan van ICT dus niet mogelijk waren geweest, staan omschreven in de Wet op de Computercriminaliteit (I en II). We onderscheiden in dit rapport de volgende clustering van thema's van computercriminaliteit waarvan in de volgende paragrafen een aantal verschijningsvormen nader zullen worden toegelicht (zie ook schema 2):
– ongeautoriseerde toegang tot ICT (paragraaf 2.4.1);
– ICT-storing door gegevensverkeer (paragraaf 2.4.2);
– ICT-storing door manipulatie van data en systemen (paragraaf 2.4.3);
– dienstverleners (paragraaf 2.4.4).

2.4.1 Ongeautoriseerde toegang tot ICT

Ondanks allerlei beveiligingsmaatregelen is het mogelijk dat mensen, zonder daartoe de bevoegde autorisatie te hebben, inbreken op ICT-netwerken en systemen. Er wordt dan wel gesproken van 'computervredebreuk' of 'hacking' en dit is in Nederland strafbaar gesteld.[90] Er zijn verschillende technieken die (vaak in combinatie) worden toegepast om te kunnen

ongemerkt worden geïnstalleerd op de computer. *Malware* (afkorting van 'malicious software') is het bulkbegrip voor computerprogramma's die zonder toestemming van de eigenaar/beheerder draaien op een computer en het systeem iets laten doen naar de wens van een buitenstaander. Zie voor een overzicht tevens paragraaf 2.4.

90 Onder de oude Wet op de Computercriminaliteit I was het inbreken op systemen alleen strafbaar indien de systeembeveiliging werd doorbroken door een technische ingreep. Deze eis is in de nieuwe Wet op de Computercriminaliteit II komen te vervallen: het inbreken op systemen is per definitie strafbaar zodra men zich op verboden terrein begeeft.

inbreken op systemen. We geven hier een uitgebreide beschrijving van hacking en botnets.

Hacking
Wanneer iemand zich op ongeautoriseerde wijze van buitenaf toegang verschaft tot ICT (computers, netwerken, systemen), is er sprake van 'hacking'. Hackers deden dit voorheen voornamelijk als hobby om veiligheidslekken in systemen aan te tonen. Hoe moeilijker de klus, hoe meer status men verwierf wanneer men erin slaagde 'binnen te komen'. Onder de hackers bestaat een ware (sub)cultuur met eigen regels en gebruiken. Daarbij is sprake van een subcultuur met een specifieke statushiërarchie, specifieke taal, normen en symbolen (Turgeman-Goldschmidt, 2005). Binnen de hackinggemeenschap delen de leden van de groep een sociale identiteit die volgens Jordan en Taylor (1998) gebaseerd is op zes indicatoren (ook aangehaald door Van der Werf, 2003):
– plezier in technologie en het onverwachtse, innovatieve gebruik ervan;
– een spanningsveld tussen geheimhouding (uit handen blijven van de opsporing) en publiciteit (informatie delen om erkenning te krijgen);
– anonimiteit (de werkelijke 'off-line' identiteit wordt verborgen gehouden);
– fluïditeit (een informele cultuur waar men soms wel en soms niet bij hoort);
– masculiene en vrouwonvriendelijke attitudes;
– voortdurende expliciete reflectie op de motivatie van het hacken (verslavende werking, nieuwsgierigheid, sensatie, macht, erkenning, en de dienstverlenende functie van het ontdekken van gaten in de beveiliging).

Hackers kunnen groepsgewijs werken in dezelfde fysieke ruimte of juist geïsoleerd maar wel deel uitmakend van een groep die af en toe samenkomt (bijvoorbeeld via bulletin boards).[91] Binnen de sociale groepen of gemeenschap voorziet men elkaar van informatie, expertise, sociale steun, training, tijdschriften en zelfs conferenties (Europol, 2003: 74; Jordan en Taylor, 1998: 758). Er is sprake van grote statusverschillen: om in aanzien te stijgen moet men zich bewijzen door anderen telkens te overtreffen met nieuwere, meer innovatieve en slimmere technieken en vaardigheden[92] (Europol, 2003: 72, 114). Tegenwoordig zijn hackers echter steeds meer financieel gemotiveerd geraakt en is er sprake van een trend

91 Toegang tot sommige bulletin boards verkrijgt men soms pas nadat men zich in technisch opzicht heeft bewezen. Sommige hackers nemen dan ook zogenoemde trofeeën of overwinningstekens mee om te laten zien (Jordan en Taylor, 1998).
92 Op een hackerconferentie in 2000 toonde een Nederlands computerbeveiligingsbedrijf aan in te kunnen breken op het tot dan toe veronderstelde onaantastbare Lotus Notes systeem (software die door nagenoeg alle banken, verzekeraars, accountantskantoren en inlichtingendiensten van overheden wordt gebruikt om vertrouwelijke informatie in op te slaan en onderling uit te wisselen) (NRC Handelsblad, 1 augustus 2000).

van '*hacking for fame*' naar *'hacking for fortune'* (Boerman en Mooij, 2006: 22). Hackers opereren dus steeds vaker met criminele bedoelingen en raken in toenemende mate betrokken bij criminele organisaties. Om die reden worden ze ook wel 'crackers' (criminele hackers) genoemd (Boerman en Mooij, 2006: 22; Govcert, 2006: 32). In Rusland, waar hacking als alternatief wordt gezien voor het gebrek aan goedbetaalde banen op de arbeidsmarkt, zouden er zelfs gespecialiseerde trainingen bestaan en kunnen instructies en hackingtools veelvuldig (gewoon op de markt) worden verkregen (Walker, 2004: 6).

Een hackpoging voldoet doorgaans aan drie criteria: het is ongeoorloofd, eenvoudig maar doordacht, en het getuigt van een hoge mate van technische onderlegdheid en expertise (Turkle, aangehaald in Jordan en Taylor, 1998: 759). Er worden verschillende hackingtechnieken gebruikt om toegang te krijgen tot computers, netwerken en systemen. Dit varieert van het raden van wachtwoorden tot het uitbuiten van beveiligingslekken in software en computersystemen (NCTb, 2006b: 20). Technische hulpmiddelen die daarbij worden gebruikt zijn bijvoorbeeld *backdoors,*[93] *rootkits,*[94] spyware, keyloggers en bots (voor een uitgebreidere beschrijving verwijzen we naar Govcert, 2006: 57-58). Bots zijn programma's die ongemerkt automatisch werk kunnen uitvoeren (malware zoals wormen en Trojaanse paarden, zie paragraaf 2.4.3) en omvatten vaak een backdoor-component waardoor zij commando's kunnen ontvangen. Computers die besmet zijn met een bot ('zombie' computers) kunnen zonder medeweten van de eigenaar/gebruiker op afstand worden bestuurd (zie ook Choo, 2007). Volgens onderzoek van Sophos (aangehaald in Choo, 2007: 3) zou een schone computer zonder antivirusprogramma of firewall maar liefst 50% kans hebben om binnen een half uur na verbinding te hebben gelegd met het internet, al te zijn geïnfecteerd tot zombie. Vaak blijven zombies zogenoemde 'slapende cellen' totdat de computers externe commando's krijgen om geautomatiseerd werk uit te voeren.

Botnets

Een *botnet* is een verzameling (heel leger) van geïnfecteerde zombiecomputers. Botnets worden veelvuldig ingezet voor dDoS-aanvallen (al dan niet in combinatie met afpersing van een persoon of bedrijf), maar ze worden ook gebruikt voor phishing, spamming, identiteitsfraude via het

93 Backdoors staan voor (onderdelen van) software die ongeautoriseerd toegang tot een systeem verschaft. Deze kunnen bijvoorbeeld door een programmeur in een systeem worden gebracht zodat men zich later toegang kan verschaffen tot de software of het systeem waar het op draait met omzeiling van de bestaande beveiligingscontroles (KLPD, DNRI, 2007a).

94 Rootkits is een verzamelnaam voor kwaadaardige programma's die zich nestelen in een besturingssysteem en daar essentiële onderdelen vervangen. Het bevat meestal software om toetsaanslagen te verzamelen (keyloggers) en achteringangen in het systeem te bouwen (backdoors). Ze zijn over het algemeen moeilijk te detecteren en infecteren het systeem zonder dat de gebruiker het weet (Wikipedia, laatst geraadpleegd op 19 juli 2007: http://nl.wikipedia.org/wiki/Rootkit).

internet en verspreiding van kinderporno (Choo, 2007; McAfee, 2006: 16; Neve, 2007). Botnets worden om die reden door Molenaar (2007: 49) ook omschreven als '…*het belangrijkste middel dat cybercriminelen in handen hebben om andere activiteiten mee te ontplooien*'. Het opzetten van een botnet vereist in principe minimale technische vaardigheden (Ianelli en Hackworth, 2005: 4). Instructies zijn openlijk te vinden op het internet maar de meeste hackers zijn bovendien bereid hun informatie met andere belangstellenden te delen (via IRC worden volledige trainingen aangeboden). Botnets worden ook te huur aangeboden (V-NDB2006). Nederland staat overigens als tiende op de ranglijst van verspreiders van botnets (Molenaar, 2007). Dit zou kunnen betekenen dat Nederlandse hackers nauw betrokken zijn bij het opzetten ervan. Een belangrijke hackingzaak die de afgelopen jaren in Nederland bekendheid kreeg, betrof de zaak van de 'Tilburgse hackers'.

> De hoofdverdachte was een 20-jarige, mannelijke mbo-student uit Loon op Zand. De andere twee verdachten waren een 28-jarige man uit Rijswijk en een 23-jarige man uit Tilburg. De verdachten hadden in 2005 twee virussen geschreven en verspreid en daarmee een botnet opgezet van ruim een miljoen zombie-computers. Met het zogenoemde Toxbot-virus werd het botnet gecreëerd (met keylog-functionaliteit om toetsaanslagen vast te leggen) dat werd misbruikt om met name Amerikaanse bedrijven af te persen en op te lichten. Met het Wayphisher-virus (een Trojaans paard waarmee inloggegevens voor online bankieren werden onderschept) en door bezoekers van de internetpagina van de bank om te leiden naar een nepwebsite werden creditcard- en betaalgegevens gestolen om rekeningen mee te plunderen en luxe apparatuur te bestellen. Interessant in deze is de connectie van de hoofdverdachte met vermoedelijke Oost-Europese criminelen (de man had een bankrekening lopen in Estland). Twee verdachten werden veroordeeld tot respectievelijk twee en anderhalf jaar gevangenisstraf plus een geldboete (De Volkskrant, 25 augustus 2006; Webwereld, 14 februari 2007, 31 januari 2007, 16 januari 2007).

De Tilburgse hackers ontwikkelden dus een botnet met spyware, persten Amerikaanse bedrijven af, gebruikten nepwebsites waar betaalgegevens werden gestolen en pleegden internetfraude. Dit voorbeeld is illustratief voor de verschillende criminele markten die hackers kunnen aanboren. De gemiddelde omvang van botnets neemt recentelijk overigens af (zodat zij minder goed traceerbaar zijn voor de opsporingsdiensten) (zie Choo, 2007: 3). Er is duidelijk sprake van *diversificatie*: verschillende vormen van computercriminaliteit worden niet alleen in combinatie toegepast (hacking, botnets, spamming, malware, pharming, dDoS-aanval) maar zijn tegelijkertijd het instrument voor verschillende vormen van cybercriminaliteit (zoals internetfraude met behulp van phishing en afpersing). Er is tevens sprake van *taakspecialisatie*: criminelen maken

gebruik van experts (of zijn zelf experts die samenwerken) die zich toeleggen op specifieke ICT-deeltaken zoals het creëren van botnets en het maken van nepwebsites (Boerman en Mooij, 2006).

2.4.2 ICT-storing door gegevensverkeer

Behalve het ongeautoriseerd inbreken op ICT-systemen, kunnen computercriminelen ook opzettelijk de werking van systemen verstoren. Dit kan op twee manieren: door het massaal verzenden van gegevens (deze paragraaf), of door het manipuleren van data en gegevens (volgende paragraaf). We lichten hier specifiek twee thema's uit waarbij sprake is van overbelasting van systemen door gegevensverkeer (zie ook schema 2):
– (d)DoS-aanval;
– spamming.

(d)DoS-aanval
Een DoS aanval staat voor Denial of Service-aanval, wat zoveel betekent als het versturen van massale hoeveelheden data (digitale gegevens) naar een server, mailbox of router waardoor websites, e-maildiensten en computernetwerken overbelast raken en onbereikbaar worden. Het kan hier gaan om het versturen van massale nepverzoeken naar een website of het massaal opvragen van een website zodat de server de vraag niet aankan en onbereikbaar wordt. Bij een zogenoemde 'web sit-in' wordt door een groot aantal deelnemers herhaaldelijk informatie opgevraagd bij een website waardoor deze overbelast raakt en buiten werking raakt (Weimann, 2005). Wanneer de aanval vanaf meerdere systemen tegelijk wordt gepleegd (bijvoorbeeld door gebruik te maken van een botnet), is er sprake van een distributed DoS-aanval (of dDoS-aanval) (Govcert, 2006: 42). Een dDoS-aanval kan afkomstig zijn van een concurrent in het bedrijfsleven die de ander schade wil toebrengen, het kan een vorm zijn van politiek protest (bijvoorbeeld dierenrechtenactivisten die protesteren tegen de bonthandel), of een uiting van wraak en vandalisme (Boerman en Mooij, 2006: 30-31). MessageLabs (2005) beschrijft dat voor een protestactie chatrooms kunnen worden opgezet waarop iedereen zich gelijktijdig aanmeldt om te chatten. Voor ieder woord dat een deelnemer van die chatsite intypt wordt dan automatisch een e-mail verstuurd naar het doelwit (doorgaans een bedrijf of instelling) om zo de ICT-systemen van het slachtoffer te overbelasten en te ontregelen. De eerste beroemde dDoS-aanval in Nederland vond plaats op 22 januari 2002. Op die dag werd de geplande chatsessie van Prins Willem-Alexander en zijn toenmalige verloofde Maxima onmogelijk gemaakt door een dDoS-aanval (KLPD, DNRI, 2007b: 2).

(d)DoS-aanvallen zijn iets van de laatste jaren (KLPD, DNRI, 2007b: 3). Voor het uitvoeren van een dDoS-aanval zijn grote hoeveelheden gehackte

computers (bots) nodig die op afstand bestuurbaar zijn. Dergelijke legers aan besmette computers, ofwel botnets, zijn relatief eenvoudig verkrijgbaar via het internet[95] (NCTb, 2006b: 26). Uit onderzoek is gebleken dat Nederlandse servers in de top 10 van doelwitten van DoS-aanvallen staan[96] (Stratix, 2007). In de meeste gevallen gaat een aanval gepaard met een poging tot afpersing (zie paragraaf 2.3.3: afpersing en chantage). Criminelen kiezen als doelwit vaak (e-commerce-)bedrijven en instellingen die voor de bedrijfsvoering sterk afhankelijk zijn van het internet (bijvoorbeeld online goksites). Meestal wordt een persoon of organisatie gedwongen geld of goederen te betalen om te voorkomen dat de aanval wordt uitgevoerd (afkoopsommen tussen de 10 en 60.000 dollar zijn geen uitzondering) (Boerman en Mooij, 2006: 30-31; MessageLabs, 2005: 3). Hoewel het aantal dDoS-aanvallen wereldwijd flink is toegenomen en de mogelijkheden in de toekomst verder zullen toenemen (door de uitbreiding in het aantal breedbandverbindingen en dus potentiële doelwitten), verwacht het KLPD in Nederland geen concrete dreiging op dit vlak (Boerman en Mooij, 2006: 34). Als reden wordt aangevoerd dat het huidige aantal afpersingspogingen met behulp van dDoS-aanvallen in Nederland (ten opzichte van bijvoorbeeld de Verenigde Staten en het Verenigd Koninkrijk) erg gering is, en bovendien worden de technologische ontwikkelingen die tegen dDoS-aanvallen kunnen beschermen steeds geavanceerder geacht.

Spamming

Spamming is het massaal verzenden van ongewenste e-mail van commerciële, ideële of charitieve aard zonder voorafgaande toestemming van de ontvanger. De inhoud van spam kan variëren van reclame (voor bijvoorbeeld medicijnen, aandelen of goederen) tot het verzoek een financiële bijdrage te leveren (de Nigeriaanse bedelbrieven). Het massale bereik is volgens Mons (aangehaald in Spits, 13 maart 2007) de kracht van spam als marketinginstrument: '*…Als er per duizend spammails slechts één product zou worden verkocht, dan kun je nagaan dat de winst bij een miljard spammails zeer interessant wordt*'. Spam wordt om diezelfde reden steeds vaker ingezet als phishing-instrument om mensen informatie te ontlokken om hen daarmee vervolgens te kunnen oplichten[97] (zie paragraaf 2.3.3: internetfraude) (De Volkskrant, 25 augustus 2006; McAfee, aangehaald in Choo, 2007: 4). Spamming gericht aan natuurlijke personen (niet aan bedrijven) is in Nederland volgens de Telecommunicatiewet verboden.[98] Hoewel spam meestal niet direct gericht is op het verstoren van de werking van ICT als zodanig, kan het door de massaliteit ervan wel dat gevolg

95 Een prijsindicatie van 250 dollar wordt gegeven voor het huren van 5.000 'voorgeïnfecteerde' machines (NCTb, 2007: 26), maar dit kan oplopen tot maar liefst 50.000 dollar (Ianelli en Hackworth, 2005: 7).
96 In de eerste helft van 2006 ging het om 6.110 aanvallen per dag (Stratix, 2007: 4, 22).
97 Oplichting per e-mail zoals de Nigeriaanse scams wordt door Govcert dan ook als spam gerekend.
98 De Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA) is in Nederland belast met de naleving op het verbod (zie Molenaar, 2007).

hebben. Schattingen van de omvang variëren: tussen de 40% en 90% van alle e-mail die wij ontvangen bestaat uit spam (Govcert, 2006; Symantec, aangehaald in Choo, 2007: 3; MessageLabs, 2005). Govcert (2006) verwacht dat dit in 2007 met nog eens 63% zal toenemen.

2.4.3 ICT-storing door manipulatie van data en systemen

Behalve door het massaal versturen van gegevens, kan de werking van ICT ook worden verstoord door daadwerkelijke manipulatie van digitale data-gegevens en systemen. Bij manipulatie van *data* worden geautomatiseerd opgeslagen gegevens bijvoorbeeld opzettelijk beschadigd, verwijderd, gewijzigd en/of vernietigd (dan wel wordt hiermee gedreigd). Bij manipulatie van *systemen* worden opzettelijk storingen veroorzaakt in de besturing van de systemen (bijvoorbeeld aanvallen op informatiesystemen die zorgen voor de aansturing van vitale infrastructuren). In dit rapport worden specifiek de volgende subthema's nader toegelicht (zie ook schema 2):
– malware in systemen (virussen, wormen, Trojaanse paarden);
– defacing (pharming);
– (h)acktivisme;
– cyberterrorisme (vitale infrastructuren).

Malware in systemen (virussen, wormen, Trojaanse paarden)
Malware (afkorting van 'malicious software') is het bulkbegrip voor computerprogramma's die zonder toestemming van de eigenaar of beheerder draaien op een computer en het systeem iets laten doen naar de wens van een buitenstaander (KLPD, DNRI, 2007a: 15). Computers kunnen op uiteenlopende manieren worden besmet met malware, bijvoorbeeld via het openen van e-mailberichten of bijlagen, door bezoek aan websites, en door het klikken op advertenties of het downloaden van (gratis) software (KLPD, DNRI, 2007a: 16-17). De OPTA (Nederlandse toezichthouder op de post- en telecommunicatie) onderscheidt vier vormen van schadelijke software (of malware):
– spyware, ofwel software waarmee gevoelige informatie (bijvoorbeeld bankgegevens) van het doelwit wordt verzameld;
– *adware*, ofwel software die zonder toestemming op de computer van het doelwit wordt geïnstalleerd en daar ongewenst advertenties rondzaait;
– traditionele *virussen*[99] die schade aan het computersysteem aanrichten;
– moderne virussen (*Trojaanse paarden*)[100] waarmee de controle over een computer wordt overgedragen aan derden (Govcert, 2007: 13)

99 Wormen en virussen zijn stukjes code. Een worm is een programma met een reeks instructies dat zichzelf vermenigvuldigt en verspreidt. Een virus is een programma met een reeks instructies dat zichzelf vermenigvuldigt en zich verspreidt door zich te bevestigen aan bestanden of programma's. Er zijn ook polymorfische wormen en virussen die zichzelf aanpassen en voortdurend veranderen om detectie te voorkomen (Govcert, 2006: 53-58; KLPD, DNRI, 2007a: 15).

100 Trojaanse paarden zijn ogenschijnlijk ongevaarlijke en nuttige programma's die onopgemerkt op een computer draaien en vaak ongewenste (kwaadaardige) acties uitvoeren, vaak met behulp van zogenoemde backdoors, rootkits, keyloggers, spyware en bots. Door Trojaanse paarden is het dus mogelijk dat computers worden besmet en vervolgens op afstand bestuurd kunnen worden. Ze worden meestal verspreid via wormen en virussen (Govcert, 2006: 53-58; KLPD, DNRI, 2007a: 15).

Tegenwoordig worden virussen en Trojaanse paarden door hackers/crackers op maat gemaakt (tegen forse betaling) met als specifiek doel het aanleggen van botnets die vervolgens te huur zijn voor spammers of criminele organisaties (MessageLabs, 2005).

Defacing (pharming)
Er is sprake van defacing wanneer een website zonder toestemming wordt veranderd, vervangen, vernield of wanneer bezoekers van een website zonder het te weten automatisch worden doorgeleid naar een andere (nep)website. Het doorgeleiden naar een nepwebsite wordt ook wel pharming genoemd (Govcert, 2006: 35). Uit interviews met deskundigen komt naar voren dat *defacing*, net als dDoS-aanvallen, als middel wordt ingezet voor afpersing (vooral e-commerce-bedrijven kunnen omzetverliezen vermijden door het betalen van een afkoopsom aan de afpersers). Internetgebruikers die als gevolg van *pharming* ten onrechte in de veronderstelling zijn met een originele website te maken te hebben, kunnen vertrouwelijke gegevens uitwisselen met de omgeleide nepwebsite (zoals wachtwoorden en creditcardgegevens). Voor criminelen is het niet moeilijk om met de onderschepte gegevens internetfraude te plegen (zie paragraaf 2.3.3).

(H)acktivisme
Massale fysieke deelname aan demonstraties is door het gebruik van ICT minder noodzakelijk geworden. Ook zonder een grote organisatie of demonstratie is het mogelijk om toch een stem te laten horen aan miljoenen anderen door bijvoorbeeld gebruik te maken van internet (NRC Handelsblad, 29 januari 1999). Hacktivisme staat voor het hacken van computersystemen uit vaak politiek gemotiveerde, activistische overwegingen en de betrokken activisten worden dan ook wel aangeduid als 'hacktivisten'. Het protest kan zich uiten door bijvoorbeeld websites te blokkeren (met behulp van dDoS-aanvallen). Zo waren de Deense overheidssites een tijdje onbereikbaar nadat in de media spotprenten waren gepubliceerd van de profeet Mohammed (NCTb, 2006: 12). Op verschillende nieuwsforums zouden gedetailleerde instructies zijn verschenen hoe een dDoS-aanval moest worden uitgevoerd. In mei 2007 waren ook de overheidssites in Estland gedurende enkele dagen onbereikbaar vanuit het buitenland als gevolg van massale dDoS-aanvallen. Dit gebeurde vlak nadat Estland besloot om een oorlogsmonument uit de Sovjettijd te verplaatsen van het centrum van Tallinn naar een buitenwijk.[101]

101 Hoewel een Estse student werd gearresteerd die op internetfora instructies had geplaatst om overheidssites aan te vallen, bestaan er vermoedens bij de Estlandse autoriteiten dat de Russen achter de aanval zitten (Security.nl 18 mei 2007; Tweakers.net 14 mei 2007).

Ook kunnen hacktivisten uit protest websites veranderen en er politiek getinte boodschappen achterlaten (defacing). Jaren geleden was China hiervan doelwit toen de mensenrechtensite van de Chinese regering en de Chinese website met censuurvoorschriften werden veranderd en/of verwijderd. Recent staan dergelijke protestacties vaak in het teken van de problematiek in het Midden-Oosten en worden veel Israëlische websites gehackt (NCTb, 2006b: 36, 74-75; NRC Handelsblad, 25 augustus 2006). Onlangs nog werd de officiële website van de Verenigde Naties gehackt als actie tegen het Amerikaanse en Israëlische beleid in het Midden-Oosten. Op de site waar normaal gesproken recente toespraken van de VN-secretaris-generaal staan weergegeven, was een korte boodschap te lezen: '*Hey Israël en VS, hou op met kinderen en andere mensen te doden. Eeuwige vrede. Geen oorlog*' (12 augustus 2007).

Behalve het blokkeren en wijzigen van websites kunnen hacktivisten ook massale e-mail (e-mailbommen) versturen waarmee systemen worden overbelast of politieke statements doen met behulp van een zogenoemde *Google-bom* (Europol, 2003: 42, 52-53; NCTb, 2006b: 36). Dit is een poging om het zoekresultaat van Google te beïnvloeden door een bepaalde pagina hoog op de resultatenlijst van een zoekopdracht te laten verschijnen. Zo werd de website van Bush jr. bijvoorbeeld het eerste zoekresultaat als men zocht op de termen 'miserable' en 'failure' (NCTb, 2007: 74-75).

Cyberterrorisme (vitale infrastructuren)
Ook terroristen kunnen door middel van dDoS-aanvallen de computersystemen die websites en andere voorzieningen aansturen overbelasten en ontwrichten (NCTb, 2006b: 19-20). Alleen ingeval het systemen betreft van vitale infrastructuren spreken we in dit rapport van cyberterrorisme. Vitale infrastructuren zijn systemen die zo vitaal zijn voor een land dat de ontregeling of vernietiging ervan een ontwrichtend effect zou hebben op de nationale veiligheid, economische zekerheid, volksgezondheid of veiligheid. Te denken valt aan de overname van besturingssystemen van het lucht- en spoorwegverkeer, van militair-strategische systemen in de ruimte, van vitale installaties in de chemische sector, van de farmaceutische industrie, of energiecentrales. Deze industriële processen worden door het Supervisory Control and Data Acquisition (SCADA-)systeem aangestuurd en gecontroleerd, en zijn ontworpen om op afstand bediend te worden (NTCb, 2006: 26). Ook kunnen aanvallen gericht zijn op het internet zodat communicatie- en transportsystemen, crisis-, informatie-, of virtuele diensten als internetbankieren worden platgelegd[102] (zie Benschop, 2007; NCTb, 2007: 7; NHTCC, 2006b: 20; Weimann, 2005) of

102 Ook het wijzigen van de samenstelling van producten in de voedingsindustrie (Benschop, 2007) of het wijzigen van patiëntengegevens in ziekenhuizen (zoals bloedgroepen of medicaties) kunnen dramatische gevolgen hebben (NCTb, 2007: 36).

kunnen aanslagen op fysieke doelen worden gepleegd via het internet (om rampen te veroorzaken dan wel te versterken).

Bij cyberterrorisme gaat het hoe dan ook om politiek gemotiveerde aanvallen tegen gegevens, informatiesystemen en computerprogramma's (ICT) die resulteren in grootschalige maatschappelijke ontwrichting, angst, geweld en terreur tegen niet-strijdende doelwitten (Europol, 2003: 42; Weimann, 2005; Stohl, 2006).

In bijlage 5 staan al verschillende argumenten opgesomd waarom het internet voor terroristen een belangrijk instrument is. In aanvulling daarop zijn er diverse redenen waarom het aanvallen van vitale infrastructuren een aantrekkelijke optie is voor terroristen (NCTb, 2006a: 16; Weimann, 2005):
- het kan op afstand worden gepleegd (tijd, locatie en omstandigheden worden zelf bepaald);
- het brengt voor de dader minder risico met zich mee op dodelijke afloop;
- het is laagdrempelig (minder fysieke training en psychologische investering vereist);
- het kan grote economische schade aanrichten;
- het gaat gepaard met veel media-aandacht.

Tegenargumenten waarom het internet geen aantrekkelijk doelwit vormt zijn er ook (NCTb, 2006a: 18). Zo zijn bijvoorbeeld de effecten relatief onvoorspelbaar, levert het geen spectaculaire beelden op en zijn terroristen zelf juist afhankelijk van een goed functionerend internet. Bovendien, stelt Weimann (2005), staan belangrijke vitale infrastructuren niet fysiek met het internet in verbinding en kunnen daardoor niet door hackers van buitenaf worden gekraakt. Al zijn er indicaties dat jihadisten belangstelling hebben voor dit type aanslagen[103] (Clarke, 2003; NCTb, 2006b: 37, 44; Weimann, 2005), concrete pogingen tot dergelijke acties zijn tot op heden ook nog niet geconstateerd (Goodman e.a., 2007),

Voormalig directeur van de National Infrastructure Protection Center van de FBI, Ron Dick (aangehaald door Clarke, internetpublicatie 2003), ziet de terreurdreiging van cyberterrorisme als reëel maar niet erg waarschijnlijk: '*…Because it doesn't have the impact that they're looking for. Most terrorist organizations want to have visuals, if you will, for the media, of loss of life and destruction of various buildings and so forth. If you have an attack in cyberspace, you're not going to have those kinds of visuals that terrorist*

103 Het is vooralsnog onbekend in hoeverre terroristen door middel van hacking (via infiltratie, op grond van eigen expertise of het inhuren ervan) informatie bemachtigen die kan worden ingezet voor de jihad, al wordt dit door de NCTb (2007: 78) wel waarschijnlijk geacht. Wel zijn er aanwijzingen van betrokkenheid van hackergroepen in de wereldwijde *jihad* (NCTb, 2007: 21).

organizations are looking for… What does keep me awake at night is that if they use visuals in conjunction with a cyber attack, it can dramatically compound the impact of that.' Dit is het geval wanneer fysieke aanvallen worden gecombineerd met een cyberaanval waardoor bijvoorbeeld crisisresponsdiensten niet in actie zouden kunnen komen. Volgens Weimann (2005) zijn het vooral wraakzuchtige insiders die een gevaar vormen voor de vitale infrastructuren: (ex-)medewerkers die bijvoorbeeld werkzaam zijn (of waren) bij en voor SCADA-systemen. Deze mensen beschikken over de specifieke technische kennis en vaardigheden om cyberaanslagen te plegen.

> In 2005 werd in Amerika het bedrijf van de 43-jarige Sylvestre (een systeembeheerder van de Amerikaanse marine) gepasseerd voor een contract. Uit wrok programmeerde de man ondeugdelijke commando's in de besturingssystemen van het computernetwerk van de United States Navy European Planning and Operations Command Center (NEPOCC) waarmee locaties en bewegingen van schepen en onderzeeboten gevolgd werden. Het was de bedoeling dat deze op tilt zouden slaan en dat de nieuw aangenomen systeembeheerder (werkzaam voor de concurrent van het bedrijf van Sylvestre) de (mogelijk fatale) computerstoring in de schoenen zou worden geschoven. Het plan werd voortijdig ontdekt waardoor catastrofale gevolgen uitbleven.

In de Nederlandse studie van Van der Werf (2004) waren de geïnterviewden het met elkaar oneens over de mate waarin er risico's bestaan op cyberterroristische aanslagen. Sommigen wezen erop dat het aansluiten van bepaalde diensten op internet het risico met zich meebrengt dat hackers zich er toegang toe verschaffen. Voor Nederland wordt het risico op een cyberterroristische aanval vooralsnog niet waarschijnlijk geacht (NCTb, 2006a). Overigens stelt het NCTb (2007: 40) wel vast dat 'social engineering', waarbij vertrouwelijke informatie onder valse voorwendselen wordt verkregen om bijvoorbeeld toegang te krijgen tot een systeem, een belangrijk middel in de voorbereiding van een cyberaanval kan zijn. Uit een oefening van de nationale veiligheidsdienst van de Verenigde Staten (NSA), in 1997, bleek dat de veiligheidssystemen van het Pentagon te kraken waren met behulp van vrij beschikbare (!) software op het internet. Hackers (die zich voordeden als IT-medewerker of hooggeplaatste functionaris binnen de organisatie) was het gelukt om medewerkers van het Pentagon over te halen om logincodes vrij te geven (Weimann, 2005).

2.4.4 ICT-dienstverleners van high-tech crime

Voorbereidingshandelingen voor high-tech crime (zoals hacking, dDoS-aanvallen, virusverspreiding en het aftappen van communicatie) is in Nederland strafbaar gesteld binnen de Wet op de Computercriminaliteit.

Het gaat bijvoorbeeld om het vervaardigen, verkopen, verwerven, invoeren, verspreiden (of het anderszins ter beschikking stellen of voorhanden hebben) van een technisch hulpmiddel, wachtwoorden of toegangscodes waardoor toegang kan worden verkregen tot een geautomatiseerd werk. In dit rapport definiëren wij ICT-dienstverleners als personen die *opzettelijk* deze middelen en technieken vervaardigen, beschikbaar stellen en verspreiden ter facilitering van high-tech crime. Meer specifiek besteden we in dit rapport aandacht aan (zie ook schema 2):
– corrupte (ex-)medewerkers;
– infiltratie van criminele ICT'ers;
– het inhuren van ICT-experts door criminele en terroristische organisaties (zie ook hoofdstuk 4).

Corruptie
Er is sprake van corruptie als ICT-werknemers '*…hand- en spandiensten verrichten ten behoeve van zware of georganiseerde criminaliteit waarbij grensoverschrijdende illegale activiteiten worden mogelijk gemaakt of vergemakkelijkt*' (KLPD, DNRI, 2004: 100) of als zij '*…misbruik maken van bevoegdheden, ten faveure van een derde partij, teneinde persoonlijk voordeel te behalen in de vorm van financiële of andersoortige gunsten*' (Boerman en Mooij, 2006: 49). Mede gezien het feit dat relatief veel ICT-personeel door bedrijven veelal extern wordt ingehuurd, is het de verwachting dat criminele netwerken zich in toenemende mate via corruptie (dus met hulp van binnenuit) een weg proberen te banen naar digitale informatie (Fox-IT, 29 januari 2004; NDB2004: 100). ICT-werknemers die kunnen worden omgekocht of bedreigd, zijn vooral personen die een hoger niveau aan ICT-bevoegdheden hebben dan de gemiddelde eindgebruiker (zoals programmeurs, systeem- en gegevensbeheerders), maar ook personeelsleden die toegang hebben tot gevoelige bedrijfsgegevens (bijvoorbeeld met betrekking tot opsporings- of defensiesystemen, of gegevens van klanten, producten en betalingen) (KLPD, DNRI, 2007c: 1). In Nederland zijn geen concrete gevallen bekend van corrupt ICT-personeel (KLPD, DNRI, 2007c: 5-7) en in de V-NDB2006 (Boerman en Mooij, 2006: 51) werd dit dan ook niet als concrete dreiging gekwalificeerd voor de Nederlandse samenleving.[104]

Infiltratie
Relatief veel bedrijven en organisaties huren tegenwoordig ICT-professionals en consultants in om ICT-systemen te bouwen, te testen en te ontwikkelen én voor het ontwikkelen van software. Dit vormt niet alleen een groot afbreukrisico voor het bedrijf (de kennis van vitale bedrijfssystemen geeft men als het ware 'uit handen') maar ook een groot veiligheidsrisico wanneer criminelen zich als ICT-consultant op de markt gaan aanbieden

104 Volgens Europol (2003: 80–81, 115) zijn de financiële gevolgen van ongeautoriseerde toegang van buitenaf (hacking) de afgelopen jaren sterk gestegen en vormt dit een grotere dreiging dan corruptie.

(bijvoorbeeld als zelfstandig ondernemer). Zo slaagde bijvoorbeeld de Japanse Aum Shinri Kyo-sekte[105] erin de opdracht te verwerven voor het ontwikkelen van software voor defensie en politie waardoor ze potentiële toegang kregen tot geclassificeerde informatie van overheids- en defensiesystemen.[106] De sekte bleek wereldwijd over een 'intelligence-tak' te beschikken van meer dan 40.000 leden die zich door middel van hacking bezighield met het stelen van staats-, bedrijfs- en onderzoeksgeheimen (Europol, 2003: 80; Weimann, 2005). Door als toeleverancier of onderaannemer van andere bedrijven te werken, bleef de betrokkenheid van de sekte lang buiten schot (Weimann, 2005). Buitenlandse bronnen (onder andere het Serious Organised Crime Agency [SOCA][107] uit het Verenigd Koninkrijk) waarschuwen voor met name Russische maffiabendes die hun leden in toenemende mate laten infiltreren in bedrijven (aangehaald in ZDNet.com, 25 april 2006). Motieven kunnen variëren van het plegen van fraude, diefstal en chantage tot het gebruiken van geheime informatie voor het plegen van aanvallen op systemen of spionage.

Inhuur expertise

Door de toegenomen beveiliging van bedrijfsnetwerken wordt het steeds moeilijker om toegang tot informatie te krijgen van buitenaf. Georganiseerde criminele en terroristische netwerken kunnen, bij gebrek aan de nodige technische expertise en vaardigheden, de kennis inhuren van experts (hackers/crackers). Zo zou de Provisional IRA ten behoeve van de voorbereiding van aanslagen hackers hebben ingehuurd om in te breken op computers waarin gegevens over politie- en justitiemedewerkers opgeslagen waren (Benschop, 2006). Indicaties zijn er ook dat terroristische stromingen gebruikmaken van ICT-experts: een 22-jarige Marokkaanse Londenaar, bekend als 'Irhabi 007', verleende hand- en spandiensten voor een aantal terroristen onder meer door het plaatsen van videomateriaal (propaganda) op gehackte websites (Kohlmann, 2006). Hoewel de computerkennis en -vaardigheden van terroristische groeperingen (in het bijzonder van jihadisten) als actueel moet worden beschouwd en in expertise toeneemt, is het mogelijk dat ook zij hackingdeskundigheid inhuren (NCTb, 2006a: 9, 11). Vooral in de voormalige Sovjet-Unie en India zijn op het moment hoogopgeleide ICT-specialisten die in eigen land niet of moeilijk aan betaald werk kunnen komen. De opbrengsten van hacking zijn bovendien dusdanig uitnodigend dat ook West-Europese experts (vooral jongeren) de georganiseerde misdaad kunnen worden ingezogen door hun diensten aan te bieden aan criminelen (zie paragraaf 2.4.1).

105 Deze sekte was verantwoordelijk voor de gifgasaanslag op de metro van Tokyo in 1995.
106 De sekte ontwikkelde software voor 80 Japanse organisaties en 10 overheidsinstellingen (Weimann, 2005).
107 Waaronder ook de National Hi-Tech Crime Unit ressorteert.

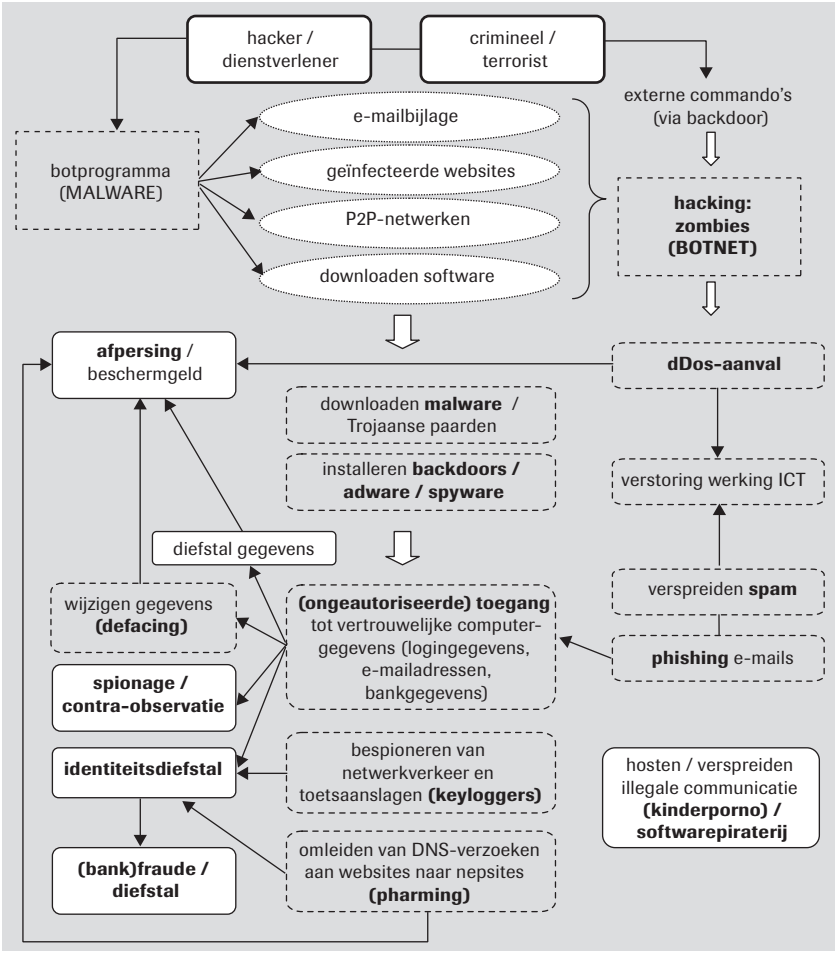
2.5 Trend naar diversificatie en taakspecialisatie

In paragraaf 2.4.1 werd al gesproken van een belangrijke trend in high-tech crime, namelijk die van diversificatie en taakspecialisatie. Er is sprake van een complex en breed scala aan criminele activiteiten waarbinnen verschillende varianten van cyber- en computercriminaliteit gecombineerd worden toegepast en in elkaar overlopen. De complexe verwevenheid tussen cyber- en computercriminaliteit blijkt vooral wanneer de multifunctionaliteit van bijvoorbeeld malware en botnets nader wordt beschouwd. In schema 3 is af te lezen dat malware (onder andere verspreid via het openen van e-mailbijlagen, het bezoeken van geïnfecteerde websites, of het downloaden van software) gebruikt wordt om botnets te creëren, ongeautoriseerde toegang tot systemen te verkrijgen (hacking), en gegevensverkeer te bespioneren (keylogging) dan wel te manipuleren (pharming). Via botnets kunnen zombiecomputers op afstand worden bestuurd door mensen met expliciete criminele en/of terroristische bedoelingen.

Een *botnet* faciliteert zowel andere vormen van computercriminaliteit (bijvoorbeeld dDoS-aanvallen, spamming en phishing) als diverse varianten van cybercriminaliteit (zoals het verspreiden van illegale communicatie, softwarepiraterij en afpersing). De gehackte, bespioneerde of omgeleide, gemanipuleerde systemen (die tot stand komen door de inzet van *malware*) maken het op hun beurt ook mogelijk om allerlei varianten van cybercriminaliteit te plegen (zoals afpersing, defacing, spionage, identiteitsdiefstal en fraude). Daarnaast faciliteren verschijningsvormen van cybercriminaliteit ook weer andere vormen van cybercriminaliteit (defacing wordt bijvoorbeeld ingezet voor afpersing, en identiteitsdiefstal wordt gebruikt voor het plegen van fraude).

Dit is slechts een illustratie van de complexiteit in het identificeren en onderscheiden van verschillende soorten high-tech crime. Er is sprake van een grote verwevenheid tussen de verschijningsvormen van high-tech crime in het algemeen, en tussen computercriminaliteit (de grijze vakken met onderbroken omlijning in schema 3) en cybercriminaliteit (de witte vakken met doorlopende omlijning in schema 3) in het bijzonder. Een beperkt aantal technieken en instrumenten kunnen voor een breed veld

Schema 3 Overlap tussen technieken en verschijningsvormen van high-tech crime



aan criminele activiteiten worden ingezet (diversificatie). Opvallend is dat met name malware en botnets (taakspecialisatie) door hun multifunctionaliteit in grote mate bepalend zijn voor de criminele markt van high-tech crime. Niet voor niets worden malware en botnets dan ook in toenemende mate aangeboden (op maat gemaakt, verhuurd en/of verkocht) (Choo, 2007). Door de Europese Commissie (22 mei 2007a) worden botnets als grootste dreiging gezien van de laatste tijd voor het plegen van aanvallen tegen informatiesystemen of organisaties en individuen.

2.6 Prioriteiten: een verdieping van thema's

Samenvattend kunnen we concluderen dat high-tech crime een grote diversiteit aan verschijningsvormen kent. Strevend naar overzicht en consistentie hebben wij in dit hoofdstuk een indeling gemaakt naar verschillende subthema's van cyber- en computercriminaliteit (de twee 'hoofdvarianten' van high-tech crime) waarbinnen diverse verschijningsvormen de revue zijn gepasseerd. Deze indeling dient als leidraad in het rapport voor het in kaart brengen van daderkenmerken zoals dat in hoofdstuk 3 aan de orde komt. Uit de grote variëteit aan verschijningsvormen van high-tech crime hebben we een selectie gemaakt van criminele activiteiten die in termen van dreiging en risico's[108] voor de Nederlandse samenleving prioriteit verdienen op de onderzoeksagenda. Bij deze prioritering is in termen van effecten een weging gemaakt van zowel de ernst als de waarschijnlijkheid van deze dreigingen[109] (zie ook NHTCC/NPAC, 2006a: 17; OM, 2004). Deze evaluatie is onder meer gebaseerd op (inter)nationale literatuur (Taylor e.a., 2006: 360), bestaande dreigingsinschattingen (Europol, 2003 en 2007b; Interpol, 2007; NDB2004; SOCA; Stratix, 2007; V-NDB2006; Van der Werf, 2003), speerpunten in de opsporing van de georganiseerde misdaad en in het veiligheidsprogramma van de Nederlandse overheid voor de periode tot 2010[110] (OM, 2007b; TK 2005-2006, 28 684, nr. 85; TK 2005-2006, 29 911, nr. 4; TK 2006-2007, 30 800 hoofdstuk VI, nr. 2), en de richtlijnen ter bestrijding van high-tech crime zoals onlangs door de Europese Commissie (22 mei 2007a) werd geformuleerd.[111]

Dit heeft geresulteerd in een aantal verschijningsvormen van high-tech crime waarvan kennis over daders als essentieel moet worden beschouwd in de bestrijding ervan. Een overzicht van thema's is weergegeven in schema 4 (zie voor een indeling naar clusters ook schema 2).

108 Het betreft (in volgorde van belangrijkheid) overwegingen met betrekking tot (1) levensbedreiging en bedreiging van de democratische rechtsorde, (2) maatschappelijke onrust en ontwrichting, (3) continuïteit in de bedrijfsvoering en (4) financieel-economische schade.

109 Omdat er nauwelijks sprake is van illegale drugshandel via het internet is dat thema hier bijvoorbeeld niet als prioriteit aangemerkt, ookal staat drugshandel als prioriteit op de Nederlandse veiligheidsagenda.

110 Speerpunten van de Nationale Recherche (ter bestrijding van georganiseerde misdaad) zijn: (a) terrorisme en ideologisch gemotiveerde misdaad, (b) illegale handel in harddrugs (cocaïne en heroïne), (c) productie en handel in synthetische drugs (XTC), (d) mensenhandel- en smokkel, (e) handel in vuurwapens en explosieven, en (f) witwassen. Buitenlandse bronnen zoals het SOCA (aangehaald in ZDNet.com, 25 april 2006) en het OCTA-rapport (Europol, 2007b) noemen ook (g) dienstverleners (zoals hackers en corrupte IT-experts) en (h) zelfstandigen (high-tech criminelen die legale bedrijven opzetten) als dreiging. Aanvullende speerpunten van het Nederlandse overheidsbeleid zijn: (i) radicalisering en extremisme, (j) discriminatie en racisme, (k) vitale infrastructuren, (l) fraude en corruptie, (m) nieuwe technologie en (n) cybercriminaliteit.

111 De volgende thema's werden expliciet benoemd: (a) illegale handel (bijvoorbeeld de handel in drugs, vuurwapens en explosieven, softwarepiraterij en mensenhandel), (b) terrorisme en ideologisch gemotiveerde misdaad, (c) kinderporno, (d) internetfraude, (e) identiteitsfraude met behulp van phishing, (f) grooming, (g) cyberterrorisme / vitale infrastructuren en (h) botnets.

Schema 4 Geprioriteerde thema's van high-tech crime

Cybercriminaliteit
- radicalisering
- terrorisme en ideologisch gemotiveerde misdaad
- kinderporno
- grooming
- softwarepiraterij
- internetfraude (waaronder identiteitsfraude met behulp van phishing)
- witwassen (e-commerce en virtuele casino's)

Computercriminaliteit
- cyberterrorisme
- ICT-dienstverleners (hacking/botnets/malware)

Gezien de reële dreiging die uitgaat van radicalisering en terrorisme staan beide thema's hoog op de veiligheidsagenda. Kinderporno en grooming worden gezien als de meest ernstige maatschappelijke delicten (zie ook Stol, 2001), al heeft dit veeleer te maken met de reactie daarop vanuit de samenleving[112] dan om de maatschappelijke ontwrichting van de delicten zelf. Softwarepiraterij heeft verreikende financieel-economische consequenties, hoewel het door delen van de samenleving als vanzelfsprekend wordt ervaren. Daarnaast zullen internetfraude en witwassen in toenemende mate aandacht vereisen in onze samenleving, onder meer door de toename van zowel de e-commerce, het aantal internetgebruikers, het toenemende gebruik van creditcards, en de steeds grotere hoeveelheid persoonlijke informatie die beschikbaar is op het internet. Identiteitsfraude met behulp van phishing is bovendien een van de prioriteiten omdat het een faciliterende, instrumentele functie heeft voor uiteenlopende criminele hoofdactiviteiten (zie ook Europese Commissie, 22 mei 2007b en Europol, 2007b: 17).

Ten aanzien van computercriminaliteit is in de voorgaande paragraaf het belang van taakgespecialiseerde expertise naar voren gekomen. Zonder deze expertise zullen veel vormen van high-tech crime ernstig gemankeerd raken. Ten behoeve van de bestrijding van high-tech crime speelt de rol van 'ICT-dienstverleners' (die bijvoorbeeld hun technische kennis en vaardigheden verhuren binnen het criminele circuit) een algemeen en belangrijk aandachtspunt (niet alleen preventief gezien maar ook met betrekking tot de opsporing). Met name de multifunctionele varianten van computercriminaliteit in relatie tot georganiseerde misdaad, zoals

112 Uit onderzoek van Intomart GfK blijkt bijvoorbeeld dat kindermisbruik via chatboxen door 35% van de Nederlanders wordt genoemd als topprioriteit voor de criminaliteitsbestrijding (Cops, 2007l).

de makers van botnets en malware (zie ook schema 3), verdienen nader onderzoek. Tot slot is cyberterrorisme ondanks de geringe dreigingsinschatting in de lijst van prioriteiten opgenomen omdat de gevolgen ervan in potentie grote maatschappelijke schade en ontwrichting kunnen aanrichten. In het volgende hoofdstuk evalueren we de stand van zaken in de literatuur met betrekking tot de kennis over daders van de geprioriteerde thema's van high-tech crime. Voor een inventarisatie van kennis over daders van de niet-geprioriteerde thema's verwijzen we naar bijlage 6.

3 Kenmerken van daders

3.1 Daderprofielen in high-tech crime?

Hoewel onderzoek naar high-tech crime nog in de kinderschoenen staat, kan worden vastgesteld dat een van de belangrijkste lacunes van dit moment het gebrek is aan kennis over daders (Broadhurst, 2005; Rogers, 2000, 2001, 2006). Bij vele vormen van high-tech crime bestaat een beeld van de manier waarop de delicten worden gepleegd, maar slechts bij een klein deel, waarin daadwerkelijk daders gearresteerd zijn (zoals in het geval van Nigeriaanse fraude) bestaat enig inzicht in hun kenmerken (Neve, 2007). Voor het bestrijden van high-tech crime (preventie, opsporing, vervolging) is daarom niet alleen technische controle en beveiliging nodig op systemen maar juist ook inzicht in daders en hun kenmerken (Nykodym e.a., 2005; Rogers, 2006: 97).

Het systematisch in kaart brengen van daderkenmerken in de vorm van risico-indicatoren wordt ook wel '*profiling*' genoemd. Denk bijvoorbeeld aan sociaal-demografische kenmerken (geslacht, leeftijd), kennis en vaardigheden waarover de dader beschikt (IT-kennis, specialistisch of generalistisch), motivatie en bijzondere gedragskenmerken (gewoonten, psychologisch profiel). De idee is dat naarmate een (verdacht) persoon of een groep personen meer voldoet aan het prototype daderprofiel van een bepaald delict, hoe groter de kans of het risico dat deze persoon (of groep) het delict heeft gepleegd of nog zal gaan plegen in de toekomst (Shaw, 2006).

Het opstellen van dader- of risicoprofielen is niet nieuw. Profiling is vooral bekend en wordt toegepast binnen opsporingsonderzoeken van zedendelicten (verkrachting) en moordzaken. Aan de hand van een gedragsmatige reconstructie van het delict wordt een profiel opgesteld van de persoonlijkheid en mogelijke motieven van de dader. Zo wordt getracht een relatie te leggen tussen kenmerken van het delict en dat van de dader(s). Hierbij worden zowel wetenschappelijke theorieën en inzichten gebruikt als ervaringen uit de politiepraktijk. De informatie die voortkomt uit eerder opgeloste, vergelijkbare zaken vormt een soort 'intelligence base', vooral wanneer daaruit (a)typische patronen zijn af te leiden.[113] Bekende methoden voor het ontwikkelen van daderprofielen zijn de 'crime scene analysis' van de FBI en het 'five-factor model' van David Canter (zie ook Douglas e.a., 1986; Petherick, 2007).

Dergelijke profielen, die zowel naar individuele personen als naar groepen te herleiden zijn (zie ook Fidis, 2005: 52), kunnen ook aan de hand van

113 Datamining (een techniek waarmee op geautomatiseerde wijze afwijkende patronen kunnen worden ontdekt in grote hoeveelheden digitale informatie) zal in de toekomst binnen de opsporing steeds belangrijker worden voor het ontwikkelen van risicoprofielen (Fidis, 2005: 30, 43).

online activiteiten (websurfen, chatboxen, transacties) en andere digitale gedragskenmerken (bijvoorbeeld het gebruik van nicknames, wachtwoorden, persoonlijke websites, manier van toegang tot het internet, wijze van toenadering tot het slachtoffer) worden gereconstrueerd voor high-tech crime. Zo kiezen gebruikers bijvoorbeeld vaak wachtwoorden die te maken hebben met hun persoonlijke interesse of hobby's (NIJ, 2007: 43) en kunnen mensen het internet op vanuit publieke gelegenheden (zoals internetcafés) of vanuit huis (Casey, 2002). Al dit soort kenmerken kunnen iets vertellen over de achtergrond van de daders (bijvoorbeeld sekse), hun zelfbeeld, interesses, gewoonten, technische vaardigheden en dergelijke. Voor de meer technische aspecten en werkwijzen van de verschillende verschijningsvormen van high-tech crime verwijzen wij naar een speciale rapportage over de sporen en opsporingsmethoden van high-tech crime (Gordon e.a., 2002; NIJ, 2007).

Daderprofielen leiden niet direct tot het identificeren van de (potentiële) dader van een delict maar geven een grove beschrijving van kenmerken waar de dader waarschijnlijk aan voldoet. Het gaat vooral om combinaties van kenmerken: de zogenoemde 'critical pathways' (zie Shaw, 2006). Het is dus niet zo dat wanneer individuen (of groepen) voldoen aan een bepaald profiel, zij ook daadwerkelijk als verdacht kunnen worden aangemerkt. Slechts de kans dat deze individuen (of groepen) crimineel gedrag (zullen gaan) vertonen is hoger dan wanneer zij niet aan een gegeven profiel voldoen. Zowel in het kader van preventie als voor de opsporing van high-tech crime is het ontwikkelen van daderprofielen onontbeerlijk. Niet alleen voor de opsporingsdiensten maar ook voor bijvoorbeeld bedrijven is dergelijke informatie nuttig om werknemers die computercriminaliteit begaan te kunnen traceren (Nykodym e.a., 2005). Zeker jongeren met kennis van ICT, of werknemers die ICT-functies vervullen met een hoog afbreuk- of veiligheidsrisico, zijn gewilde dienstverleners vanuit het oogpunt van georganiseerde criminaliteit (zie hoofdstuk 4). Aan de hand van risicoprofielen kunnen dan preventieve maatregelen worden genomen.

Ondanks de mogelijkheden die daderprofielen te bieden hebben, kleven er ook gevaren aan het gebruik ervan. Enerzijds kunnen onschuldige mensen (zogenoemde 'false positives') verdacht worden gemaakt of worden gestigmatiseerd omdat zij voldoen aan een bepaald risicoprofiel, terwijl anderzijds juist de werkelijke daders ten onrechte buiten schot kunnen blijven omdat het profiel niet klopt (zogenoemde 'false negatives') (Casey, 2002; Fidis, 2005: 52; Rogers, 2006). Profiling is een opsporingstechniek en beslist geen instrument van wetmatigheden. Te allen tijde vereist het gebruik van daderprofielen dus belangrijke nuances in de toepassing ervan. Gegeven dat de opbouw van kennis en expertise op het gebied van profiling (niet alleen in Nederland maar internationaal) nog

sterk in ontwikkeling is, zijn de toepassingen ervan op dit moment überhaupt nog (te) beperkt. Desondanks is er wel steeds meer aandacht voor het in kaart brengen van daderprofielen van high-tech crime (zie bijvoorbeeld Tompsett e.a., 2005). Tot op heden is dit nog maar beperkt van de grond gekomen en vooral toegepast op hackers (Biancuzzi, 2006; Casey, 2002: 551). We kunnen in dat kader dan ook beter spreken van inzicht in het soort daders dan van daderprofielen.

Een belangrijke reden voor het gebrek aan daderprofielen is het tekort aan data (Bednarz, 2005). Bij gebrek aan een 'intelligence database' die high-tech crime bijhoudt is het moeilijk om goed zicht te krijgen op daders (en hun werkwijzen).[114] Bijkomend probleem is dat er in de Nederlandse politieregistraties vaak geen onderscheid wordt gemaakt tussen criminaliteit met of zonder ICT (Europol, 2003: 12; Stol, 2001). Er is dus nog veel onderzoek nodig om tot betekenisvolle risicoprofielen van daders van high-tech crime te komen (Casey, 2002; Rogers, 2006). Er zullen systemen ontwikkeld moeten worden om daderkenmerken systematisch in kaart te kunnen brengen, met concreet onderscheid tussen de verschillende verschijningsvormen van high-tech crime. Op basis van de inzichten die hieruit voortvloeien kan op actievere en meer gerichte wijze worden gewerkt aan preventie en biedt dit verbeterde mogelijkheden voor het ontwikkelen en toetsen van scenario's en hypothesen voor de opsporingsautoriteiten.

In dit hoofdstuk inventariseren wij wat er in de literatuur bekend is over daders van de verschillende verschijningsvormen van high-tech crime (we spreken dus met nadruk niet van daderprofielen). Voor zover de beschikbare literatuur en bronnen dat toelaten, inventariseren we hier de kennis over daders van de geprioriteerde thema's van high-tech crime. Kennis over daders van de niet-geprioriteerde thema's komt terug in bijlage 6.

3.2 Kenmerken van daders van high-tech crime

High-tech crime werd voorheen vooral gekenmerkt door vernuftige computerexperts voor wie het een hobby was om in te breken op andermans computer en daar status en erkenning voor kregen. Tegenwoordig is high-tech crime echter steeds meer financieel gemotiveerd (Boerman en Mooij, 2006: 22; Choo, 2007; Post, 2006). Europol (2003: 73) onderscheidde de volgende algemene dadermotieven van high-tech crime:

– het behalen van voordeel (in de vorm van bijvoorbeeld informatie, financieel gewin, het vermijden van betalingen);

114 Nederland is volgens Europol (2003: 107) één van de landen die (in tegenstelling tot bijvoorbeeld Frankrijk, Duitsland, Griekenland, Italië, Spanje en het Verenigd Koninkrijk) geen database bijhoudt over daders.

– politieke overwegingen (waaronder ook persoonlijke overtuiging, ideologische of morele overwegingen) (zie ook NHTCC, 2006b: 7);
– nieuwsgierigheid;
– kwaadwilligheid en vandalisme;
– pesterij;
– behoefte aan macht.

Sommige onderzoekers opperen dat (potentiële) daders van high-tech crime niet veel anders zijn dan die in de fysieke wereld (Yar, 2005). Het algemene daderprofiel van de gemiddelde high-tech crimineel (blank, man, tussen de 12 en 28 jaar) is volgens Rogers (2001: 131) dan ook niet specifiek voor high-tech crime maar schetst een algemeen beeld van de 'gemiddelde crimineel'. Anderen stellen daarentegen dat daders van high-tech crime wel degelijk specifieke kenmerken zijn toe te schrijven (bijvoorbeeld McFarlane en Bocij, 2003). In de onderhavige literatuurstudie zijn we echter geen studies tegengekomen waar daderkenmerken van 'fysieke' en 'high-tech' criminaliteit daadwerkelijk empirisch met elkaar werden vergeleken.

Veel uitspraken en beweringen in zowel literatuur als diverse mediaberichten berusten op subjectieve oordelen en evaluaties van praktijkdeskundigen en onderzoekers. Het ontbreekt tot op heden zeker nog aan gevalideerde instrumenten waarmee op basis van gedragswetenschappelijk onderzoek subcategorieën van daders van high-tech crime (bijvoorbeeld aan de hand van de indeling als in schema 2 van hoofdstuk 2) kunnen worden onderscheiden (Rogers e.a., 2006b). In het navolgende zullen we op grond van de bevindingen uit de literatuur inventariseren wat er globaal bekend is over de daders van verschillende verschijningsvormen van high-tech crime. Er worden slechts aanwijzingen gegeven van mogelijke daderkenmerken die, voor het ontwikkelen van concrete daderprofielen, nog aan wetenschappelijke toetsing en evaluatie aan de (politie)praktijk bloot moeten worden gesteld. Er is dus nadrukkelijk slechts sprake van een summiere aanzet tot de ontwikkeling van risicoprofielen. Op basis van voortschrijdend inzicht en aanvullend onderzoek zal op langere termijn een nadere verfijning en uitbreiding op de hier gepresenteerde beschrijvingen noodzakelijk zijn.

Van de geprioriteerde thema's van high-tech crime (zie hoofdstuk 2) evalueren we specifiek de volgende daderkenmerken (zie ook Alison, McLean en Almond, 2007):
– sociale demografie (leeftijd, geslacht, opleiding, beroep);
– (technische) kennis en vaardigheden;
– primaire motivatie;
– sociaal-psychologisch profiel (gedragskenmerken in brede zin);
– criminele carrière (is er sprake van een strafblad);

– verschijningsvormen van high-tech crime (is er sprake van diversificatie).

3.2.1 Radicalisering

Radicalisering heeft een dynamisch karakter. Hoewel mensen ook individueel kunnen radicaliseren (de zogenoemde 'zelfontbranders'), is doorgaans sprake van een groepsproces en sociale beïnvloeding. Globaal worden de volgende risicokenmerken beschreven (TK 2004-2005, 29 754, nr. 26: 41):

Algemene daderkenmerken radicalisering:
- jongeren lopen verhoogd risico om te radicaliseren
- men daagt elkaar uit om zich steeds radicaler te uiten (gewelddadige trekken)
- men zet zich af tegen de maatschappij
- men maakt gebruik van symbolen en leuzen
- er is sprake van los-vaste (fluïde) groepen
- het gaat om actieve internetgebruikers (MSN, discussieforums, verspreiden van gedachtegoed)
- behalve virtueel is men ook fysiek actief in bijeenkomsten
- men beschikt over overtuigingskracht en kan goed debatteren

Daarnaast zijn er verschillende publicaties waarin typen daders worden beschreven die betrekking hebben op specifieke stromingen zoals het rechts-extremisme (Lonsdale jongeren) en het islamistisch radicalisme.[115] We geven een kort overzicht.

Rechts-extremisme
Volgens Linden (aangehaald in Van Beek, 2007: 11) zijn er vier typen rechts-radicalen te onderscheiden, namelijk de zoekers (met overtuigde nationalistische ideeën), de bekeerlingen (die iets willen doen voor de 'gewone man'), de conformisten (meelopers), en de revolutionairen (die militaristisch zijn ingesteld en zichzelf zien als redders van het blanke volk). Bij de revolutionairen kan volgens Linden sprake zijn van een voorbijgaande levensfase (gekenmerkt door veel bier, feesten, meisjes en geweld) maar een deel daarvan (vaak hoogopgeleide, intelligente, belezen personen) bijt zich vast en ontpopt zich tot radicale extremist. De volgende kenmerken worden met het rechts-extremisme geassocieerd (Linden, aangehaald in Van Beek, 2007; Schafer, 2003):

115 Op grond van de geraadpleegde literatuur is van het dierenrechtenactivisme geen specifieke daderinformatie voorhanden.

Daderkenmerken rechts-radicalisme:
Sociaal-demografische kenmerken:
- blank
- jongere tussen de 15 en 24 jaar
- variabel opleidingsniveau, van school gestuurd of baan kwijtgeraakt
- gebrekkig toekomstperspectief

(Technische) kennis en vaardigheden:
- *geen bijzonderheden bekend*

Primaire motivatie:
- ideologie is levensstijl (men wil niet in de maatschappij/gevestigde orde meedraaien)

Sociaal-psychologisch profiel:
- provocerend in gedrag (uitspraken, symbolen)
- geïnteresseerd in Nederlandse en Duitse geschiedenis, WOII en militarisme
- ziet zichzelf als strijder en redder van het blanke volk
- gebrek aan ouderlijke supervisie
- houdt zich op in groepen (drugs, alcohol en vechten op straat)
- bestudeert ingewikkelde teksten en opvattingen

Criminele carrière:
- *geen bijzonderheden bekend*

Verschijningsvormen van high-tech crime:
- *geen bijzonderheden bekend*

Islamistisch radicalisme
Volgens Demant (aangehaald in Van Beek, 2007: 10) zijn er drie radicaal-islamistische hoofdstromen te onderscheiden, namelijk de a-politieke salafisten (die tegen democratie en geweld zijn en zich willen terugtrekken in een eigen enclave), de politieke salafisten (die tegen democratie zijn maar het systeem wel gebruiken om hun doelen te bereiken), en de jihadistische salafi's (die de democratie actief willen bestrijden, desnoods met geweld). Alleen de jihadistische salafi's zijn volgens Demant werkelijk extremisten. De oorzaken voor de ontvankelijkheid van moslimjongeren voor radicalisering en extremisme moet volgens de AIVD (2006a: 57, 65) worden gezocht in:
- religieuze zingeving (een fixatie op de puriteinse islam);
- politiek-maatschappelijke problemen (woede en frustratie over de positie van moslims in het Westen en in de islamitische wereld zelf die men wil veranderen);
- sociaal-psychologische, sociale en culturele factoren (meelopers die op zoek zijn naar een identiteit en weinig inhoudelijke affiniteit hebben met het radicalisme).

Islamistische radicalisten en extremisten zijn veelal in Europa geboren kinderen van migranten met een islamitische (Noord-Afrikaanse

Daderkenmerken islamistisch radicalisme:
Sociaal-demografische kenmerken:
– jongeren onder de 20 jaar, geboren en getogen in Europa (home-grown)
– kind van migranten met islamitische achtergrond (Noord-Afrika, Pakistan)
(Technische) kennis en vaardigheden:
– intelligent, belezen, maar geen goede beheersing Arabische taal
– actieve internetgebruikers (MSN, discussiefora, websites)
– trainingservaring
– primaire motivatie:
– op zoek naar identiteit, behoefte aan aandacht en zelfbevestiging
– politiek-religieus (fixatie op de puriteinse islam)
– gefrustreerd over de maatschappelijke positie van moslims
Sociaal-psychologisch profiel:
– fluïde netwerken door sociale affiliatie (religie, familie, vriendschap, trainingservaringen)
– eclectisch gebruik van klassieke geschriften en opvattingen
– verzamelt selectief informatie en verwerkt dit tot eigen ideologie ('knip-en-plak-radicalisme')
Criminele carrière:
– *geen bijzonderheden bekend*
Verschijningsvormen van high-tech crime:
– propaganda (virtuele wereld is complementair aan het fysieke)

of Pakistaanse) achtergrond (AIVD, 2006a: 8, 17). De harde kern in Nederland is relatief klein (enkele honderden personen in circa 10 tot 20 netwerken) (AIVD, 2006a: 54-55). Uit een rapport van de NCTb (2006b: 50) over het gebruik van internet blijkt dat vooral jongeren (onder de 20 jaar) betrokken zijn bij het verspreiden van radicale propaganda. Zij begeven zich in lokale, fluïde, informele netwerken waarbinnen men een bepaalde vorm van verwantschap deelt (dit kan zijn een politiek-religieuze ideologie, familie- of vriendschapsbanden, of gemeenschappelijke trainingservaringen in bijvoorbeeld Pakistan) (AIVD, 2006a: 13). Personen die in de 'fysieke wereld' onderdeel uitmaken van een radicaal islamistisch netwerk (zoals de Hofstadgroep) blijken vaak actieve internetgebruikers met een beperkte beheersing van de Arabische taal (NCTb, 2006b: 64, 66). Volgens de AIVD (2006a: 44) zijn vooral de behoefte aan aandacht en zelfbevestiging sturend in de webdiscussies die plaatsvinden op het internet. Het profiel van de aan terrorisme sympathiserende moslim die gebruikmaakt van het internet vertoont volgens de AIVD (aangehaald door de NCTb, 2006a: 52) echter grote overeenkomsten met de hele allochtone internettende jeugdpopulatie. Opvallend is wel dat in Nederland, in vergelijking met andere Europese landen, moslima's een actieve rol spelen binnen de fysieke en virtuele propagandanetwerken (NCTb, 2006a: 51). Zij ontwikkelen MSN-groepen en websites, zijn actief betrokken bij het verspreiden

van het gedachtegoed via discussiefora, verrichten documentatieonderzoek, en maken Nederlandse vertalingen van jihadistische literatuur.

3.2.2 Terrorisme en ideologisch gemotiveerde misdaad

Van alle terroristenverdachten[116] die in 2006 binnen de EU zijn gearresteerd, kan op grond van gegevens van Europol (2007a) het volgende beeld worden geschetst: daders zijn mannelijke (88%) EU-staatsburgers (52%) met een gemiddelde leeftijd van 36 jaar (waarvan de meeste tussen de 26 en 46 jaar). In de literatuur zien we een scheve verdeling in de aandacht voor daders: het overgrote deel is gericht op het islamistisch terrorisme. Van extreem-rechtse terroristen wordt alleen gezegd dat zij een nationalistische ideologie hebben (die het volledige politieke, sociale en economische systeem willen omgooien naar rechtse maatstaven) en dat zij hun terroristische activiteiten met (illegale) wapenhandel financieren (Europol, 2007a). Op grond van de beschikbare bronnen beperken we onze aandacht hier tot kennis over daders van het islamistische terrorisme.

Islamistisch terrorisme
Islamistische terroristen kenmerken zich door een extreme interpretatie van de islam. De meeste islamistische verdachten binnen de EU (in 2006) waren afkomstig uit Noord-Afrika (Marokko, Algerije en Tunesië) en hadden losse banden met terroristische groeperingen. De gemiddelde leeftijd van de verdachten lag tussen de 26 en 41 jaar en sommigen volgden trainingsactiviteiten in het buitenland (dit kan variëren van lessen in de radicale ideologische interpretatie van de islam tot het toepassen van terroristische, militaire technieken zoals het gebruik van explosieven en het opzetten en financieren van terroristische cellen). Verdachten zijn bovendien betrokken bij criminele activiteiten zoals identiteitsvervalsing, documentvervalsing en creditcardfraude (Europol, 2007a). Vooral oudere mannen (tussen de 30 en 41 jaar) worden in verband gebracht met documentvervalsing, de financiering en de daadwerkelijke uitvoering van terroristische activiteiten. De jongere garde (mannen en vrouwen jonger dan 30 jaar) houdt zich meer bezig met faciliterende activiteiten (documentvervalsing) en rekrutering (op scholen, spirituele ontmoetingsplekken zoals moskeeën, en gevangenissen).

Bakker (2006) deed onderzoek naar daderkenmerken van islamistische terroristen die betrokken waren bij 31 incidenten in Europa tussen september 2001 en oktober 2006. Het betrof in totaal 242 individuen (en 28 netwerken). Kenmerkend voor deze netwerken is dat er binnen de groepen sprake is van homogeniteit wat betreft leeftijd, woonplaats en

116 Dierenrechtenactivisten komen in het Europol-rapport niet expliciet aan de orde.

nationaliteit. Volgens de auteur duidt dit op een proces van sociale affiliatie (men komt via familie of vrienden met elkaar in contact en raakt op die manier verweven met het terrorisme). Met uitzondering van de volgende kenmerken is er volgens Bakker geen typisch daderprofiel van deze islamistische terroristen op te stellen:

- man;
- alleenstaand;
- leeftijd tussen 16 en 59 jaar (gemiddelde leeftijd 27 jaar ten tijde van arrestatie);
- geboren (> 40%) en getogen (55%) in Europa (1e, 2e, of 3e-graads migrant)
- ouders met Noord-Afrikaanse (Marokko, Algerije) of Pakistaanse afkomst;
- variabel opleidingsniveau (laag tot hoog);
- lagere sociaal-economische positie;
- strafblad (waaronder wapenbezit);
- woede en frustratie over de positie en belediging van moslims in Europa
- op zoek naar een eigen identiteit;
- in de tijd een gradueel toenemende involvering in het geloof (anderen willen bekeren, levendige deelname aan discussies, ook op het internet).

In een overzichtsartikel van Loza (2007) naar de psychologische kenmerken van extremisten en terroristen werd het verschil benadrukt tussen de internationaal georiënteerde en de lokale 'home-grown' islamistische terrorist van eigen bodem. Internationaal georiënteerde terroristen zijn volgens Loza doorgaans goedopgeleide (universitaire) ambitieuze jonge mannen (met een gemiddelde leeftijd tussen de 17 en 26 jaar), afkomstig uit middenklassefamilies. De 'home-grown' terroristen zijn lager opgeleid, werkloos, sociaal vervreemd en kunnen min of meer worden getypeerd als zogenoemde 'drop-outs' van de maatschappij. Loza schreef verder de volgende algemene kenmerken toe aan islamistische terroristen: jonger dan 25 jaar, hoger opgeleid dan de ouders, een rigide (primitieve, naïeve, utopische) manier van denken[117] en het analytische denkvermogen is minder goed ontwikkeld ,[118] algemene gevoelens van ontevredenheid, gevoel van vervreemding van de maatschappij, zich afzetten tegen de Westerse cultuur (soms gepaard met een 'dresscode'), sterke identificatie met moslimslachtoffers in landen als Irak, en een externe oriëntatie om het eigen gedrag mee te verantwoorden (het is de 'wil van God'). We vatten de volgende kenmerken samen:

117 Afwijkende ideeën worden niet getolereerd, er is sprake van sterk zwart-witdenken (goed versus slecht), complexe zaken worden te eenvoudig voorgesteld, men is ervan overtuigd persoonlijk symbool te staan voor de islam en ziet zichzelf als vrijheidsstrijder.

118 Er is in hoge mate sprake van groepsdenken, een gedeelde groepsidentiteit en gehoorzaamheid aan de grotere groep. De extreme ideologie die men aanhangt gaat gepaard met sterk polariserend denken (in termen van 'wij' en 'zij').

Daderkenmerken islamistisch terrorisme:
Sociaal-demografische kenmerken:
- man
- alleenstaand
- variabele leeftijd (het gros tussen de 17 en 41 jaar oud)
- variabel opleidingsniveau
- 1e, 2e, of 3e-graads Europees migrant
- ouders met Noord-Afrikaanse (Marokko, Algerije, Tunesië) of Pakistaanse afkomst
- lagere sociaal-economische positie (bijvoorbeeld werkloos)

(Technische) kennis en vaardigheden:
- virtueel actief (MSN, documentatieonderzoek, verspreiden vertalingen)
- mogelijk trainingservaring in het buitenland (radicale interpretatie islam, militaire technieken)

Primaire motivatie:
- woede en frustratie over de positie en belediging van moslims in Europa
- op zoek zijn naar een eigen identiteit

Sociaal-psychologisch profiel:
- sociaal vervreemd van de maatschappij
- begeeft zich in homogene groepen (familiebanden, vriendschappen)
- rigide, primitieve, naïeve, utopische manier van denken (extreme interpretatie van de islam)
- analytisch denkvermogen is minder goed ontwikkeld (sterk polariserend denken: wij vs zij)
- hecht sterk aan groepsidentiteit en gehoorzaamheid aan grotere groep
- algemene gevoelens van ontevredenheid
- zet zich af tegen de westerse cultuur (gaat soms gepaard met een dress-code)
- identificeert zich met moslimslachtoffers in landen als Irak
- sterke externe oriëntatie om eigen gedrag mee te verantwoorden (het is de 'wil van God')

Criminele carrière:
- strafblad (waaronder wapenbezit)

Verschijningsvormen van high-tech crime:
- identiteits- en documentvervalsing
- creditcardfraude

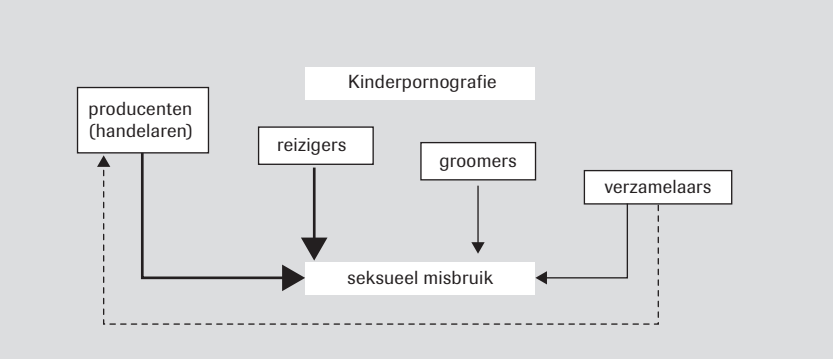
3.2.3 Kinderporno

Met betrekking tot kinderpornografie is er een onderscheid te maken tussen vier categorieën daders (Durkin, aangehaald door Alexy e.a., 2005: 810; McLaughlin, 2000):

1. *Vervaardigers en handelaren* die het materiaal maken en verspreiden. Het seksueel misbruiken van kinderen (zelf of door anderen hiertoe aan

te zetten) behoort voor deze dader tot 'core business' om handelsmateriaal te produceren.
2. *Verzamelaars* die het materiaal downloaden en gelijkgeïnteresseerden ontmoeten in een virtuele ruimte en tot een virtuele gemeenschap (pedofielennetwerk) behoren. Men komt in principe niet direct fysiek in contact met minderjarigen, maar de Britse politie schat dat in ongeveer 20% van de gevallen wel degelijk sprake is van seksueel misbruik van kinderen (Gelderblom, 2004).[119]
3. *Reizigers* die kinderen daadwerkelijk seksueel misbruiken. Deze dader gaat heel ver om tot een fysieke ontmoeting met kinderen te komen (vandaar de naam 'reiziger').
4. *Groomers en chatters* (zie McLaughlin, 2000) die ongepast seksueel getinte communicatie voeren met kinderen, bijvoorbeeld via chatsites, wat in sommige gevallen uitmondt in daadwerkelijk seksueel misbruik (na een fysieke ontmoeting geregeld te hebben of via de webcam).

Schema 5 Dadercategorieën van kinderporno in relatie tot seksueel misbruik van minderjarigen



De relatie tussen het verspreiden van kinderporno en het seksueel misbruiken van jonge kinderen verdient nog nader onderzoek (Sullivan, 2005). Voor de verschillende dadercategorieën van kinderpornografie staat de relatie tot het seksueel misbruiken van kinderen weergegeven in schema 5. Producenten/handelaren en reizigers worden in sterkere mate in verband gebracht met seksueel misbruik (de dikke pijlen in schema 5). Door de eenvoudige beschikbaarheid van digitale fotografie en het uitwisselen van afbeeldingen binnen de pedofiele netwerken worden verzamelaars zelf ook in toenemende mate handelaren (de 'loop' in schema 5).

119 Deze cijfers worden gesteund door onderzoek van Lunnemann en anderen (2006: 145-148).

Wat betreft daderkenmerken komen de makers en verspreiders van kinderporno voor in alle lagen van de bevolking en begeven ze zich vaak in netwerken[120] (Van der Werf, 2003: 47). Er is dus sprake van een divers, heterogeen daderprofiel. Van de verspreiders en verzamelaars van kinderporno kan de volgende algemene profielschets worden gegeven (Alexy e.a., 2005; Jewkes en Andrews, 2007: 67; Lunnemann e.a., 2006: 122-123; McLaughlin, 2000; Sullivan, 2005, 2007[121]): het gaat veelal om een blanke man, variabel in leeftijd (gemiddeld tussen de 30 en 37 jaar), die in het dagelijks leven regelmatig via beroep of vrijetijdsbesteding in contact komt met kinderen (bijvoorbeeld een coach, leraar, jeugdwerker). De verzamelaar heeft een sterke behoefte aan macht en controle, maakt overmatig (compulsief en obsessief) gebruik van het internet, heeft een enorme verzamelingsdrang en kan kampen met mentale of psychische problemen (bijvoorbeeld seksuele stoornissen, drank- of drugsmisbruik). De primaire motivatie voor het verzamelen van kinderporno is seksuele stimulatie. In sommige gevallen zijn daders in het bezit van een strafblad (de meesten in verband met een zedendelict).[122]

McLaughlin (2000) bestudeerde 200 daders die waren gearresteerd in het kader van een drie jaar durend onderzoek naar kinderporno. Het betrof hier kinderpornografisch materiaal met jonge jongetjes als object/slachtoffer waardoor de resultaten van dit onderzoek niet zonder meer te generaliseren zijn. Het overgrote deel van de daders (ruim tweederde, N=143) werd gekarakteriseerd als verzamelaar of als reiziger (bijna een kwart, N=48). Van de overige daders ging het in 4% van de gevallen daadwerkelijk om producenten/vervaardigers (N=8) en in slechts één geval betrof het een chatter of groomer (zie ook volgende paragraaf). In het navolgende wordt per dadertype een beschrijving van kenmerken gegeven op basis van het onderzoek van McLaughlin (2000).

120 In Nederland zijn er in 2004 en 2005 circa 440 verzamelaars van kinderporno opgepakt (via operatie Neon en onderzoek dat deels door de FBI tot stand werd gebracht). Alle verdachten waren mannen (Cops, 2007h).

121 Het betreft hier profiling-onderzoek uit Nieuw Zeeland naar verspreiders van kinderporno over het internet. De database telde ten tijde van dit rapport (2007) 215 daderprofielen.

122 Gedurende het onderhavige onderzoek verschenen er diverse berichten in de Nederlandse media over arrestaties van verdachten van kinderporno. Het betrof in de meeste gevallen het bezit en verspreiden van kinderporno (via MSN-kinderpornogroepen) (Cops, 2007f, 2007i en 2007l). Verdachten bleken autochtone mannen in de leeftijd van 29 tot 65 jaar. In één geval betrof het een 32-jarige Nederlandse producent van kinderporno. De man, die lid was van een internationaal pedofielennetwerk, had jonge meisjes (van 5 en 12 jaar oud) verkracht en op film gezet voor distributie. Hij werd in mei 2007 veroordeeld tot 4,5 jaar cel en TBS (Cops, 2007l).

Ad 1. Vervaardigers. Bezoekt publieke ruimten (zoals zwembaden en stranden) om kinderen te fotograferen. Heeft relatief vaak een strafblad (voor zedendelicten en/of kindermishandeling) en in sommige gevallen (50%) wordt onderdak verleend aan kinderen die van huis zijn weggelopen. Maakt gebruik van 'reflectorsites' waarop meerdere gebruikers, die een perifere computercamera hebben aangesloten, tegelijk kunnen inloggen en elkaar tegelijkertijd ook in beeld kunnen zien. De reflectorsites worden door jongeren gebruikt om publiekelijk seksuele handelingen te verrichten. Het is voor de vervaardiger tamelijk eenvoudig om deze beelden op te nemen en ze vervolgens te verspreiden onder derden. Niet zelden krijgen minderjarige tieners onder valse voorwendselen webcams opgestuurd om hen vervolgens over te halen tot seksuele handelingen voor de camera.

Daderkenmerken vervaardiger (naar McLaughlin, 2000):

Sociaal-demografische kenmerken:
- man
- variabele leeftijd (van 26 tot 53 jaar, met een gemiddelde van 41 jaar)

(Technische) kennis en vaardigheden:
- bezoekt reflectorsites, neemt beelden op en verspreidt ze aan derden

Primaire motivatie:
- *geen bijzonderheden bekend*

Sociaal-psychologisch profiel:
- is manipulatief (haalt kinderen over tot seksuele handelingen voor webcam)
- bezoekt publieke ruimten (zwembad, strand) om kinderen te fotograferen
- verleent onderdak aan weggelopen kinderen

Criminele carrière:
- strafblad (zedendelict of kindermishandeling)

Verschijningsvormen van high-tech crime:
- *geen bijzonderheden*

Ad 2. Verzamelaar. Verkrijgt het meeste materiaal gratis via het internet of door te ruilen met anderen. Maakt van favoriete afbeeldingen regelmatig 'hard copies' en hangt deze plaatjes in de slaapkamer waar ze worden gebruikt voor seksuele stimulatie. Door de veelheid aan afbeeldingen gebruikt men veel computergeheugen en beschikt men over extra hard- en zipdrives. Van de zogenoemde 'statische' internetlocaties (zoals het bezoeken van websites en nieuwsgroepen) gaan de meeste verzamelaars gaandeweg over op 'dynamische' internetlocaties (zoals chatrooms en Internet Relay Chat). Op dat moment is de verzamelaar door uitwisseling van afbeeldingen met anderen ook verspreider geworden van kinderporno.

Daderkenmerken verzamelaar (naar McLaughlin, 2000):
Sociaal-demografische kenmerken:
– man
– variabele leeftijd (van 13 tot 65 jaar)
– alleenstaand en alleenwonend
(Technische) kennis en vaardigheden:
– bezoekt websites, nieuwsgroepen, chat rooms en maakt gebruik van IRC
– beschikt over uitgebreid computergeheugen (extra hard- en zipdrives)
– maakt gebruik van afscherming (encryptie)
Primaire motivatie:
– seksuele stimulatie (favoriete afbeeldingen hangen in de slaapkamer)
– sociaal-psychologisch profiel:
Sociaal geïsoleerd
– in het dagelijks leven in contact met kinderen (21%)
– ruilt plaatjes met andere geïnteresseerden (verzameldrift)
– verslavingsgevoelig
Criminele carrière:
– geen strafblad
Verschijningsvormen van high-tech crime:
– *geen bijzonderheden*

Ad 3. Reizigers. Chat online met kinderen en manipuleert of dwingt hen tot een fysieke ontmoeting voor seksueel contact. Doet zich in het begin vaak voor als tiener en probeert persoonlijke informatie van het kind los te krijgen, het kind vertrouwen te geven, maakt seksuele toespelingen en stuurt pornografische afbeeldingen op (meer dan de helft stuurt uiteindelijk [naakt]foto's van zichzelf). Men is er doorgaans van overtuigd dat de kinderen zelf seksueel contact willen en reist hiervoor soms zelfs naar andere landen. Kinderen worden echter ook overgehaald om naar de dader toe te komen. Het kind wordt in sommige gevallen overtuigd om van huis weg te lopen en de dader betaalt dan bijvoorbeeld de reiskosten (of stuurt een heel reisticket op). De meeste reizigers zijn ook verzamelaar en een kleine selectie (7%) heeft ook sadistische pedofiele trekken.

Ad 4. Chatter. Is buitensporig veel op het internet te vinden (soms meer dan 12 uur per dag) en doet zich daar voor als raadgever en vertrouwenspersoon van kinderen. Kinderen worden er indirect toe aangezet om raad te vragen en vragen te stellen, bij voorkeur op het gebied van seks. De chatter heeft geen behoefte aan fysiek contact met het kind maar probeert om telefonisch in gesprek te komen in de hoop dat dit gesprek zich ontwikkelt tot een vorm van telefoonseks. Er is mogelijk sprake van andere seksuele gedragingen of fantasieën (parafilie)[123] die over het algemeen als afwijkend kunnen worden beschouwd.

123 Bijvoorbeeld seksuele opwinding door voorwerpen, voyeurisme, masochisme (Wikipedia, laatst geraadpleegd op 19 juli 2007).

Daderkenmerken reiziger (naar McLaughlin, 2000):
Sociaal-demografische kenmerken:
– man
– variabele leeftijd (van 17 tot 56 jaar, met een gemiddelde van 35 jaar)
(Technische) kennis en vaardigheden:
– chat online met kinderen (en doet zich voor als tiener)
Primaire motivatie:
– seksueel contact met kinderen
Sociaal-psychologisch profiel:
– is manipulatief (dwingt of haalt kinderen over tot een ontmoeting met fysiek contact)
– reist naar de kinderen toe (ook in het buitenland) of laat kinderen zelf reizen
– doet seksuele toespelingen en stuurt (naakt)foto's van zichzelf of ander pornografisch materiaal
– is ervan overtuigd dat kinderen zelf seksueel contact willen
Criminele carrière:
– geen strafblad
Verschijningsvormen van high-tech crime:
– *geen bijzonderheden*

Daderkenmerken chatter (naar McLaughlin, 2000):
Sociaal-demografische kenmerken:
– man
(Technische) kennis en vaardigheden:
– buitensporig veel op het internet te vinden (> 12 uur per dag)
Primaire motivatie:
– geen behoefte aan fysiek contact, wil graag telefoonseks
Sociaal-psychologisch profiel:
– werpt zich op als vertrouwenspersoon voor kinderen (raadgever op gebied van seks)
– mogelijk sprake van andere vormen van parafilie
Criminele carrière:
– *geen bijzonderheden bekend*
Verschijningsvormen van high-tech crime:
– *geen bijzonderheden bekend*

3.2.4 Grooming

Bij grooming is sprake van seksuele toenadering van minderjarigen door een volwassen persoon via chatsites en webcams, die zich daarbij in eerste instantie voordoen als een leeftijdgenoot. Ook over deze daders is in de literatuur weinig bekend. Recentelijk is grooming vaker in het nieuws geweest. In sommige gevallen bleken de chatsessies ook daadwerkelijk

tot ontuchtige handelingen met minderjarigen en verkrachting te hebben geleid (Cops, 2007b, 2007c en 2007d). De daderkenmerken van de 'reiziger' (zie kinderporno) zijn waarschijnlijk het meest illustratief voor groomers. Bij de berichtgeving in de media betrof het in alle gevallen mannen, vermoedelijk autochtoon, in de leeftijd van 23 tot 58 jaar. Niet zelden chanteerde de dader het slachtoffer via MSN tot het verrichten van seksuele handelingen voor de webcam. Daarbij was in één geval ook sprake van doelbewuste stalking van minderjarige meisjes (via hun mobiele telefoon en MSN) (Cops, 2007b en 2007d). Op grond van de mediaberichten worden de volgende daderkenmerken beschreven:

Daderkenmerken grooming:
Sociaal-demografische kenmerken:
- man
- leeftijd van 23 tot 58 jaar
- autochtoon

(Technische) kennis en vaardigheden:
- benadert kinderen via chatsites (MSN) en maakt gebruik van webcam

Primaire motivatie:
- seksuele stimulatie

Sociaal-psychologisch profiel:
- voert seksueel getinte chatsessies
- stuurt afbeeldingen van zichzelf
- haalt kinderen over of dwingt ze tot seksuele handelingen (fysiek of virtueel)

Criminele carrière:
- *geen bijzonderheden bekend*

Verschijningsvormen van high-tech crime:
- stalking via MSN of mobiele telefoon

3.2.5 Softwarepiraterij

In hoofdstuk 2 werden verschillende vormen van softwarepiraterij onderscheiden. Hieruit volgt dat er ook minimaal vier typen softwarepiraten te onderscheiden zijn: eindgebruikers, overgebruikers, internetpiraten, en illegale handelaren. *Eindgebruikers* (die software zonder toestemming kopiëren of installeren) en *overgebruikers* (die een programma vaker gebruiken dan de licentie toestaat) zijn niet alleen particuliere 'consumenten' maar ook bedrijven die illegaal gebruikmaken van allerlei software (Gelderblom, 2004: 101). Particuliere eindgebruikers die piraterij plegen blijken vooral mannen te zijn met enige computerervaring en -vaardigheden (Seale e.a., aangehaald door Lau, 2006). Over bedrijven die piraterij plegen is in de literatuur niets bekend. Daders van *internetpiraterij* (die illegaal bestanden met muziek, films, games en ander auteursrechtelijk beschermd materiaal downloaden of uitwisselen via P2P-netwerken)

zijn veelal particuliere hobbyisten en (semi-)professionele inbreukmakers die geld verdienen aan het illegale aanbod van software (Brein, 2007). Het gaat in dit geval bijvoorbeeld ook om mensen die namaaksoftware via internetveilingen aanbieden. Volgens onderzoek van Packard Bell naar het gebruik van mp3-spelers, downloadt 84% van de gebruikers muziek illegaal via het internet: vooral oudere jongeren in de leeftijd tussen 18 en 35 jaar (Metro, 27 juni 2007). Als voornaamste motief voor softwarepiraterij wordt het financiële voordeel genoemd (Lau, 2006). Onderzoek van Higgins (2005) toonde bovendien aan dat studenten die lager scoren op zelfcontrole zich vaker schuldig maken aan softwarepiraterij. Over daderkenmerken van *illegale handelaren* (die software verveelvoudigen en verkopen)[124] is in de literatuur weinig bekend. Wat er van de verschillende dadertypen aan kenmerken uit onderzoek is gebleken wordt onderstaand samengevat.

Daderkenmerken Softwarepiraterij:

Sociaal-demografische kenmerken:
- particulieren én bedrijven (eindgebruikers en overgebruikers)
- particulieren (internetpiraten en illegale handelaren)
- leeftijd tussen 18 en 35 jaar (internetpiraten)
- man (particuliere eindgebruiker)

(Technische) kennis en vaardigheden:
- computerervaring (particuliere eindgebruiker)

Primaire motivatie:
- financieel voordeel (of waargenomen nadelen beperken)
- hobby

Sociaal-psychologisch profiel:
- gebrek aan zelfcontrole

Criminele carrière:
- *geen bijzonderheden bekend*

Verschijningsvormen van high-tech crime:
- *geen bijzonderheden bekend*

3.2.6 Internetfraude: voorschot- en identiteitsfraude

Wat betreft daders van oplichting via het internet (internetfraude) maken we expliciet onderscheid tussen voorschotfraude en identiteitsfraude (zie ook hoofdstuk 2).

124 We verstaan hieronder ook het verkopen van nieuwe computers met illegale exemplaren van software op de harde schijf.

Daderkenmerken voorschotfraude:
Sociaal-demografische kenmerken:
– man
– tussen de 18 en 48 jaar
– afkomstig uit West-Afrika (Nigeria, Soedan, Liberia) (sommigen illegaal)
(Technische) kennis en vaardigheden:
– beperkte ICT-expertise
– professioneel
Primaire motivatie:
– financieel gewin
Sociaal-psychologisch profiel:
– gebrek aan schuldbesef
Criminele carrière:
– hoge recidive (oplichting en fraude)
– internationale connecties (georganiseerde misdaad)
Verschijningsvormen van high-tech crime:
– crimineel netwerk (met internationale connecties)
– versturen van spam
– oplichting via e-mail en internet
– plunderen van internetrekeningen
– vervalste en gestolen (persoons)documenten
– witwassen

Voorschotfraude
Enkele jaren geleden was er nog weinig zicht op de specifieke kenmerken van daders van de Nigeriaanse voorschotfraude (Van der Werf, 2003: 37). Wel was duidelijk dat het hier ging om een vorm van georganiseerde misdaad en werden er banden gesuggereerd met kerken in Nederland die als dekmantel zouden fungeren om zwart geld naar het buitenland te loodsen (Cops, 2007h). Inmiddels is gebleken dat het vooral mannelijke daders zijn die veelal in (internationaal) groepsverband opereren en zich steeds verder professionaliseren. De meeste daders hebben een strafblad (op het gebied van oplichting en fraude) en de recidive is hoog: men begint ook na veroordeling gewoon opnieuw, desnoods in een ander land (Cops, 2007h). Met name in Amsterdam (maar ook Rotterdam en Den Haag) zijn een aantal groepen actief die waarschijnlijk onderdeel uitmaken van een wereldwijd crimineel netwerk. Uit diverse Nederlandse berichtgevingen van verdachten van internetoplichting (op het gebied van spam, oplichting via e-mail en internet, en het plunderen van internetrekeningen) bleken de gearresteerden overwegend mannen tussen de 18 en 48 jaar, opererend in groepjes van 4 tot 21 personen. Meestal opereerden zij vanuit steden met een grote Nigeriaanse gemeenschap (zoals Amsterdam of Londen) en maakten zij

gebruik van bijvoorbeeld internetcafés of een gehuurd kantoor (Cops, 2007h; Internetoplichting.nl, 2007; KLPD, juni 2007; OM, 26 september 2006; Webwereld, 2007). De meeste verdachten hadden een West-Afrikaanse achtergrond (Nigeria, Soedan, Liberia), waarvan sommigen illegaal in ons land verbleven. Tot de verdachten behoren echter enkele Nederlanders. In minstens één geval werd gebruikgemaakt van een stroman (een 78-jarige Rotterdammer) om hand- en spandiensten te verlenen zoals het ophalen van spullen op het postkantoor (OM, 26 september 2006). Slachtoffers, voor zover bekend, zijn vooral Amerikanen en Europeanen en mensen op leeftijd (de buit liep in sommige gevallen op tot 2,5 miljoen euro) (Internetoplichting.nl, 2007; OM, 26 september 2006). De oplichters maken veelvuldig gebruik van vervalste en gestolen (persoons)documenten en worden verdacht van witwassen (Cops, 2007h; KLPD, juni 2007; OM, 26 september 2006).

Identiteitsfraude

Over de daders van identiteitsfraude (met behulp van phishing) is op grond van deze literatuurstudie weinig informatie verkregen. In het V-NDB2006 (Boerman en Mooij, 2006) werd gesteld dat het om hackers gaat (zie hacking) die de overstap hebben gemaakt naar computercriminaliteit voor financieel gewin. Er zijn bij de Nationale en Bovenregionale Recherche maar een beperkt aantal opsporingsonderzoeken naar identiteitsfraude gedaan (KLPD, DNRI, 2007a: 24-26). Uit internationale literatuur komt naar voren dat identiteitsdiefstal steeds meer het werkterrein is van criminelen die zich voorheen bezighielden met drugshandel (Newman en McNally, 2005). De grote opbrengsten en geringe pakkans maken deze vorm van high-tech crime voor de opportunistische kanszoeker een aantrekkelijker alternatief dan de handel in drugs. Uit onderzoek van Copes en Vieraitis (2007), waarbij 59 gedetineerden werden geïnterviewd, blijkt dat daders van identiteitsdiefstal niet te definiëren zijn als homogene dadergroep. Primaire motivatie is het op relatief eenvoudige manier snel geld verdienen terwijl daar een geringe waargenomen pakkans tegenover staat. Andere kenmerken die worden omschreven zijn: werkende middenklasse, strafblad (bijvoorbeeld fraude, drugs), manipulatief sterk, technische vaardigheden en kennis van systemen (bijvoorbeeld banken en andere financiële instellingen). Een deel van de daders bleek een arbeidsverleden te hebben waarbinnen deze kennis kon worden vergaard: men werkte bijvoorbeeld bij een hypotheekinstelling, overheidsdienst of andere bedrijven die toegang bieden tot persoonlijk identificerende gegevens als creditcardnummers (banken, warenhuizen). Wij vatten een aantal daderkenmerken onderstaand samen.

Daderkenmerken identiteitsfraude (phishing):
Sociaal-demografische kenmerken:
– werkende middenklasse
(Technische) kennis en vaardigheden:
– professionele hacker als dienstverlener
– taakspecialisatie: men werkt in groepsverband en/of op huurbasis
– gebruik van botnets
– maken van nepwebsites
– technisch vaardig
– kennis van systemen van banken (soms in relatie tot arbeidsverleden)
Primaire motivatie:
– financieel gewin (grote opbrengsten, geringe waargenomen pakkans)
Sociaal-psychologisch profiel:
– manipulatief
Criminele carrière:
– voorheen mogelijk betrokken bij drugshandel
– strafblad (fraude, drugs)
Verschijningsvormen van high-tech crime:
– dDoS-aanvallen
– clickfraude
– spamming

3.2.7 Witwassen

Over daders van witwaspraktijken met behulp van ICT is in de literatuur ook weinig tot niets bekend. Enige uitzondering daarop vormt de verdenking van daders van Nigeriaanse voorschotfraude die met witwassen in verband worden gebracht. Hoewel er volgens experts redenen zijn om aan te nemen dat virtuele casino's, online veilingsites, e-commerce- en m-commerce-bedrijven (organisaties die in hun bedrijfsvoering gebruikmaken van respectievelijk digitale en mobiele communicatie en transacties) als dekmantel fungeren voor crimineel geld, zal nader onderzoek naar de virtuele geldstromen in deze sector meer inzicht moeten geven op dit vlak (Cops, 2007h; Europol, 2003: 40).

3.2.8 Cyberterrorisme

Aangezien er nog geen cyberterroristische aanslagen zijn geweest[125] kunnen er slechts *potentiële* dadercategorieën worden beschreven

125 Weliswaar werden er op 11 september 2001 aanslagen gepleegd in de VS met behulp van vliegtuigen en werden er in 2005 aanslagen gepleegd (7 juli) en verijdeld (21 juli) in Londen waarbij het ondergrondse metronet doelwit was, maar aangezien er hier geen sprake was van aanvallen tegen gegevens, informatiesystemen en computerprogramma's (ICT) om de betrokken vitale infrastructuren te ontregelen spreken we in dit rapport niet van cyberterrorisme.

(zie Weimann, 2005). Het kan gaan om politiek gemotiveerde terroristen die ICT als wapen gebruiken tegen vitale infrastructuren of om sympathisanten die hun hackervaardigheden inzetten ten behoeve van terroristen.[126] Het spreekt voor zich dat er bij gebrek aan daders ook (nog) geen daderkenmerken in kaart kunnen worden gebracht. Wat betreft mogelijke aanslagen van terroristen op vitale infrastructuren zijn er volgens het NCTb (2006b: 23) wel indicaties dat de technische competenties van deze potentiële cyberterroristen toeneemt. In aanvulling op bovenstaande verwijzen we voor daderkenmerken naar terroristen (paragraaf 3.2.2) en naar hackers en Critical Information Technology Insiders (CITI's) (paragraaf 3.2.9).

3.2.9 Multifunctionele instrumenten: hacking, malware en dienstverleners

Zoals in hoofdstuk 2 (paragraaf 2.5) al is gebleken, fungeren enkele varianten van computercriminaliteit als multifunctioneel instrument voor meerdere andere verschijningsvormen van high-tech crime. Het gaat in het bijzonder om hacking (botnets), malware in systemen (virussen, wormen, Trojaanse paarden) en om ICT-dienstverleners (corrupt ICT-personeel, infiltratie van criminele ICT'ers en het inhuren van ICT-expertise). In het navolgende evalueren we voor deze drie thema's wat er aan daderkenmerken in de literatuur bekend is.

Hacking
Iedereen die de beschikking heeft over een computer is in principe in staat om andermans computer te hacken doordat veel instrumenten en benodigde software beschikbaar zijn op het internet[127] (Europol, 2003: 73). Er zijn in het verleden meerdere categorisaties gemaakt van subtypen van hackers die allemaal van elkaar verschillen. Zo worden dadertypen onderscheiden naar beschrijvingen van activiteiten (Furnell, 2002), naar motivatie (Furnell, 2002; Turgeman-Goldschmidt, 2005), naar motivatie in combinatie met expertise (bijvoorbeeld Europol, 2003: 83) en naar delictsoort (zie Rogers, 2000). Wellicht de meest uitgebreide daderbeschrijving van delictsoorten betreft de zogenoemde 'Computer Crime Adversarial Matrix' die in 1995 werd ontwikkeld voor de FBI (zie Casey, 2002). Behalve motivatie, persoonlijke kenmerken en kwetsbaarheden (gedrag) en de mate van planning, expertise en gebruikte methoden (uitvoering), categoriseerde men ook de mate van organisatie (rekrutering, internationale connecties) en de benodigde resources (training, materiaal, steun) (zie

126 Weimann categoriseerde ook cyberjoyriders en landen als potentiële cyberterroristen. De activiteiten van cyberjoyriders zijn echter niet politiek gemotiveerd en is dus geen cyberterrorisme, net zo min als landen die ICT inzetten ten behoeve van oorlogsvoering (dit valt onder '*information warfare*').

127 Volgens onderzoek van Europol (pp. 45, 76) waren er in 2003 ongeveer 400.000 websites in de lucht waarin zogenoemde 'would-be hacker tools' werden aangeboden.

bijlage 7). De matrix heeft echter maar betrekking op drie varianten van high-tech crime (hacking/cracking, fraude en spionage) en is inmiddels gedateerd. Uit het FBI-profiel van hackers volgt dat er sprake is van een (tegen)subcultuur van groepen die over de hele wereld contact met elkaar onderhouden. Hackers die niet in groepsverband opereren zijn vaak 'loners' die hacken om de intellectuele uitdaging en zijn vaak lid van een (hacker- of ICT-) tijdschrift of bulletin board. Afgaande op de literatuur kan er globaal een drietal dadertypen worden onderscheiden:
1. de jeugdige crimineel;
2. de ideologische hacker;
3. de financieel gemotiveerde hacker.

Ad 1. De jeugdige crimineel. Uit sommige onderzoeken blijkt dat hacking veelal een mannelijke aangelegenheid is waar veel tieners en jonge volwassenen (tussen de 12 en 28 jaar) zich mee bezighouden (Turgeman-Goldschmidt, 2005; Yar, 2005b). Yar (2005b) spreekt daarom van hacking als een vorm van jeugdcriminaliteit, die vatbaar is voor dezelfde criminologische analyses als andere vormen van delinquentie onder jongeren.[128] Op grond van een fenomenologische studie (ongestructureerde diepte-interviews met 54 Israëlische hackers[129]) concludeerde Turgeman-Goldschmidt (2005: 20) dat hacking doorgaans positief gemotiveerd is. Velen doen het voor de lol, sensatie en uitdaging en daarom wordt het ook wel bestempeld als een nieuwe vorm van entertainment: een sociale activiteit waarbij digitale technologie het spelelement vormt. De zogenoemde 'script kiddies' kraken computers, wissen informatie uit systemen en defacen websites met behulp van door anderen ontwikkelde instrumenten die openlijk verkrijgbaar zijn via het internet. Zij willen indruk maken op vrienden maar beschikken meestal over onvoldoende kennis en vaardigheden om de dramatische gevolgen van hun acties te overzien (Van der Werf, 2003: 26-27). Deze script kiddies kunnen worden vergeleken met vandalistische jongeren '*…die in de fysieke wereld bushokjes slopen of rotzooi trappen op het schoolplein*' (Van der Werf, 2003: 28).[130]

Ad 2. De ideologische hacker. De meeste hackers zijn intelligente mensen met een expliciete behoefte aan kennisverrijking, maar in sommige gevallen betreft het daders die obsessief zijn, antisociaal, met een minderwaardigheidscomplex en mogelijk in hun jeugd fysiek of seksueel mishan-

128 De auteur pleit ervoor criminologische inzichten over jeugddelinquentie te gebruiken bij de analyse van hacking (aspecten als morele ontwikkeling, gezinsproblematiek, sociale beïnvloeding en subculturele groepsvorming).

129 De respondenten (geworven via advertenties, conferenties en computerbedrijven) waren allemaal mannen, met een gemiddelde leeftijd van 24 jaar, de meesten alleenstaand (78%) met een bovengemiddeld inkomen (74%).

130 De hackergemeenschap zelf onderscheidt overigens drie vergelijkbare dadertypen: de '*elite*' (hackers die hun eigen software en instrumenten ontwikkelen), de '*gewone hacker*' (die door anderen ontwikkelde tools gebruikt om te hacken), en de '*darksider*' (die hackt uit winstbejag) (Adamski 1999, aangehaald in Rogers, 2000: 7).

deld (zie Casey, 2002: 551). Op basis van HKS-gegevens over 2001 en 2002 stelde Van der Werf (2003: 29) vast dat hackers weinig gemeenschappelijke kenmerken hebben: het gaat zowel om mannen als vrouwen (met een duidelijke toename van vrouwelijke hackers) en om daders van zowel Nederlandse als niet-Nederlandse afkomst (bijvoorbeeld West-Europa, Suriname en Marokko). De voorlopige onderzoeksbevindingen uit het lopende Hacker's Profiling Project[131] (Biancuzzi, 2006; Chiesa en Ducci, 2006) beschrijven hackers als intelligente mensen met een expliciete behoefte aan kennis, persoonlijke uitdaging en macht en een sterk gevoel voor burgervrijheid.

Ad 3. De financieel gemotiveerde hacker. Hacking is echter in toenemende mate financieel gemotiveerd en bovendien gerelateerd aan andere verschijningsvormen van high-tech crime. Europol (2003: 73) maakt dan ook onderscheid tussen de 'white-hat hacker' (die ideologisch gedreven en nieuwsgierig is en uit op het identificeren van kwetsbaarheden in systemen) en de 'black-hat hacker' (die expliciete criminele bedoelingen heeft en handelt uit winstbejag of wraak).

Algemene daderkenmerken hacking:

Sociaal-demografische kenmerken:
- variabel

(Technische) kennis en vaardigheden:
- variabel

Primaire motivatie:
- hacking als een manier van leven (lol, sensatie, uitdaging, entertainment)
- behoefte aan kennis (nieuwsgierigheid) en voortdurende persoonlijke uitdaging
- macht (aandacht voor politieke en sociale problemen)
- indruk maken op vrienden
- financieel gewin

Sociaal-psychologisch profiel:
- intelligent, creatief en vastbesloten
- sterk gevoel voor burgervrijheid (zet zich af tegen autoriteiten)

Criminele carrière:
- *geen bijzonderheden bekend*

Verschijningsvormen van high-tech crime:
- *geen bijzonderheden bekend*

---

131 De studie bestond uit drie delen: een literatuurinventarisatie, een vragenlijst die hackers konden invullen, en een zogenoemde 'honeypot' om hackeraanvallen te evalueren.

De meest uitgebreide categorisatie van hackers waarin uiteenlopende inzichten over hackers zijn geïntegreerd is de hackertaxonomie van Rogers (2000, 2001, 2006; cf. Furnell, 2002[132]). De hackertaxonomie maakt onderscheid tussen negen verschillende, elkaar niet per definitie uitsluitende, dadercategorieën:

1. *Novices of newbies* (NV), die zich kenmerken door een gebrek aan technische kennis in combinatie met een flinke dadendrang (vergelijkbaar met jeugdbendes).
2. *Cyberpunks* (CP), de zogenoemde 'vandaal-hackers' (waar de meeste studies aan refereren).
3. *Internals* (IT), ontevreden of ex-werknemers of criminelen (waarschijnlijk de grootste dadercategorie in omvang).[133]
4. *Petty thiefs* (PT), die hacken om de lucratieve, criminele mogelijkheden: de klassieke crimineel waarvan de slachtofferdoelgroep zich meer en meer profileert op het internet (bijvoorbeeld banken, creditcardmaatschappijen en naïeve eindgebruikers).
5. *Old guard hackers* (OG), die worden gedreven door intellectuele uitdaging en scripts en codes schrijven voor anderen (gebruiken deze dus niet zelf).
6. *Virus writers of coders* (VW), schrijven scripts en geautomatiseerde tools die door anderen worden gebruikt (fungeren als mentor voor nieuwelingen).
7. *Professional criminals* (PC), onderwereldfiguren met kennis van de laatste snufjes en technieken die niet uit zijn op de roem of reputatie (men wil juist buiten de schijnwerpers blijven en wordt dan ook zelden tot nooit gepakt).
8. *Information warriors* (IW),[134] die politiek vermengen met criminele activiteiten en als werk hebben om de besturingssystemen van vitale infrastructuren te bewaken of aan te kunnen vallen (mogelijk afkomstig van opgeheven intelligence-organisaties uit het Oostblok).
9. *Political activists* (PA), die slechts als *potentiële* negende categorie door Rogers werd toegevoegd.

132 Furnell (2002) onderscheidde acht dadertypen: (a) *'script kiddies'* met beperkte computervaardigheden die voor de lol hacken met andermans tools (cf. de 'novice' NV); (b) '*warez d00dz'* ofwel softwarepiraten die inbreken op systemen (cf. de 'cyberpunk' CP); (c) *'phreakers'* die inbreken op telefoonnetwerken (cf. de 'petty thief' PT); (d) '*schrijvers van malware'* die virussen, wormen en Trojaanse paarden ontwikkelen (cf. de 'virus writer' VW); (e) *'samurais'* die worden ingehuurd voor legale opdrachten, (f) *'cyberwarriors'* die oorlogsaanvallen plegen tegen vitale infrastructuren, en (g) *'cyberterrorists'* die politiek gemotiveerde aanvallen plegen en de sociaal-maatschappelijke agenda willen beïnvloeden (allen vergelijkbaar met de 'information warrior' IW); en (h) *'hacktivists'* die inbreken op systemen en soms websites wijzigen om aandacht te vragen voor de activistische agenda (cf. de 'political activist' PA). In vergelijking tot Rogers (2006) maakte Furnell geen apart onderscheid voor de 'internal', de 'old guard hacker' en de 'professional criminal'.

133 Volgens Power (1997: 9 aangehaald in Rogers, 2000) is 70% van alle computercriminelen een 'internal'.

134 Eerder werd deze categorie door Rogers (2000, 2001) 'cyberterrorists' genoemd.

De professional criminals (PC) en de information warriors (IW) zijn volgens Rogers de meest gevaarlijke daders op het gebied van high-tech crime. Volgens de auteur is het meeste onderzoek dat wordt verricht (en ook de meeste media-aandacht) echter gericht op 'cyberpunks' en is van de overige categorieën (vooral van de 'internals') relatief weinig bekend. Rogers wijst overigens met nadruk op het gevaar van al te snelle generalisaties[135] en het gebruik van daderprofielen in het algemeen. Meer onderzoek is nodig om te bepalen of daderprofielen van high-tech crime überhaupt mogelijk zijn. Aan de hand van de hackertaxonomie van Rogers (2000, 2001, 2006) zijn daderkenmerken samengevat in schema 6 en worden weergegeven met een kruisje (x). Daderkenmerken die aan de hand van overige onderzoeken naar voren zijn gekomen (Casey, 2002; Furnell, 2002; Morris, 2004, Nykodym e.a., 2005) zijn aan het schema toegevoegd en worden weergegeven met een sterretje (*).

Schema 6 Een selectie van daderkenmerken naar verschillende typen hackers

	NV	CP	IT	PT	OG	VW	PC	IW	PA
Sociale demografie									
Leeftijd 12–30 jaar	x	x				x			
'ouder'			*				x		
Middenklassefamilie		x							
Slechte schoolprestaties		x							
Goed opgeleid			*				x	x	
Ontevreden (ex-)werknemer			x						
Technisch beroep			x					x	
Kennis / vaardigheden									
Computervaardigheden (1: beperkt, 3: expert)	1	2	2/3	2	3	3	3	3	
Programmeerervaring (1: toolkit, 3: schrijft zelf)	1	2			3	3	3	3	
Talent voor ICT		x							
Bijnamen uit Science Fiction		x							
Misbruikt privileges			x						
Intelligence-achtergrond								x	
Primaire motivatie									
Sensatie (media-aandacht)	x	x							
Status (zichzelf bewijzen)	x	*				x	-		
Financieel gewin		x	x *	x		*	x	x	
Wraak	*	x	x	x		*			*

135 Zijn onderzoekspopulatie is niet representatief voor de grotere criminele doelgroep van hackers.

Schema 6 (Vervolg)

	NV	CP	IT	PT	OG	VW	PC	IW	PA
Kwaadaardigheid/vandalisme	*	x		*		*			
Macht		x				x			
(Intellectuele) uitdaging		*		*	x	*		*	
Nieuwsgierigheid					x				
Nationalistisch								x	
(Politiek) ideologisch		*						x	x
Sociaal-psychologisch profiel									
Op zichzelf ('loner')		x	*						
Wil ergens bijhoren (virtueel)		x							
Niet op gemak in groep		x							
Ontevreden met zichzelf		x	*						
Niet carrièregericht		x							
Lost problemen op met ICT			*						
Onderdrukte woede		x							
Prikkelbaar, snel gefrustreerd			x						
Schept graag op		x							
Voelt zich achtergesteld			x						
Gebrek aan empathie			x						
Eist speciale behandeling			x						
Sociaal-psychologisch profiel (vervolg)									
Matige sociale vaardigheden			x						
Mentor						x			
Sterk ontwikkeld persoon			*				x		
Criminele carrière									
Crimineel verleden			x	x					
Georganiseerde misdaad							x		
Verschijningsvormen HTC									
dDoS-aanvallen	x								
Malware/Trojaanse paarden		x				x			
Spamming		x							
Defacing		x							
(Identiteits)fraude		x	*	x					
Bedrijfsinformatiesystemen			x						
Creditcardfraude				x					
Spionage						*	x	x	

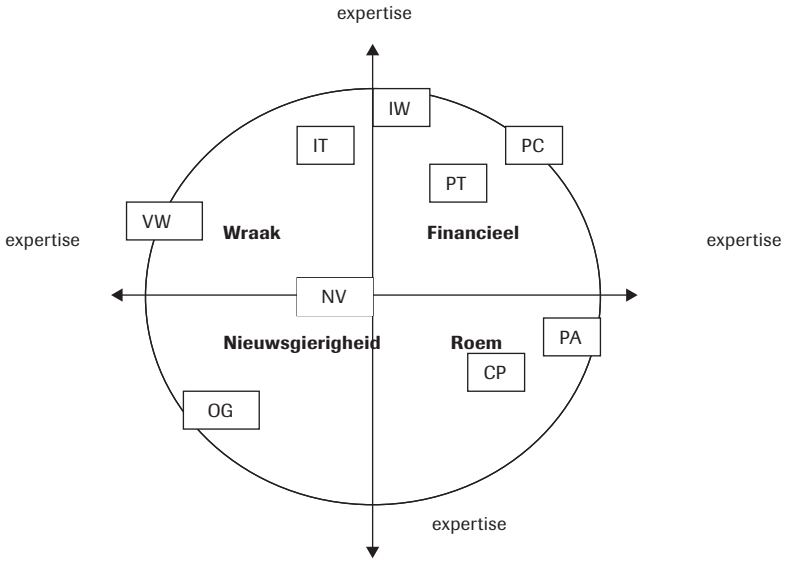
x naar Rogers (2006);

* naar Casey, 2002; Furnell, 2002; Morris, 2004; Nykodym e.a., 2005

De negen dadercategorieën uit de hackertaxonomie kunnen op grond van motivatie en expertise worden ingedeeld in het zogenoemde 'hacker circumplex' (Rogers, 2006): zie schema 7. De belangrijkste motieven worden in vier kwadranten verdeeld:

1. linksboven: wraak (gericht tegen personen, organisaties, landen of werelddelen);
2. rechtsboven: financieel (hebzucht en persoonlijk, financieel gewin);
3. linksonder: nieuwsgierigheid (kennis, sensatie, intellectuele uitdaging);
4. rechtsonder: roem (media-aandacht, opschepperij, volksheld).

Schema 7 Hacker circumplex (Rogers, 2006)



De mate van technische expertise en ICT-vaardigheden van daders zijn af te lezen op de assen. Dat wil zeggen, naarmate een dader over meer expertise en vaardigheden beschikt, zal deze meer aan de uiterste zijden van de circumplex (buitenste assen) worden gepositioneerd. Uit schema 7 is bijvoorbeeld af te lezen dat 'information warriors' (IW) niet alleen over veel technische expertise en vaardigheden beschikken (buitenste as van het circumplex), maar ook dat zij sterk financieel gemotiveerd zijn en deels mogelijk opereren uit wraak. De 'novices' (NV) daarentegen, zijn technisch minder vaardig (binnenste as van het circumplex) en worden veelal gemotiveerd door nieuwsgierigheid. Het gaat in het circumplex vooral om de relatieve positie van hackers ten opzichte van elkaar: dadercategorieën die nauw aan elkaar verwant zijn (bijvoorbeeld de PT: 'petty thiefs' en de PC: 'professional criminals') staan in het circumplex dichter bij elkaar. Dit geldt ook omgekeerd: categorieën die niet aan elkaar

gerelateerd zijn (dat wil zeggen met negatieve samenhang) staan juist tegenover elkaar in het circumplex (zoals de PC: 'professional criminals' en de OG: 'old guard hackers'). Volgens Rogers (2006) vormt de circumplex een basisinstrument voor het in kaart brengen van daderprofielen (de '*psychological crime scene analysis*'[136]). Op grond van verschuivingen in motivatie en vaardigheden zijn ook criminele carrières van hackers in kaart te brengen via het circumplex. Bij gebrek aan datamateriaal is deze indeling (zowel het circumplex als de hackercategorieën in het algemeen) echter nog niet empirisch gevalideerd. Het model van Rogers (2006) blijft dus hypothetisch en vereist nadere empirische toetsing en ontwikkeling.

Eén categorie spionnen die door Morris wordt aangehaald (2004) komt binnen de taxonomie van Rogers (2000, 2001, 2006) minder goed tot zijn recht: de bedrijfsspion. Hoewel de bedrijfsspion gelijkenis vertoont met de wraakzuchtige 'internal' (beiden opereren van binnenuit de organisatie) bezit de bedrijfsspion andere kenmerken. Bedrijfsspionage wordt gepleegd door insiders of met hulp van binnenuit (zie ook corruptie ICT-personeel) en de daders zijn doorgaans zo ICT-vaardig dat zij niet kunnen worden getraceerd. Zij hebben een sterke criminele motivatie en worden bovendien zeer goed betaald. Juist deze mensen vormen volgens Europol (2003: 79) ook een bedreiging voor aanvallen op vitale infrastructuren. Werknemers die het beste gepositioneerd zijn om gevoelige en vertrouwelijke bedrijfsinformatie te verzamelen hebben volgens Nykodym en anderen (2005) een hogere positie in het bedrijf (bijvoorbeeld binnen het managementteam). Op grond van hun functieprofiel zijn zij naar verwachting dus wat ouder (tussen de 30 en 60 jaar).[137] Naar waarschijnlijkheid gaat het om een onopvallend figuur (geen extreme uitspraken of uiterlijke vertoning), die zich graag mengt in gezelschap, rustig en geheimzinnig is, met flink wat kennis op het gebied van ICT en ook in staat is om digitale sporen te wissen. Deze beschrijving is echter niet op empirisch materiaal gebaseerd en dient met enige voorzichtigheid te worden geïnterpreteerd.

Malware in systemen (virussen, wormen, Trojaanse paarden)
Ook schrijvers van malware zijn een belangrijke groep daders omdat zij meerdere verschijningsvormen van high-tech crime faciliteren (zie bijvoorbeeld schema 3 van hoofdstuk 2). Bij deze categorie computercriminelen is op basis van de literatuur echter niet eenduidig vast te stellen of de ontwikkelaars van malware zelf ook daadwerkelijk kwaadaardige aan-

136 Aan de hand van '*salient case points*' wordt informatie in kaart gebracht (bijvoorbeeld over de digitale kenmerken: gebruikte methoden, sporen, het soort data of systeem waarop de misdaad gericht was, de mate waarin onnodige schade aan data en systemen is aangericht) en aan de hand daarvan kan een 'quick scan' van de dadercategorie worden gedaan in de circumplex.

137 Van saboteurs van binnen het bedrijf (wraakzuchtige werknemers die uit wraak handelen omdat zij bijvoorbeeld een promotie misliepen) wordt juist verwacht dat ze wat jonger zijn (tussen de 25 en 40 jaar).

vallen plegen op ICT om storingen te veroorzaken. Binnen de hackercategorisatie van Rogers (2006) kan de aanvaller in principe een novice (NV) zijn, een cyberpunk (CP)[138] of een petty thief (PT), terwijl de instrumenten die zij gebruiken worden ontwikkeld door bijvoorbeeld old guard hackers (OG) of virus writers (VW). Rogers (2000, 2001, 2006) benadrukte al dat er relatief weinig bekend is van deze dadergroep en dat beduidend meer onderzoek nodig is.

ICT-dienstverleners
Ook dienstverleners van high-tech crime kunnen en worden voor meerdere criminele delicten ingeschakeld. In hoofdstuk 2 werden drie typen dienstverleners onderscheiden, namelijk de corrupte ICT'ers (die misbruik maken van bevoegdheden ten behoeve van anderen om persoonlijk voordeel te halen), de ICT-infiltranten (die crimineel zijn maar zich laten inhuren als IT-professional of consultant), en de IT-experts die zich (al dan niet betaald) laten inhuren door de georganiseerde misdaad Uit onderzoek van Ernst en Young uit 2000 (aangehaald door Europol, 2003: 81) bleek dat 82% van alle fraude-incidenten binnen bedrijven was toe te schrijven aan eigen werknemers. In bijna een derde van de gevallen betrof het leden van het eigen management. Over de kenmerken en achtergronden van *corrupt ICT-personeel* ('internals' volgens de hackertaxonomie van Rogers: zie voor een beschrijving schema 6) is relatief weinig bekend. Daders kunnen door hebzucht en financieel gewin worden gemotiveerd (bijvoorbeeld in het geval van fraude) of handelen uit persoonlijke motieven (bijvoorbeeld door schulden, relatieproblemen of wrok tegen de leiding van een bedrijf) (zie ook schema 6) (Boerman en Mooij, 2006: 50-51; Ernst en Young, aangehaald door Europol, 2003: 81-82; Shaw, 2006). In een recent rapport van het KLPD/DNRI (2007c: 5-6) werd geconcludeerd dat er geen daderprofiel van corrupte ICT'ers kan worden geschetst omdat daders weinig gemeenschappelijke kenmerken hebben. Uit onderzoek blijkt wel dat wraakzuchtige werknemers vaak mannen zijn[139] waarvan 25% tot 33% ook een strafblad heeft (op het gebied van geweld, verdovende middelen en diefstal) (KLPD/DNRI, 2007c; Rogers, 2006; Shaw, 2006).

De laatste jaren zijn de activiteiten van 'cyberprofiling' ook gericht op de 'Critical Information Technology Insiders' (CITI's),[140] ofwel individuen die vitale infrastructuren bedreigen van binnenuit (zie Casey, 2002). Deze groep daders heeft volgens Casey[141] als gemeenschappelijk kenmerk dat ze introvert zijn en weinig geneigd om op een constructieve wijze steun te

138 Zo bleek het bekende Anna Kournikova-virus, dat wereldwijd behoorlijk wat schade aanrichtte, bijvoorbeeld afkomstig van een 20-jarige jongen uit Sneek (Alberdingk Thijm, 2007).
139 Dit kan echter een artefact zijn van het gegeven dat de IT-sector nog overwegend een 'mannenberoep' is.
140 Deze daders zijn niet politiek gemotiveerd en vallen volgens de gehanteerde definities in dit rapport niet onder cyberterrorisme.
141 Casey (2002) baseert zich op onderzoek van onder andere Shaw, Ruby en Post (1998) die kenmerken afleidden uit case studies en vragenlijstonderzoek (zie ook www.pol-psych.com/sab.pdf).

zoeken als men onder druk komt te staan (zo vraagt men bijvoorbeeld niet snel om hulp en is men geneigd om problemen eerder via de e-mail dan face-to-face aan te kaarten). Hun voorgeschiedenis kenmerkt zich door persoonlijke en sociale frustraties, computerafhankelijkheid, verminderde loyaliteit, gebrek aan empathie (naar het slachtoffer), en narcistische trekken (de overtuiging dat men speciale erkenning verdient bij gebrek waarvan men sterke wraakgevoelens ervaart). Voor zover deze daderkenmerken nog niet in schema 6 waren opgenomen voor de 'internal hacker' van Rogers zijn deze toegevoegd (met een *).

Specifieke daderkenmerken van criminele *ICT-infiltranten* of *IT-experts* die zich laten inhuren door de georganiseerde misdaad (zie ook hoofdstuk 4) is in de literatuur niets bekend. Volgens de hackertypologie van Rogers (2006) kan het in beide gevallen gaan om een 'professional criminal' (PC) en om 'virus writers' (VW) of 'information warriors' (IW) (zie schema 6).

3.3 Implicaties voor beleid en praktijk

In het voorgaande zijn voor een aantal verschijningsvormen van high-tech crime afzonderlijk enkele daderkenmerken in kaart gebracht. Door deze in samenhang weer te geven ontstaat inzicht in de relatie tussen daders en verschillende verschijningsvormen van high-tech crime. Een dergelijk overzicht zou het begin kunnen zijn van een risicoprofiel en biedt aanknopingspunten voor de bestrijding (preventie en opsporing) van high-tech crime. Zo kunnen bijvoorbeeld patronen worden blootgelegd die door hun overlap aanwijzing kunnen zijn dat verschillende delicten door dezelfde (type) dader wordt gepleegd. Overlap in de benodigde technieken en vaardigheden voor het plegen van bepaalde delicten kan ook inzicht bieden in de mate waarin dienstverleners door criminelen kunnen worden ingeschakeld. Meer in zijn algemeenheid worden vooral lacunes zichtbaar in de bestaande kennis over daders en verschijningsvormen van high-tech crime.

In schema 8 staat ter illustratie (op grond van eerdere bevindingen uit dit hoofdstuk) een *selectie* van daderkenmerken weergegeven. Onder 'diversificatie' staat bovenin het schema de overlap tussen de verschillende verschijningsvormen (de niet-geprioriteerde thema's uit bijlage 6 staan schuingedrukt). Zo is direct te zien dat met name internetfraude en hacking veelal in combinatie met andere vormen van high-tech crime worden gepleegd. Ook toegepaste technieken en de sociaal-demografische, kennistechnische, motivationele en criminele antecedenten van daders staan in het schema weergegeven. Aan de hand daarvan zien we bijvoorbeeld dat terrorisme, kinderporno, grooming, softwarepiraterij en internetfraude vooral een mannelijke aangelegenheid zijn en dat

met name hackers, schrijvers van malware en ICT-dienstverleners over geavanceerde expertise (programmeerervaring) beschikken. Piraten en internetfraudeurs blijken (samen met hackers, schrijvers van malware, corrupte ICT'ers en in te huren IT-experts) vooral financieel gemotiveerd (hoewel hackers en schrijvers van malware, en in mindere mate ook corrupte ICT'ers, andere motieven kunnen hebben). En de criminelen die actief zijn op het gebied van terrorisme, internetfraude en hacking, alsook daders van kinderporno en corrupte ICT'ers blijken nogal eens over een strafblad te beschikken.

Opvallend is dat daders die betrokken zijn bij terroristische activiteiten, internetfraude en hacking ook geassocieerd worden met creditcardfraude. Mogelijk zijn de daaraan verwante delicten gerelateerd aan het hebben van een strafblad Een logische vraag zou vervolgens zijn: 'wat hebben deze daders verder met elkaar gemeen?' en 'is het bijvoorbeeld mogelijk dat het om dezelfde dader(categorieën) gaat?'. Wat zijn überhaupt opvallende persoonskenmerken die iemand mogelijk tot een risico maken voor het plegen van high-tech crime? Dergelijke vragen kunnen aan de hand van risico-indicatoren en profielen worden beantwoord. Daarmee ontstaat meer inzicht in het fenomeen high-tech crime en worden in potentie aanknopingspunten geboden ten behoeve van zowel de preventie (risicogroepen) als de opsporing en vervolging van high-tech crime.

Schema 8 Selectie van daderkenmerken voor geprioriteerde thema's van high-tech crime

	Radicalisering	Terrorisme	Kinderporno	Grooming	Softwarepiraterij	Internetfraude	Witwassen	Cyberterrorisme	Hacking	Malware	Corrupte ICT'ers	ICT-infiltranten	Inhuur expertise
Diversificatie													
Radicalisering													
Terrorisme	x												
Kinderporno													
Grooming													
Softwarepiraterij													
Internetfraude		x											
Witwassen						x							
Cyberterrorisme													
Hacking					x	x		?					
Malware						x		?	x				
Corrupte ICT'ers					x	x		?					
ICT-infiltranten								?		x			
Inhuur expertise		x				?		?	x	x			

Schema 8 (Vervolg)

	Radicalisering	Terrorisme	Kinderporno	Grooming	Softwarepiraterij	Internetfraude	Witwassen	Cyberterrorisme	Hacking	Malware	Corrupte ICT'ers	ICT-infiltranten	Inhuur expertise
Propaganda	x												
Creditcardfraude		x				x			x				
dDoS-aanval						x			x				
Defacing / pharming						x			x				
Cyberstalking				x									
Spionage										x		x	x
Technieken													
Afscherming			x										
Spamming						x							
Botnets						x			x				
Social engineering						x							
Professionaliteit						x							
Sociale demografie													
Man		x	x	x	x	x							
< 20 jaar	x	x											
< 40 jaar		x	x										
Etnische achtergrond*		2,3	1	1		x							
Kennis/vaardigheden													
Virtueel actief	x	x	x	x					x				
Computerervaring			x		x				x	x	x	x	x
Programmeerervaring									x	x	x	x	x
Primaire motieven													
Uitdaging									x	x			
Ideologie	x	x							x				
Frustratie/wraak	x	x							x	x	x		
Seksuele stimulatie			x	x									
Macht			x						x	x			
Financieel gewin					x	x			x	x	x		x
Vandalisme									x				
Criminele carrière													
Strafblad		x	x			x			x		x		
Georganiseerde misdaad			x			x			x				

* 1 = blank; 2 = Afrikaans; 3 = Aziatisch

Schema 8 fungeert hier slechts als voorbeeld op een selectie van gegevens. In navolging van de 'Computer Crime Adversarial Matrix' van de FBI (zie Casey, 2002) kunnen standaardindicatoren zoals gedrag (motivatie, persoonlijke kenmerken en kwetsbaarheden), uitvoering (de mate van planning, expertise en gebruikte methoden), organisatie (rekrutering, internationale connecties), en resources (training, materiaal, steun) in een dergelijk schema worden opgenomen (zie ook bijlage 7). Het strekt tot aanbeveling om een dergelijk 'intelligence'-systeem en database te ontwikkelen en te toetsen naar bruikbaarheid.

Concluderend moeten we aan de hand van deze inventarisatiestudie constateren dat er weinig bekend is in de literatuur over individuele daders van high-tech crime. Informatie ontbreekt in zijn geheel over dierenrechtenactivisten, extreem-rechtse terroristen, overgebruikers (bedrijven) en illegale handelaren van softwarepiraterij, witwassen (in de *e*- en *m*-commerce) en cyberterroristen. In het laatste geval ligt de oorzaak erin dat er nog geen daadwerkelijke politiek gemotiveerde, cyberterroristische aanvallen zijn gepleegd. Studies rond drijfveren van plegers van piraterij leunen sterk op onderzoek onder studenten. Over hackers is meer geschreven maar dit beperkt zich vooral tot de categorie cyberpunks (of scriptkiddies). Vooral waar het gaat om hacking in relatie tot de schrijvers van malware en dienstverleners (corrupt personeel, CITI's, ICT-infiltranten en in te huren IT-experts) is meer kennis over daders wenselijk te noemen. Van sommige (maar niet alle) radicale en terroristische stromingen, alsook cyberpunk hackers (script kiddies) en daders van voorschotfraude is relatief het meeste bekend, maar ook daarvoor geldt dat de informatie over daders tamelijk ongestructureerd en summier is. Bovendien is dit deels gebaseerd op anekdotisch materiaal en/of hypothesen. In zijn algemeenheid ontbreekt voor vele verschijningsvormen het inzicht in de criminele carrières van de daders en de overlap tussen de verschillende verschijningsvormen van high-tech crime. Een literatuurinventarisatie als deze volstaat niet om daderkenmerken in enig detail in beeld te krijgen. Er zijn echter alternatieve onderzoeksmogelijkheden denkbaar (bijvoorbeeld onderzoek op politie- en strafdossiers) die aanvullende inzichten kunnen opleveren. Nader onderzoek naar de verschillende verschijningsvormen van high-tech crime is dus nodig. In het volgende hoofdstuk evalueren we aan de hand van de literatuur in hoeverre de georganiseerde misdaad betrokken is bij de geprioriteerde thema's van high-tech crime (voor de niet-geprioriteerde thema's verwijzen we naar bijlage 6).

4 Georganiseerde high-tech crime

Tot nog toe is in dit rapport een inventarisatie gemaakt van wat er in de (inter)nationale literatuur bekend is over individuele daders van high-tech crime (en wat de lacunes zijn in die kennis over daders). Daders van high-tech crime werken echter niet altijd op eigen houtje en spannen/werken soms samen met anderen binnen een crimineel samenwerkingsverband (CSV). We besteden in dit hoofdstuk om twee redenen afzonderlijk aandacht aan de betrokkenheid van de georganiseerde misdaad bij high-tech crime. Ten eerste hoeven de risicoprofielen van individuele daders niet zonder meer gelijk te zijn aan de risicoprofielen van individuen die in groepsverband opereren, en ten tweede is er bij groepen bovendien sprake van overstijgende groepskenmerken die in kaart kunnen worden gebracht. In het navolgende evalueren we op basis van de literatuur of en in hoeverre sprake is van georganiseerde misdaad bij high-tech crime.[142] Wanneer de georganiseerde misdaad specifiek *in relatie* wordt gebracht met high-tech crime, gebruiken we in dit rapport de term 'high-tech criminele samenwerkingsverbanden' (hierna: HT-CSV's). Voor de traditionele georganiseerde misdaad *in het algemeen* spreken we in dit rapport van 'georganiseerde misdaad' of 'criminele samenwerkingsverbanden' (hierna: CSV's).

4.1 Georganiseerde misdaad of online criminelen?

De georganiseerde misdaad in Nederland vormt een aantasting van collectieve belangen en gaat gepaard met grote financiële belangen, economische macht, maar ook geweld (bijvoorbeeld liquidaties) en corruptie (OM, 2007b). De bestrijding van georganiseerde misdaad is belegd bij het Landelijk Parket van het OM. We spreken in dit rapport van georganiseerde criminaliteit als: '*…groepen primair gericht zijn op illegaal [financieel of materieel] gewin en systematisch misdaden plegen met ernstige gevolgen voor de samenleving*' (Parlementaire Enquêtecommissie Opsporingsmethoden, Bijlage VII, 1996; Fijnaut e.a., 1998; Kleemans e.a., 1998: 22-23). In het NDB2004[143] (p. 44) werd geconcludeerd dat de traditionele CSV's in Nederland in beperkte mate betrokken zijn bij high-tech crime en dat dit te maken heeft met een relatief gebrek aan kennis en expertise: ICT wordt vooral gebruikt als communicatie- en afschermingsmiddel. Volgens Nederlandse experts behoort high-tech crime echter wel tot de top 10 van criminele verschijnselen in de zware of georganiseerde criminaliteit (KLPD, DNRI, 2004: 186). McAfee (2006: 9) omschrijft high-tech crime zelfs als een lucratievere business dan de traditionele vormen van georganiseerde misdaad, omdat de opbrengsten (afgezet tegen de beperkte investeringen en risico's) flink kunnen oplopen. Het exploiteren

142 Voor de niet-geprioriteerde thema's verwijzen we naar bijlage 6.
143 Waarin dreigingsanalyses werden gemaakt van de zware of georganiseerde criminaliteit voor de Nederlandse samenleving over de periode 2004-2009.

van een commerciële website met kinderporno levert (omgerekend) bijvoorbeeld al gauw ruim 1 miljoen euro per maand op (Alexy e.a., 2005).

Een belangrijke vraag is dan ook of traditionele CSV's hun activiteiten inmiddels hebben verlegd naar het terrein van high-tech crime, of dat er sprake is van een nieuwe lichting 'online criminelen' die om praktische redenen min of meer toevallig met elkaar samenwerken. Dit onderscheid is volgens McCusker (2006: 261) fundamenteel. Van HT-CSV's wordt verondersteld dat zij wisselen van samenstelling en vluchtig (eenmalig) zijn. Het KLPD (KLPD, DNRI, 2007b: 14-15) spreekt ook wel van '*…een netwerk waarin criminele projecten worden uitgevoerd*'. Doordat contacten vooral online plaatsvinden, blijft de identiteit van daders onderling verborgen en is er niet of nauwelijks sprake van een sociale (vertrouwens)basis en het uitvoeren van interne sancties. De beschikbare 'phishing kits' en mogelijke inhuur van dienstverleners maken in principe ook geen omvangrijke HT-CSV's noodzakelijk (KLPD/DNRI, 2007a). De gedachte is daarom dat HT-CSV's net zo snel worden beëindigd als zij worden opgestart.

Voor het KLPD is er sprake van georganiseerde criminaliteit wanneer een *'meer dan eenmalige samenwerking van drie of meer personen probeert gezamenlijk gewin te behalen met ernstige gevolgen voor de Nederlandse samenleving'* (Boerman en Mooij, 2006: 13-15). Volgens de WODC-monitor Georganiseerde Criminaliteit (Kleemans e.a., 2002; Van de Bunt en Kleemans, 2007) kenmerkt de traditionele georganiseerde misdaad zich tegenwoordig echter juist door 'fluïde' en dynamische CSV's die aan verandering onderhevig zijn. Dit betekent dat er niet altijd sprake hoeft te zijn van een 'meer dan eenmalige samenwerking' en in die zin vormen de online criminelen van McCusker (de HT-CSV's) daarop dus geen uitzondering. In een recente interne rapportage (over identiteitsfraude met behulp van phishing) erkent het KLPD/DNRI (2007a: 39, 57) dat het lastig is te bepalen in hoeverre daadwerkelijk sprake is van HT-CSV's. Het zicht op daders is namelijk relatief beperkt en een meer dan eenmalige samenwerking tussen drie of meer personen is empirisch vaak moeilijk aantoonbaar. De Raad van Europa (aangehaald door Gordon en Ford, 2006: 259) concludeerde in 2004 ook al dat er te weinig gegevens beschikbaar zijn om op een betrouwbare manier een relatie te kunnen leggen tussen georganiseerde misdaad en high-tech crime (HT-CSV's). Volgens een eerder verschenen Europol-rapport (2003: 109) zou alleen het Verenigd Koninkrijk actief zijn geweest op het gebied van intelligence met betrekking tot HT-CSV's.

In de geraadpleegde literatuur bleek ook weinig te vinden over HT-CSV's. Volgens Fisher (aangehaald door McCusker, 2006: 271) is sprake van zowel traditionele CSV's (zoals de Russische en Oost-Europese maffia die expertise inhuren of afdwingen), als nieuwe fluïde HT-CSV's waarbinnen

experts (bijvoorbeeld hackers en schrijvers van malware) hun krachten bundelen voor het plegen van high-tech crime. Ondanks dat de kenmerken van deze groepen (en betrokken individuen) mogelijkerwijs van elkaar verschillen,[144] spreken we in beide gevallen van HT-CSV's. McCusker (2006: 268) waarschuwt dat de literatuur over HT-CSV's soms deels gebaseerd is op logisch redeneren, hypothesen, veronderstellingen en anekdotische verhalen (die auteurs bovendien van elkaar overnemen). Er is in veel gevallen dus (nog) geen empirische ondersteuning, wat betekent dat er nader onderzoek nodig is.

High-tech crime is door zijn virtuele kenmerken een grensoverschrijdende vorm van criminaliteit. HT-CSV's blijken doorgaans dan ook internationaal georganiseerd te zijn (McAfee, 2006: 17). Volgens de politie zijn er in ieder geval aanwijzingen dat Russische en Oost-Europese HT-CSV's betrokken zijn bij dDoS-aanvallen en afpersing van online goksites en andere e-commerce-websites (zie ook bijlage 6) (Europol, 2003: 125; Walker, 2004). De grotere criminelen opereren vooral vanuit landen waar weinig bronnen worden ingezet in het kader van opsporing en vervolging van high-tech crime (bijvoorbeeld ontwikkelingslanden) (Europol, 2003: 37). Op basis van gegevens van de Raad van Europa (2004), de Canadese criminele inlichtingendiensten (CISC), de FBI en dreigingsanalyses uit 2006 over de georganiseerde misdaad in de Verenigde Staten en Canada,[145] concludeerde McCusker (2006) dat er HT-CSV's actief zijn bij verschillende vormen van cyber- en computercriminaliteit: afschermingstechnieken (bijvoorbeeld ten behoeve van de drugshandel), internet- en identiteitsfraude, softwarepiraterij, spionage, afpersing, witwassen, handel in kinderporno, hacking, defacing van websites, en botnets. De handel in botnets lijkt daarbij een aparte handelsindustrie te worden waar de georganiseerde misdaad bij wijze van spreken 'grootafnemer' is (Hynds 2005, aangehaald door McCusker, 2006: 270). In de volgende paragraaf evalueren we voor de geprioriteerde verschijningsvormen van high-tech crime wat er in de literatuur bekend is over HT-CSV's.

4.2 Inzichten in criminele samenwerkingsverbanden

4.2.1 Radicalisering

De AIVD (2004) beschrijft radicalisering als een groepsproces waarbij sprake is van wederzijdse sociale beïnvloeding binnen los-vaste (fluïde) netwerken. De netwerken professionaliseren zich in toenemende mate

144 Onderzoek daarnaar ontbreekt tot op heden.
145 Hoewel de gegevens verwijzen naar officiële bronnen is op basis van deze studie geen toetsing mogelijk op empirische houdbaarheid.

en acties vinden plaats in georganiseerd (inter)nationaal verband. Van de afzonderlijke stromingen (zie ook bijlage 4) zijn echter geen concrete literatuurstudies bekend waarin expliciet wordt ingegaan op kenmerken of profielen van dergelijke HT-CSV's.

4.2.2 Terrorisme en ideologisch gemotiveerde misdaad

Onderzoek naar terroristische of ideologisch gemotiveerde HT-CSV's heeft zich vooral gericht op het islamistisch terrorisme (zie ook bijlage 5). Uit de literatuur blijkt dat islamistische netwerken heterogeen zijn en zich niet laten kenmerken door een typisch profiel. Tussen de groepsleden onderling is wel sprake van homogeniteit in leeftijd, woonplaats en nationaliteit: men komt ook vooral via sociale affiliatie (vrienden, familie) met elkaar in contact (Bakker, 2006).[146] Onderzoek van het KLPD heeft geen aanwijzingen opgeleverd van samenwerking tussen criminele en terroristische CSV's (Boerman en Mooij, 2006: 86). Wel zijn terroristische CSV's betrokken bij diverse criminele activiteiten om het terrorisme mee te financieren. De grotere CSV's (met internationale connecties) zijn betrokken bij de handel in verdovende middelen, afpersing en mensensmokkel. De losser georganiseerde, lokale netwerken (van eigen bodem) houden zich op kleinere schaal bezig met paspoortfraude, inbraak en diefstal. Uit de literatuur blijkt echter niet dat dit ook zou gelden voor HT-CSV's.

4.2.3 Kinderporno

Wat betreft de handel en productie in kinderporno is sprake van virtuele pedofiele georganiseerde groeperingen en in toenemende mate betrokkenheid van HT-CSV's die afkomstig zijn uit Rusland en Oost-Europa (KLPD, DNRI, 2004: 116-117; Lunnemann e.a., 2006: 108-109; McCusker, 2006; Van der Werf, 2003: 43-48). Voor de georganiseerde misdaad is het een lucratieve business waarin veel geld te verdienen is: kinderpornosites kunnen miljoenen opbrengen (NDB2004). Specifieke informatie is in de literatuur echter niet te vinden.

4.2.4 Grooming

De aard van de activiteiten van grooming, waarbij kinderen via chatsites seksueel worden benaderd door volwassenen, wordt niet aangemerkt als vorm van georganiseerde misdaad: men is immers ook niet uit op illegaal, financieel of materieel gewin.

146 De NCTb zal naar verwachting in het voorjaar van 2008 een onderzoeksrapport uitbrengen waarin meer kenmerken van islamistische netwerken worden beschreven.

4.2.5 Softwarepiraterij

Van daders van softwarepiraterij blijkt uit onderzoek dat zij sterk zijn georganiseerd en er zijn aanwijzingen dat dit gepaard gaat met drugshandel (Europol, 2003: 36-37; McCusker, 2006). Volgens door het KLPD geïnterviewde experts zijn hierbij soms HT-CSV's betrokken, met name bij de meer traditionele vormen van muziekpiraterij (illegale kopieën van cd's) (Neve, 2007). In Italië zou de maffia zich hiermee bezighouden, waarbij bedreiging met geweld (om tegenstanders in toom te houden) niet wordt geschuwd. In Nederland is een Turks HT-CSV actief met een soort cd-bladenmap (illegale verzamelalbums) waarop mensen zich kunnen abonneren (Stichting Brein, 2007; Neve, 2007). Deze verzamelalbums worden professioneel gemastered en geperst op cd of dvd en het uiterlijk van deze producten is kwalitatief vaak zeer goed.[147] Vooral in Aziatische en Oost-Europese landen worden op grote schaal kopieën van muziek, films en software geperst in illegale fabrieken.

4.2.6 Internetfraude

In Nederland zijn er HT-CSV's actief op het gebied van internetfraude, diefstal en oplichting. Ook McCusker (2006) concludeerde op basis van verschillende bronnen dat er sprake is van georganiseerde criminele activiteiten met betrekking tot internetfraude. Uit onderzoek van Van der Werf (2003: 37) blijkt dat er echter weinig zicht is op de specifieke kenmerken van daders die hierbij betrokken zijn. Wat is er nu vanuit de literatuur bekend over HT-CSV's van voorschotfraude en identiteitsfraude?

Voorschotfraude
Bij de Nigeriaanse voorschotfraude gaat het om professionele daders die in groepsverband opereren, deel uitmaken van een wereldwijd (crimineel) netwerk, en veelal aangestuurd worden vanuit Nigeria. In sommige gevallen wordt gebruikgemaakt van acteurs om zo professioneel mogelijk over te komen. Het betreft zware criminaliteit waarbij soms ook echte ontmoetingen worden geregeld, die gevaar van ontvoering of zelfs moord met zich mee brengen. In Amsterdam waren in 2002 zo'n zes à zeven HT-CSV's operationeel die zich, naast fraude, ook bezighielden met onder meer vrouwenhandel, verdovende middelen en geweldsmisdrijven (Van der Werf, 2003: 36-37). Er zijn recentelijk meerdere opsporingsactiviteiten geweest op dit gebied waarvan nog geen bronnen te raadplegen zijn.

147 Dit in tegenstelling tot dat van individuele hobbyisten die bijvoorbeeld een kopietje maken van een bestaand hoesje.

Identiteitsfraude
Uit onderzoek van de FBI is gebleken dat de laatste jaren vooral drugsdealers zich steeds meer zijn gaan richten op identiteitsfraude. De verdiensten ervan zijn nagenoeg gelijk aan die in de drugshandel terwijl de risico's (mate van geweld, de pakkans en de strafmaat) van identiteitsfraude een stuk geringer zijn. Zo worden bijvoorbeeld creditcardgegevens verzameld en gebruikt voor het maken van nepkaarten waarmee straatdealers goederen aankopen (voor bedragen beneden de 200 dollar per persoon). Deze goederen worden vervolgens via veilingwebsites weer doorverkocht en op die manier worden de winsten gemaakt (Security.nl, 25 april 2007). Volgens Europol (2003: 29) is nader onderzoek nodig naar de relatie tussen identiteitsfraude en HT-CSV's, vooral in relatie tot mensenhandel en creditcardfraude. Het gebrek aan zicht op daders en HT-CSV's wordt ook door een recent onderzoek naar identiteitsfraude bevestigd (KLPD, DNRI, 2007a).

Een variant op identiteitsfraude met behulp van phishing is *pharming*, waarbij bezoekers van websites op slinkse wijze worden omgeleid naar een nepwebsite. Internetgebruikers laten daar gegevens achter die naderhand worden misbruikt (zie ook identiteitsfraude). Er zijn aanwijzingen dat HT-CSV's actief zijn op dit vlak. Zo werd in oktober 2000 een initiatief verijdeld waarbij een 'digitale kloon' van de Bank of Sicily een EU-subsidie van 400 miljoen Amerikaanse dollars had moeten confisceren. Het ging om een groep van twintig verdachten waarvan sommigen directe contacten hadden met verschillende Italiaanse maffiafamilies en er in ieder geval een bankmedewerker betrokken was (Williams, 2001). Aan concrete studies die zicht geven in daderkenmerken en HT-CSV's ontbeert het echter (zoals dat overigens opgaat voor vele andere verschijningsvormen van high-tech crime).

4.2.7 Witwassen

Witwassen is onlosmakelijk verbonden met traditionele vormen van georganiseerde criminaliteit (bijvoorbeeld drugshandel) waarbij onder- en bovenwereld nauw met elkaar zijn verweven. Met de komst van het internet is witwassen bovendien een stuk gemakkelijker geworden. Grote geldstromen zijn door internetbankieren, e-commerce en online veilingen redelijk ontraceerbaar geworden en er wordt dan ook een toename verwacht van deze vorm van criminaliteit (Williams, 2001). In de geraadpleegde literatuur zijn, met uitzondering van de door McCusker (2006) geraadpleegde bronnen (paragraaf 4.1), echter geen aanwijzingen te vinden op het gebied van specifieke HT-CSV's met betrekking tot witwaspraktijken. Wel zijn er aanwijzingen uit de media dat de Russische maffia zou zijn geïnfiltreerd in bijvoorbeeld het Amerikaanse bankwezen om hun witwaspraktijken, waarmee biljoenen dollars gemoeid zijn,

te verwezenlijken (Walker, 2004: 2). Onderzoeksverslaggever Walker beschrijft een grote witwasoperatie in de VS waarbij een Russisch samenwerkingsverband voor miljarden Amerikaanse dollars witwaste. Bij het complot waren volgens Walker twee hooggeplaatste bankfunctionarissen van Russische afkomst betrokken.

4.2.8 Cyberterrorisme

Van cyberterrorisme in relatie tot HT-CSV's is in de literatuur geen informatie beschikbaar.

4.2.9 Hacking en malware

Hacking is in steeds grotere mate georganiseerd. Wat kan beginnen als een soort virtuele gemeenschap van mensen met gedeelde interesses en belangen, kan al gauw escaleren tot een vorm van georganiseerde misdaad (Europol, 2003: 72). Europol en Olson (2006, aangehaald door McCusker: 265-266) benadrukken dat de 'ondergrondse cultuur' van hackers uitstekend past binnen het ondergrondse netwerk van de traditionele georganiseerde criminaliteit. Verschillende bronnen en geïnterviewde deskundigen geven ook aan dat er in het hacken en het ontwikkelen van malware sprake is van een ontwikkeling naar wat McAfee (2006) noemt 'cybergangs'. Ook jongeren raken in toenemende mate betrokken bij HT-CSV's die gericht zijn op het hacken van systemen. Het gaat hier veelal om diefstal van gegevens met als doel afpersing en oplichting (Europol, 2003: 76; Van der Werf, 2003: 30).

Bij onvoldoende beveiligde banksystemen is het echter ook mogelijk gebleken om hele geldstromen met behulp van hacking te veranderen. Zo kraakte een jonge Russische hacker in 1994 de computersystemen van de Citi Bank in Boston en realiseerde daarbij een buit van 10 miljoen Amerikaanse dollars door geld van anderen over te maken naar eigen rekeningen (Williams, 2002; Grabosky, 2004). De man zou vermeende connecties hebben gehad met de Russische maffia (dit werd overigens nooit bewezen) en had handlangers in zowel de VS, Finland, Duitsland, Israël en Nederland (Rotterdam). Recent nog verschenen er berichten in de media waaruit bleek dat enkele Belgische banken het slachtoffer zijn geworden van fraude. Een woordvoerder van de Commissie voor het Bank-, Financiën- en Assurantiewezen (CBFA) stelde dat er sinds 2005 in België rond de 800.000 euro is buitgemaakt omdat HT-CSV's erin slaagden de systemen van internetbankieren te kraken (De Tijd, 9 oktober 2007). Volgens het parket zijn er aanwijzingen dat Russische criminele organisaties verantwoordelijk zijn.

Ook in Nederland zou sprake zijn van samenwerking tussen Nederlandse hackers en Oost-Europese (onder andere Russische) HT-CSV's. Hoe de hackers precies in contact komen met deze groeperingen blijft vooralsnog onduidelijk (Neve, 2007). Volgens het KLPD vindt rekrutering plaats via het internet (KLPD, DNRI, 2007b: 14). Los van het feit dat HT-CSV's de nodige expertise gericht inhuren, moet er volgens Europol (2003: 82-83) ook sterk rekening mee worden gehouden dat er inmiddels een 'eliteklasse' van criminelen bestaat die niet alleen goed georganiseerd is maar ook technisch zo goed onderlegd dat zij via hacking op eenvoudige wijze klant- en creditcardgegevens kan bemachtigen. Vooralsnog is hierover in de literatuur geen kennis voorhanden. Belangrijke conclusie uit het NDB2004 (KLPD, DNRI) is dat de opsporing nog niet in voldoende mate beschikt over kennis over de manier waarop criminele groeperingen ICT inzetten bij hun activiteiten. Daarbij wordt ook uitgesproken dat de opsporing achter zal blijven lopen bij de komende ontwikkelingen en de flexibiliteit mist om soepel in te spelen op deze ontwikkelingen. Er moet dus meer kennis en expertise verzameld worden over ICT en high-tech crime.

4.2.10 ICT-dienstverleners

Het gebruik van facilitators of dienstverleners is in vele opzichten typerend voor de georganiseerde misdaad (Kleemans e.a., 2002; NDB2004; Van de Bunt en Kleemans, 2007). Onder dienstverleners van HT-CSV's verstaan we in dit rapport corrupt ICT-personeel, inhuur van expertise, en infiltratie binnen bedrijven. Uit onderzoek is gebleken dat high-tech crime voor een deel HT-CSV's betreft waarbij criminelen gebruikmaken van specialistische, al dan niet ingehuurde kennis (KLPD, DNRI, 2004: 119-120; NHTCC, 2006b: 35). Jonge studenten worden gerekruteerd (op universiteiten, computerclubs en online forums) maar ook hoogopgeleid ICT-personeel wordt omgekocht of ingehuurd en criminele IT'ers infiltreren binnen ICT- of e-commerce-bedrijven (Europol, 2003: 27-30; McAfee, 2006; McCusker, 2006; NCTb, 2006b: 23; Williams, 2001). Juist doordat relatief veel bedrijven hun meest gevoelige kernactiviteit (de door ICT-aangestuurde, digitale informatie- en betalingssystemen) uitbesteden aan experts zijn de infiltratiemogelijkheden voor HT-CSV's breed toegankelijk geworden (Europol, 2003: 59, 82).

Het is vooral de jongere generatie met goed ontwikkelde ICT-kennis en -vaardigheden die kwetsbaar is om de georganiseerde criminaliteit ingezogen te worden (Europol, 2003: 30). Uit onderzoek, onder andere van de FBI Cyber Division, blijkt dat HT-CSV's steeds vaker jongeren (14-19 jaar), IT-studenten (of afgestudeerden) en computermedewerkers rekruteren. Zij hebben verstand van het internet en hun technische expertise kan worden ingezet bij criminele oplichtingspraktijken (zie Europol, 2003: 27; McAfee, 2006). De meeste jongeren raken hierin verzeild doordat er veel geld mee

kan worden verdiend (bedragen als 15 duizend euro voor anderhalve dag zijn geen uitzondering). Soms laten jonge hackers die betrokken raken bij HT-CSV's hun informatica-opleiding financieren in ruil voor het ontwikkelen van bijvoorbeeld *botnets* om specifieke aanvallen uit te voeren (Neve, 2007). McAfee (2006, aangehaald door McCusker) spreekt zelfs van 'KGB-achtige methoden' waarmee jonge mensen gebonden worden aan de georganiseerde criminaliteit.

In de WODC-monitor Georganiseerde Criminaliteit (Kleemans e.a., 2002; Van de Bunt en Kleemans, 2007) worden de zogenoemde 'facilitators'[148] als belangrijke schakels gezien in het criminele proces. Het belang van netwerken, facilitators (dienstverleners) en brokers (strategische bruggenbouwers die meer specifiek in staat zijn de samenwerking tot stand te brengen en te bevorderen tussen IT-experts en high-tech criminelen) kwam ook al naar voren in het NDB2004 (KLPD, DNRI, 2004: 21-31). In dat rapport werd gesuggereerd dat ICT-dienstverleners wel eens de rol zouden kunnen gaan spelen van facilitator/specialist waarmee criminele netwerken het makkelijker krijgen (KLPD, DNRI, 2004: 127). Hoewel IT'ers en ICT-bedrijven interessante partners kunnen zijn voor HT-CSV's, is de aandacht hiervoor bij de Nederlandse opsporing volgens het KLPD nog vrij gering (KLPD, DNRI, 2004). Concreet zicht op de betrokkenheid van IT'ers bij georganiseerde misdaad in Nederland is er dan ook niet.

4.3 Conclusie

Uit deze literatuurinventarisatie blijkt dat er erg weinig concrete kenmerken en informatie te vinden zijn in de literatuur over HT-CSV's. Er blijken te weinig gegevens beschikbaar te zijn om op een betrouwbare manier een relatie te kunnen leggen tussen georganiseerde misdaad en high-tech crime. Op basis van het materiaal dat wij wel hebben kunnen raadplegen is een selectie van kenmerken (deels overgenomen uit de Computer Crime Adversarial Matrix van de FBI: uit Casey, 2002: 552-554; zie ook bijlage 7) weergegeven in schema 9.[149] Onder 'diversificatie' wordt boven in het schema de overlap tussen de verschillende verschijningsvormen van high-tech crime waar HT-CSV's zich mee bezighouden weergegeven (met overige criminele activiteiten schuingedrukt). Zo is direct te zien dat met name bij hacking en malware dienstverleners betrokken zijn (corrupt personeel, ICT-infiltranten en ingehuurde expertise). En met name internetfraude en islamistisch terrorisme worden door HT-CSV's in combinatie met andere vormen van high-tech crime gepleegd. Op basis van schema 9 lijkt van alle

148 Bijvoorbeeld ondergrondse bankiers, documentenvervalsers en transporteurs.
149 Informatie over het criminele netwerk (structurele kenmerken en kwetsbaarheden) alsook hulpbronnen (training, materiaal, steun) zijn bij gebrek aan informatie uit het schema weggelaten.

verschijningsvormen vooral kinderporno een relatief geïsoleerde criminele hoofdactiviteit van HT-CSV's te zijn. Ook toegepaste technieken, vereiste kennis en vaardigheden, de wijze van organisatie (rekrutering, internationale connecties), uitvoering (planning), structurele kenmerken van netwerken, en hulpbronnen (in termen van training, steun en materiaal) zijn in het schema weergegeven. Aan de hand daarvan zien we bijvoorbeeld dat er bij de meeste (geprioriteerde) vormen van high-tech crime sprake is van enige vorm van criminele samenwerking (HT-CSV) en internationale connecties. Voor het overgrote gedeelte moeten we echter concluderen dat er ook ten aanzien van HT-CSV's sprake is van een gebrek aan kennis.

Hoewel men een ontwikkeling voorziet in een toename van ICT als communicatie- en afschermingsmiddel en als informatiebron, ligt het volgens het NDB2004 (p. 46) niet voor de hand dat high-tech crime een nieuwe vorm van georganiseerde misdaad wordt of de core business zal worden van de traditioneel georganiseerde groepen. Dat neemt echter niet weg dat de technologische expertise voor high-tech crime ook in het criminele milieu in toenemende mate zal professionaliseren (bijvoorbeeld door deze in te huren) en in de toekomst meer georganiseerd en grootschaliger zal plaatsvinden (KLPD, DNRI, 2004). High-tech crime biedt de georganiseerde criminaliteit vele lucratieve mogelijkheden. Het internet is vrij toegankelijk en wordt massaal gebruikt waardoor de groep potentiele slachtoffers groot is. In combinatie met een relatief kleine pakkans en aanzienlijke criminele winsten levert dit aantrekkelijke mogelijkheden op voor criminele groeperingen, die altijd op zoek zijn naar manieren om snel geld te verdienen. Al blijven de activiteiten van CSV's vooralsnog vooral beperkt tot de 'fysieke' wereld, naar verwachting zal high-tech crime steeds meer verweven raken met de georganiseerde misdaad en daardoor explosief kunnen toenemen. Er zijn recente aanwijzingen dat dit ook het geval is (Europese Commissie, 22 mei 2007). Met name (jonge) hackers die de beschikking hebben over botnets zijn belangrijke partners voor criminelen voor het faciliteren van bijvoorbeeld phishing en pharming.

4.3.1 Trends in high-tech crime

Er zijn verschillende bronnen geraadpleegd waarin belangrijke voorspellingen worden gedaan voor de komende jaren op het gebied van high-tech crime (AIVD, 2006a: 5; Cops, 2007h; Kohlmann, 2006; McAfee, 2006: 14, 16, 30 november 2006; MessageLabs, 2005; Morris, 2004: vii, 16; NHTCC, 2006b: 30, B13; Spits, 13 maart 2007; Taylor e.a., 2006: 357-383; Van der Werf, 2003: 54). De volgende dreigingen worden daarbij als trends gesignaleerd waarbij een aantal varianten in toenemende mate ook interessant werkgebied is voor de georganiseerde misdaad[150] (gemarkeerd met een sterretje [*]).

150 Zie ook Boerman en Mooij, 2006: 21, 29-30; Europol, 2003: 52, 72, 77-79, 116; McAfee, 2006: 14, 16; NDB2004: 77-78; Van der Werf, 2003: 53-57.

Nieuwe ontwikkelingen:
- malware in MPEG-videobestanden;
- aanvallen op mobiele telefonie (SMiShing: gelijk aan phishing via e-mail maar dan toegepast op tekstberichten via SMS);
- hacken van VoIP (Voice over IP) (vishing, ofwel voice phishing: phishing via e-mail maar via een service-telefoonnummer waarop men eerst moet 'inloggen');
- hacken van RFID (radio frequency identification: vervanger van de streepjescode waarmee op afstand informatie via radiogolven wordt opgeslagen en gelezen);
- spammail met afbeeldingen ('picture spam': moeilijker te herkennen);
- afpersing van particulieren met behulp van dDoS (om schade en/of verlies van waardevolle documenten te herstellen: bijvoorbeeld bankgegevens, werkbestanden en documenten met sentimentele waarde als muziek en foto's) (McAfee, 2006: 16);
- cyberterrorisme.

Toename van bestaande trends:
- logistiek en communicatie* (op het gebied van terrorisme);
- radicalisering en rekrutering (jonge moslims);
- afscherming (P2P-applicaties);
- internetfraude* (waaronder identiteitsfraude met behulp van phishing en creditcardfraude);
- malware* (verspreiden van virussen, Trojaanse paarden en wormen via het internet);
- bots en botnets*;
- pharming*;
- spamvolume (toename in breedbandverbindingen);
- georganiseerde misdaad (waaronder witwassen*, identiteitsfraude en kinderporno);
- ICT-dienstverleners* (hackers);
- spionage (waaronder bedrijfsspionage en softwarepiraterij);
- defacing* (vernietigen van ICT-communicatie, dataverwerking en opslag);
- kinderporno*;
- grooming;
- software- of ICT-piraterij*;
- afpersing met behulp van dDoS-aanvallen* (meer bedrijven gaan over op open systemen met internetverbinding);
- illegale handel via het internet;
- hacking (financieel gemotiveerd)*;
- hacktivisme (onder jongeren).

Het grote scala aan criminele activiteiten en vooral de dynamische ontwikkelingen op dit vlak vergen het stellen van prioriteiten in termen

van opsporing, opbouw van expertise en specialisaties (onder andere voor de politie). Daarnaast is het van belang dat de ontwikkelingen blijvend worden geëvalueerd in relatie tot het strafrecht, onderzoeksmethoden, en in het kader van voorlichting en preventie. Het grensoverschrijdende karakter van high-tech crime wordt nog eens benadrukt door het bestaan van transnationale HT-CSV's. Onderzoek naar daders en HT-CSV's en de bestrijding van high-tech crime in het algemeen (zowel op het gebied van preventie als in de opsporing en vervolging) is om die reden waarschijnlijk het best gediend met een integrale aanpak waarbinnen diverse opsporingsinstanties en andere betrokken partijen intensief met elkaar samenwerken.

Schema 9 Kenmerken van CSV's op het gebied van high-tech crime

	Radicalisering	(Islam.) terrorisme	Kinderporno	Softwarepiraterij	Internetfraude	Witwassen	Cyberterrorisme	Hacking	Malware	Corrupte ICT'ers	ICT-infiltranten	Inhuur expertise
Diversificatie												
Radicalisering												
(Islamistisch) terrorisme												
Kinderporno												
Softwarepiraterij												
Internetfraude												
Witwassen												
Cyberterrorisme												
Hacking					x							
Malware					x			x				
Corrupte ICT'ers						x		x	x			
ICT-infiltranten								x	x			
Inhuur expertise					x			x	x			
Inbraak/diefstal		x						x	x			
Geweld				x	x							
Mensenhandel		x			x							
Drugshandel		x		x	x	x						
Afpersing		x										
Documentenvervalsing		x										
Technieken												
Afscherming												
Botnets												
Kennis/vaardigheden												
Computerervaring								x	x	x	x	x
Programmeerervaring								x	x	x	x	x
Organisatie												
Organisatie												
Rekrutering/aantrekkingskracht												
Internet								x	x			x
Sociale affiliatie		x										
Internationale connecties		x	x	x	x	x		x	x			x
Rusland			x			x		x	x			x
Oost-Europa			x	x				x	x			x
West-Europa												x
Azië				x								x
Uitvoering												
Planning												
Niveau expertise												
Methoden												
Taakspecialisatie								x				

5 Conclusie en discussie

Doel van dit onderzoek was om kennis over daders van high-tech crime te inventariseren op basis van (inter)nationale literatuur. De uitkomsten zouden de transparantie op het gebied van high-tech crime moeten verbeteren en een bijdrage moeten kunnen leveren voor meer gericht onderzoek en meer probleemspecifieke beleidsmaatregelen op het gebied van de preventie, opsporing en handhaving van high-tech crime. Op basis van dit rapport kunnen we concluderen dat de kennis van daders (in ieder geval in de literatuur) nog grove lacunes laat zien. Voor een deel heeft dat te maken met een gebrek aan overzicht ten aanzien van het fenomeen en het criminaliteitsterrein zelf, en voor een deel met een gebrek aan studies die inzicht geven over daders en daderkenmerken. De aanbevelingen uit dit rapport beperken zich hoofdzakelijk tot het geven van richting aan de kennisontwikkeling die op dit vlak nodig is.

Harmonisatie en kennisuitwisseling
Een duidelijke beschrijving van het criminaliteitsterrein met een harmonisatie in definities en begrippen is een noodzakelijke stap in de verbetering van de aanpak van high-tech crime. Bestaande kennis wordt dan beter zichtbaar en lacunes in kennis kunnen dan ook beter worden aangepakt. Een consistent en valide begrippenkader is de enige mogelijkheid om de daadwerkelijke aard en omvang van het probleem goed in kaart te brengen (bijvoorbeeld voor internationaal vergelijkend onderzoek) (zie Gordon en Ford, 2006). Bovendien zal het de onderlinge afstemming, samenwerking en kennisuitwisseling tussen verschillende spelers in het veld bevorderen.

Trendwatching van high-tech crime
Om meer te kunnen doen aan preventie, opsporing en handhaving moet meer kennis en expertise verzameld worden over ICT en high-tech crime. Het is van groot belang om op de hoogte te blijven van de kennisontwikkeling op technologisch gebied en van de wijze waarop deze ontwikkelingen mogelijkheden kunnen bieden voor criminelen (en terroristen). Het is zaak om door middel van trendwatching de dynamische ICT-ontwikkelingen te blijven volgen, zowel in relatie tot cyber- als computercriminaliteit (NHTCC/NPAC, 2006a: 35). In het Ontwerp 'Nationale Infrastructuur Bestrijding Cybercrime' wordt gesproken van een jaarlijks terugkerende high-tech crime monitor waarmee de aard en omvang van het probleem in beeld zou kunnen worden gebracht (NHTCC/NPAC, 2006a: 64). Voordat een dergelijke monitor van werkelijk nut zal zijn, is behalve harmonisatie en verbeteringen in de registraties, ook aansluiting wenselijk met internationale initiatieven. Mede gezien het grensoverschrijdende karakter dat inherent is aan high-tech crime is dit een pré. Te denken valt aan wetenschappelijke onderzoeksinitiatieven (denk ook aan het 7e kaderprogramma van de Europese Commissie), praktijkgerelateerde onderzoeken (bijvoorbeeld politiediensten, Europol), en aan beleidsge-

richte initiatieven ter bestrijding van high-tech crime (bijvoorbeeld van de Europese Commissie).

Alternatieve onderzoeksmethoden
Meer kennis is nodig over individuele daders van high-tech crime en de betrokkenheid van de georganiseerde criminaliteit. Het ontbreekt in de literatuur sterk aan specifieke daderkennis, zowel in termen van organisatie (zoals rekrutering), uitvoering (expertise), gedrag (waaronder persoonlijke kenmerken) als van de gebruikte resources. Meer inzicht in de deeltaken (taakspecialisatie) van high-tech crime en in de overlap van werkwijzen en instrumenten tussen de verschillende verschijningsvormen (diversificatie) is nodig, alsook nader onderzoek naar de samenwerking tussen Oost-Europese en Russische criminele netwerken en West-Europese (waaronder Nederlandse) hackers die daarvoor worden ingehuurd. In zijn algemeenheid geldt voor de meeste verschijningsvormen bovendien dat het inzicht ontbreekt in de criminele carrières van daders en in de overlap tussen de verschillende verschijningsvormen van high-tech crime. Aangezien de literatuur hier vooralsnog (te) weinig uitsluitsel biedt, is het te overwegen om alternatieve onderzoeksmethoden te gebruiken die aanvullende inzichten kunnen opleveren (bijvoorbeeld case studies en/of onderzoek op politie- en strafdossiers). Het strekt tot aanbeveling om meer deelonderzoeken te verrichten naar de *afzonderlijke* verschijningsvormen van high-tech crime zodat in meer detail informatie kan worden verkregen die betere aanknopingspunten vormen in termen van preventie en opsporing. Ook aandacht voor subculturen en jeugdcriminaliteit kan inzichten opleveren waarvoor specifieke probleemgerichte maatregelen moeten worden ontwikkeld.

Prioriteiten op de onderzoeksagenda
Welke verschijningsvormen op de onderzoeksagenda prioriteit moeten krijgen is vooral aan de beleidsmakers om te bepalen. Binnen alle themaclusters die staan beschreven in dit rapport zijn wel ontwikkelingen gaande die nopen tot extra aandacht. In het kader van *legale communicatie* en afscherming van communicatie ten behoeve van illegale doeleinden is de aandacht tot nog toe sterk gericht op de invloed van het islamistisch radicalisme. Kennis over daders van bijvoorbeeld dierenrechtenactivisten en extreem-rechtse radicalen is echter evenzo belangrijk voor het bevorderen van veiligheid. Een toenemend probleem op het vlak van *illegale communicatie* zijn delicten waarmee de publieke moraal of de persoonlijke levenssfeer van slachtoffers wordt aangetast. Grooming, discriminatie en haatzaaien op het internet zorgen voor verontwaardiging en onrust in de maatschappij en gevoelens van onveiligheid. Van alle high-tech crimes wordt *financieel-economische criminaliteit* (waaronder identiteitsfraude met behulp van phishing) beschouwd als een van de snelst groeiende vormen van niet-gewelddadige criminaliteit. Door de toenemende virtuele

geldstromen is de verwachting dat internetfraude (en identiteitsdiefstal) de komende jaren veel slachtoffers en financiële schade zal aanrichten. In alle opzichten is van belang meer kennis te vergaren over de ondersteunende functie van allerlei *computercriminele activiteiten* die instrumenteel zijn voor het plegen van allerlei vormen van cybercriminaliteit (zoals hacking en botnets). Het beteugelen van computercriminaliteit is bovendien van fundamenteel belang voor het goed kunnen blijven functioneren en de verdere ontwikkeling van de hele ICT-sector. De belangrijke rol van *dienstverleners* staat hier natuurlijk buiten kijf. Als aandachtsgebied op de korte termijn gelden wellicht in eerste instantie de activiteiten die multifunctioneel zijn voor het plegen van meerdere vormen van high-tech crime (en veelal ook in combinatie met andere delicten wordt gepleegd). Uit deze literatuurinventarisatie blijkt onder meer dat vooral *internetfraude* en *hacking* criminele verschijnselen zijn die veelal in combinatie met andere vormen van high-tech crime worden gepleegd. De handel in *botnets*, *malware* en *Trojaanse paarden* is een belangrijke criminele markt binnen de georganiseerde misdaad Zij spelen bovendien bij vele andere verschijningsvormen een belangrijke rol en vormen om die reden een aanzienlijke bedreiging die dient te worden aangepakt.

Theoriegestuurd onderzoek
Behalve expliciete aandacht voor onderzoek naar uiteenlopende verschijningsvormen van high-tech crime is het van belang om meer voordeel te halen uit bestaande theoretische kennis en fundamenteel wetenschappelijk onderzoek (zie ook Leeuw, 2006). Gedragswetenschappelijke theorieën kunnen bijvoorbeeld meer inzicht geven in factoren die van invloed zijn op het plegen van high-tech crime, en daarmee kunnen inzichten worden gegenereerd die sturend zijn voor het ontwikkelen en/of implementeren van beleidsmaatregelen. Een voorbeeld van het toepassen van verklarende theorieën wordt gegeven door Taylor e.a. (2006: 36-65). Zij belichten het fenomeen high-tech crime aan de hand van rationele keuzetheorieën, psychologische theorieën, en theorieën over sociale structuren en processen.

Volgens de rationele keuzetheorie (waaronder de Routine Activity Theory van Cohen en Felson uit 1979, aangehaald door Taylor e.a., 2006: 37-39; zie ook Jolls e.a., 1998; Khong, 2004) nemen mensen beslissingen door de voordelen (opbrengsten) van hun gedrag af te wegen tegen de nadelen (investeringen, obstakels) en de relatieve opbrengsten te maximaliseren. Wanneer een bepaald (crimineel) gedragsalternatief meer voor- dan nadelen met zich meebrengt, is de kans groter dat men dit gedrag dus daadwerkelijk zal vertonen. Vanuit dit perspectief bezien is het zinvol om de potentiële nadelen voor een high-tech crimineel zo groot mogelijk te maken, de voordelen ervan zoveel mogelijk te beperken, en/of gedragsalternatieven meer aantrekkelijk te maken. Dergelijke maatrege-

len kunnen van uiteenlopende aard zijn en betrekking hebben op meerdere snijvlakken van preventie, opsporing, vervolging en handhaving.

Er zijn ook psychologische theorieën (zoals de Cognitieve Ontwikkelingstheorie van Kohlberg uit 1969, aangehaald door Taylor e.a., 2006: 41-44; zie ook Rogers e.a., 2006b) die inzichten kunnen opleveren over de motieven, persoonlijkheidskenmerken en de morele ontwikkeling van daders van high-tech crime. Sommige criminelen zijn in hun morele ontwikkeling niet verder dan het niveau van een kind en ervaren hun criminele activiteiten pas als negatief en ongewenst wanneer zij daarvoor daadwerkelijk worden gestraft. Vanuit dit perspectief bekeken geldt dat het verhogen van de pakkans (opsporing) en het verzwaren van de strafmaat van high-tech crime (vervolging) instrumenteel zouden kunnen zijn voor het doorbreken van criminele activiteiten. Meer kennis over daders (motieven, persoonlijkheid, gewoontegedrag, attitudes, waargenomen consequenties) en hun sociale omgeving (sociale normen en faciliterende omstandigheden) blijft echter van instrumenteel belang voor het ontwikkelen van effectief beleid (zie ook Higgins, 2005, 2007; Limayem e.a., 2004).

Andere wetenschappelijke stromingen benadrukken meer de invloed van de sociale context en de sociale omgeving van individuen en groepen. Theorieën over sociale structuren (zoals de Strain Theory van Merton uit 1968 en van Agnew uit 1992, of de deprivatietheorieën van Mills uit 1940, van Cohen uit 1955 en van Cloward en Ohlin uit 1960, allen aangehaald door Taylor e.a., 2006: 44-50) en sociale netwerken (Burt, 1992; Coleman, 1988; Granovetter, 1973; Lin, 1999) definiëren criminaliteit bijvoorbeeld in termen van (beperkte) gelegenheidsstructuren. De gedachte is dat wanneer het voor mensen moeilijk is om via de reguliere weg (bijvoorbeeld een goede opleiding of baan) maatschappelijk en economisch succes te oogsten of wanneer men dit succes niet als zodanig ervaart,[151] men eerder op zoek zal gaan naar alternatieven om succes via andere wegen en middelen (criminele activiteiten) te bereiken. Ook het ontstaan van subculturen, waar eigen gecreëerde doelen, normen en waarden alternatieven bieden voor het bereiken van status en succes, is volgens sommige wetenschappers het resultaat van beperkte kansen en mogelijkheden in de bestaande maatschappelijke structuren. Binnen dergelijke subculturen (bijvoorbeeld zoals dat van hackers) worden de nieuwe normen en waarden onder invloed van de sociale omgeving dusdanig bekrachtigd en geïnternaliseerd dat men overtuigt raakt van de rechtmatigheid van het eigen handelen. Dit nodigt uit tot creatieve beleidsmaatregelen waarbij

151 Sommige theoretici (bijvoorbeeld Agnew, zie Taylor e.a., 2006: 46) veronderstellen dat de aanwezigheid van negatieve gevoelens en frustraties op zich al voldoende kunnen zijn voor het bevorderen van crimineel gedrag. Bijvoorbeeld doordat men minder presteert dan anderen, doordat men minder presteert dan men zelf verwacht had, maar ook door stressvolle gebeurtenissen zoals het verlies van een dierbare, interpersoonlijke conflicten of mishandeling.

aanknopingspunten kunnen worden gezocht in theorieën over sociaal leren (rolmodellen, incentives, self-efficacy, invloed van de media) en sociale netwerken (zie Taylor e.a., 2006: 46-59 maar ook in Burt, 2004 en Rogers, 2001: 136-143).

Het voert hier te ver om een uitgebreid inhoudelijk betoog te voeren over het nut van verklarende gedragswetenschappelijke theorie in beleidsonderzoek. Het inzetten en toetsen van gedragsmodellen, waarbij beleidsvraagstukken zo concreet mogelijk worden vertaald naar toetsbare hypothesen, biedt echter aantrekkelijke mogelijkheden voor nieuw onderzoek. Op basis daarvan kunnen verschillende inzichten vanuit de (sociale) psychologie, sociologie, antropologie en de economie helpen om criminologische fenomenen als high-tech crime beter te begrijpen en daardoor effectiever tegen te gaan. Voor toekomstig onderzoek is meer theoretische verdieping aan te bevelen (voor een nadere toelichting zie Leeuw, 2006).

Preventieve maatregelen
Op het gebied van criminaliteit is preventie tweeledig. Enerzijds gaat het om het identificeren van risicogroepen (daders) om te voorkomen dat zij de criminaliteit ingaan of (opnieuw) delicten plegen, anderzijds gaat het om het beschermen van potentiële slachtoffers. Kennis over daders van high-tech crime kan mogelijk bijdragen aan het identificeren van risicogroepen. Zo is gebleken dat corrupte ICT'ers en criminelen die actief zijn op het gebied van terrorisme, internetfraude, kinderporno en hacking nogal eens over een strafblad beschikken. Meer kennis over deze daders, hun motieven en achtergronden kunnen licht werpen op de criminele carrières en eventueel aanknopingspunten bieden voor effectieve preventie. Uit deze literatuurstudie kwam ook naar voren dat jongeren met kennis van ICT via het internet, op computerclubs en universiteiten worden gerekruteerd om te ondersteunen bij malafide praktijken van criminelen. Hetzelfde geldt voor afgestudeerden en IT-medewerkers. Deze doelgroepen lopen dus het risico om de criminaliteit ingezogen te worden en in een criminele spiraal te belanden waar moeilijk uit te komen is. Ook werd eerder beschreven dat medewerkers binnen bedrijven gevoelig kunnen zijn voor corruptie en wordt gewaarschuwd voor wraakzuchtige (ex-)werknemers en voor IT-consultants met criminele bedoelingen die kunnen infiltreren binnen bedrijven. Voor de bestrijding van high-tech crime kan dus gedacht worden aan voorlichting en preventie gericht op jongeren en IT-medewerkers maar ook aan functionarissen die verantwoordelijk zijn voor een goed personeelsbeleid. Dit houdt in een goede screening van personeel, oplettendheid bij afwijkend gedrag van medewerkers, het opleiden en behouden van eigen IT-personeel, en bijvoorbeeld het introduceren van een gedragscode en vertrouwensfuncties binnen de ICT. Het technisch beveiligen van (bedrijfs)systemen is eveneens een preventief

middel dat blijvende aandacht vraagt. In dat kader dienen ook potentiële slachtoffers met gebrekkige kennis van ICT (bijvoorbeeld ouderen) goede voorlichting en ondersteuning te krijgen.

Opsporingstechnieken
Uit het onderzoek komt met regelmaat naar voren dat vele vormen van high-tech crime (bijvoorbeeld illegale handel op het internet) zo aantrekkelijk zijn omdat de pakkans relatief gering is. Dit vergt niet alleen prioriteiten op de onderzoeksagenda maar ook op het gebied van de opsporing waarbij opbouw van expertise en specialisaties van cruciaal belang is (onder andere bij de politie). Ook de effectiviteit van onderzoeks- en opsporingsmethoden zou nader onder de loep genomen kunnen worden. De ontwikkeling van *risico- en daderprofielen* als hulpmiddel in de preventie en opsporing van high-tech crime is een mogelijke optie. Het gebrek aan kennis over daders door het ontbreken van een zogenoemde 'intelligence database' is echter een belangrijke reden voor het gebrek aan ontwikkeling van daderprofielen. Daarom is het zaak dat er voldoende betrouwbare en gevalideerde gegevens worden verkregen over daders en werkwijzen van high-tech crime.[152] Het beperkte inzicht in daders dat in deze studie naar voren is gekomen volstaat niet en dient te worden aangevuld met gegevens uit de praktijk. Vervolgens dienen deze nauwkeurig te worden getoetst alvorens te kunnen spreken van echte risico-indicatoren. Er zijn nog voldoende openliggende vragen waarop voor de verschillende verschijningsvormen van high-tech crime nader onderzoek gewenst is. Welke sociaaldemografische kenmerken karakteriseren de daders (sekse, leeftijd, etniciteit, nationaliteit, woonplaats, opleiding, studie/beroep, religie of levensovertuiging, stoornis, verslaving, crimineel verleden)? Wat zijn hun motieven (is dat financieel, politiek/ideologisch, sociaal of emotioneel) en wat voor werkwijze hanteren zij (wat is de aard, frequentie, omvang, technische expertise, organisatiegraad, internationale connecties, mate van diversificatie of specialisatie)? En in hoeverre zijn deze kenmerken van daders en criminele activiteiten daadwerkelijk aan elkaar gerelateerd (is er sprake van een homogeen profiel)? Of dergelijke inzichten daadwerkelijk tot een betere opsporing zullen leiden is vooralsnog de vraag. De effectiviteit van het gebruik van risicoprofielen is tot op heden nog onvoldoende onderzocht.

Toekomstbeeld
Het toekomstbeeld van high-tech crime vormt op meerdere punten een dreiging voor onze samenleving. Dit geldt niet direct voor alle verschijningsvormen van high-tech crime. Voor sommige varianten zijn de dreigingen en/of risico's (in ieder geval voor de Nederlandse samenleving)

152 Een belangrijke bron vormen politiedossiers van opsporingsonderzoeken, strafdossiers van het OM, maar ook interviews met daders.

meer actueel dan voor andere. De dreigingen variëren zowel in waarschijnlijkheid als in omvang (of frequentie) en ook de aard en ernst van de consequenties kunnen uiteen lopen. Zo zijn bijvoorbeeld radicalisering, terrorisme en ideologisch gemotiveerde misdaad de meest *levensbedreigende* vormen van high-tech crime waarbij bovendien de democratische rechtsorde in het geding is. Ook zonder hoge waarschijnlijkheid en prevalentie van het probleem kunnen deze verschijningsvormen door hun aard en consequenties als dreiging worden gekwalificeerd. Andere vormen, zoals kinderporno en grooming (waarbij kwetsbare minderjarigen het slachtoffer zijn van onzedelijke intenties en gedragingen van volwassenen), veroorzaken behalve *persoonlijk leed* veel *maatschappelijke onrust*. Weer andere verschijningsvormen veroorzaken vooral *financieel-economische schade*, bijvoorbeeld softwarepiraterij en internetfraude (en ondersteunende instrumenten als hacking, malware en ICT-dienstverleners), waarbij in sommige gevallen tevens sprake is van *schade in de continuïteit van bedrijfsvoering* binnen bepaalde sectoren. Andere verschijningsvormen van high-tech crime, zoals de handel in drugs op en via het internet (zie ook bijlage 6), vormen in mindere mate een bedreiging voor onze samenleving omdat het relatief weinig voorkomt in Nederland, omdat het probleem relatief goed beheersbaar is en/of omdat de schade die wordt veroorzaakt relatief gering is. Zeker is dat meerdere verschijningsvormen van high-tech crime het werkterrein zijn van de *georganiseerde criminaliteit* (bijvoorbeeld witwassen, kinderporno, softwarepiraterij, internetfraude, hacking, malware en ICT-dienstverleners). In termen van economische schade, maatschappelijke onrust en het toepassen van (extreem) geweld binnen de samenleving vormt dit een bedreiging op zich die streng dient te worden aangepakt.

In hoeverre de dreigingen die in dit rapport worden genoemd actueel blijven en hoe deze zich verder zullen ontwikkelen is vooralsnog onduidelijk. Dit zal mede afhankelijk zijn van maatregelen op het gebied van onder meer preventie (voorlichting, technische expertise en ICT-beveiliging), opsporing (inzet en opbouw van expertise, vergroten van de pakkans) en handhaving (toezicht, controle en – inter – nationale samenwerking). Naarmate de criminele mogelijkheden (bijvoorbeeld in ontwikkelingslanden) en de relatieve opbrengsten van high-tech crime (ten opzichte van de investeringen, risico's en alternatieve activiteiten) afnemen, zal het fenomeen high-tech crime minder lucratief worden. Het fenomeen kan langzaam uitdoven of mogelijk plaats maken voor weer nieuwe vormen van criminaliteit. Gezien de steeds voortschrijdende technische innovaties, ook op het gebied van ICT, ligt het echter voor de hand dat ook de criminele mogelijkheden in de toekomst verder zullen toenemen. Het ontstaan van geheel nieuwe verschijningsvormen van high-tech crime is daarbij niet uitgesloten.

Het veiligheidsprogramma van de Nederlandse regering en dat van de EU heeft de aanpak van high-tech crime als een van de speerpunten uitgeroepen in de bestrijding van criminaliteit. Feit is dat high-tech crime echter een veelomvattend fenomeen is dat niet onder één noemer kan worden gevat. Verschillende verschijningsvormen van high-tech crime vereisen een eigen probleemgerichte aanpak. Om de aanpak van high-tech crime als globaal beleidsspeerpunt te formuleren zonder nadere uitwerking of specificatie van thema's en probleemstellingen is te ontraden. Hiermee ontstaat namelijk de valkuil van te weinig probleemgestuurde programma's en aspecifieke beleidsmaatregelen die nauwelijks of geen samenhang vertonen met het daadwerkelijk onderliggende probleem. Zo ligt het immers voor de hand dat daders van kinderporno een andere aanpak vereisen dan terroristen of hackers. Een goede aanpak vereist dan ook balans tussen algemene, generalistische beleidsmaatregelen en een specialistische aanpak die toegesneden is op bijzondere verschijningsvormen van high-tech crime.

De Europese Commissie (2007a) heeft zich recentelijk expliciet uitgesproken over de aanpak van thema's als kinderporno, botnets, internetfraude en identiteitsfraude. De Raad van de EU (2007) richt zich in de strijd tegen het terrorisme onder meer op de volgende thema's: de aanpak van radicalisering via het internet ('check the web') en de beveiliging van kritieke infrastructuren. In het nieuwe beleidsprogramma van het Nederlandse kabinet 'Veiligheid begint bij Voorkomen' (TK, 2007-2008, 28 684, nr. 119) worden als belangrijke speerpunten onder meer aangeduid de '*minder zichtbare en ernstige vormen van criminaliteit*' (p. 3). In het bijzonder richt men zich op de aanpak van high-tech crime (of cybercriminaliteit), financieel-economische criminaliteit en georganiseerde criminaliteit. Voor deze speerpunten, die overigens deels overlappen, worden versterkingsprogramma's ontwikkeld en geïmplementeerd in overeenstemming met de Landelijke prioriteiten voor de Politie (2008-2011). Gelijk aan de prioriteiten van de Europese Commissie richt het Nederlandse kabinet zich wat betreft high-tech crime expliciet op de aanpak van kinderporno en internetfraude (waaronder identiteitsfraude). De overige beide speerpunten, financieel-economische fraude (zoals fraude, witwassen en corruptie) en georganiseerde misdaad, vertonen echter ook overlap met verschijningsvormen van high-tech crime en vragen in dat kader om nauwe explicitering.

In alle opzichten lijkt het zaak om vooral de trend naar professionalisering van high-tech crime tegen te gaan. De aandachts- en discussiepunten uit dit rapport bieden aanknopingspunten voor een betere transparantie en voor het maken van een kennisslag die nodig is om de aanpak en bestrijding van high-tech crime te verbeteren. Het verdient aanbeveling om de combinatie van maatregelen zoals die zijn voorgesteld in het nieuwe

beleidsprogramma (onderzoek, preventie, organisatie, deskundigheid, capaciteit en internationale samenwerking) zo nauw mogelijk te specificeren naar verschijningsvorm. Hiermee wordt gewaarborgd dat ook de aanpak van andere dreigingen voor de Nederlandse samenleving (zoals grooming, softwarepiraterij, hacking, malware en ICT-dienstverleners) nadrukkelijk als thema op de (internationale) beleidsagenda komt en dat de nationale aanpak van andere belangrijke thema's (zoals radicalisering, terrorisme en ideologisch gemotiveerde misdaad, maar ook cyberterrorisme) beter worden afgestemd met (lopende) initiatieven in Europees verband.

Summary

High-tech crime, different crime types and perpetrators: A literature review

In this current digital era we live in, core processes throughout society are often controlled by ICT and digital technologies. The worldwide use of ICT and the internet by both private individuals and the business community has increased during the past decade. Our society has come to depend heavily on a fully operational network of digital and inter-connective systems. This dependency will continue to grow as more government bodies, companies, organisations and natural persons start to use them. The specific conditions associated with this development – such as the growing use of networks that have an open internet connection, and the anonymity and broad reach of the internet – also provide lucrative opportunities, however, for the criminal circuit (Van Amersfoort et al., 2002). The opportunities for a wide range of criminal activities – described here as *high-tech crime* – have increased significantly in recent years (NHTCC/NPAC, 2006a: 6). The financial, economic and social consequences of high-tech crime may have a deep impact on our society. Not only is it important for the core processes in our society to continue functioning well and to continue in their development, but the user's faith in a secure ICT environment is also a vital aspect. As a result, preventing and combating high-tech crime is one of the spearheads in the Dutch and European security policies. The lack of knowledge concerning the perpetrators of high-tech crime and the involvement of organised crime is an important gap in terms of developing an efficient and effective policy. As such, the Ministry of Justice felt that it was fitting to commission a *literature* inventory, mapping the status quo and existing knowledge in relation to high-tech crime and, more particularly, its perpetrators (including perpetrators of organised crime).

This study focuses on the following six research questions:
- What do we mean by the term 'high-tech crime'?
- What phenomena of high-tech crime can be distinguished?
- How can the perpetrators (or perpetrator groups) of high-tech crime be characterised?
- What is the extent of organised crime's involvement in high-tech crime?
- What gaps exist in the literature in terms of knowledge concerning the perpetrators of high-tech crime?
- What developments in high-tech crime should we expect in the near future?

For each research question, the main findings are summarised and a few points of concern and discussion are assessed for the purpose of further interpretation of the research and policy programming in the field of high-tech crime.

What is high-tech crime?

The literature shows that it is not easy to clearly define the criminal area of high-tech crime. There is no conventional norm on shared concepts and often, different definitions are used interchangeably. The scope of high-tech crime is infinite and difficult to delimit due to the close relationships between 'traditional' forms of crime (such as fraud and theft) on the one hand, and advanced ICT and digital technologies on the other. Moreover, new criminal markets are also emerging at the same time. As a result, researchers, policy-makers and law enforcement workers have a tendency to speak different languages: identical concepts used to describe a phenomenon may have widely diverging meanings to different stakeholders and vice versa (different terms that actually refer to the same problem), and some use a narrower set of definitions than others. The area of crime is also referred to differently by different people. For instance, terms like cyber crime (or cyber criminality) and high-tech crime are often used as equivalents, but terms like ICT, internet, digital, information and e-crime are also used on a regular basis. This lack of a total overview and the absence of consistency cause confusion and do not benefit the development of a good approach, knowledge exchange and collaboration in the field of high-tech crime.

This report uses *high-tech crime* as the umbrella term that refers to a range of criminal activities which make use of ICT. Such criminal activities may target persons, property and organisations (using ICT as a means), or electronic communication networks and information systems (with ICT being both the means and the objective). When compared to the term *cyber crime*, *high-tech crime* offers a wider and more dynamic perspective – a better match for the fast technological developments in time. The umbrella term also covers new forms of crime that may emerge from new ICT innovations (not just the internet), which by definition means that high-tech crime is not a static umbrella term. In order to further define the difference between traditional offences and new forms of crime that have resulted from ICT, this report distinguishes between two sub-categories of high-tech crime. Where ICT can be characterised explicitly as the means *and* the target, we use *computer crime*. For all other ICT-related (often traditional) offences we use *cyber crime*. There are different, closely related phenomena of both sub-categories, which are often committed simultaneously. A characteristic that the phenomena of computer crime (e.g. hacking and virus distribution) share, is that they are of an extremely technical, virtual nature: they have emerged from – and cannot exist without – ICT. But the phenomena of cyber crime, to the contrary, generally involve traditional offences that can be committed without ICT (e.g. child pornography and extortion) but have now emerged

in a new (more efficient) form due to the use of advanced, technical – ICT-based – resources.

What are the phenomena of high-tech crime?

This report uses a holistic perspective in order to create an inventory of as much knowledge as possible relating to the perpetrators of high-tech crime. To this end, we have categorised the different phenomena of cyber and computer crime into eight theme clusters on the basis of the literature (see also Figure 2.2 in Chapter 2):

Cyber crime:
1. legal communication and covert shielding;
2. illegal trade;
3. economic and financial crime;
4. illegal communication.

Computer crime:
5. unauthorised access to ICT;
6. ICT failure due to data traffic;
7. ICT failure due to data and system manipulation;
8. service performers.

This classification represents a preliminary inventory and serves as a basis for the further development of a typology of high-tech crime. The overview is necessary to provide a starting point for further knowledge development and policy creation in the prevention of and fight against high-tech crime. However, the classification can be adjusted and supplemented with new, complementary knowledge at all times. Each of the theme clusters and associated phenomena is summarised below.

Cyber crime

Cyber crime refers to the use of ICT as a tool to commit a range of offences. In many cases, this relates to the supporting function of ICT in communication (between perpetrators or between perpetrators and victims), but also, for instance, about using ICT to execute (voluntary or forced) transactions with goods and services, as well as financial transactions.

Legal communication and covert shielding
ICT has a great many functions. In relation to crime, for instance, the internet acts as a virtual source of inspiration, a virtual meeting place,

and a platform for knowledge exchange and secure and unsecured communication. When these functions are used for *illegal* purposes (e.g. to recruit radical youths), this report refers to cyber crime. This cluster covers three themes: radicalisation and extremism, terrorism and ideologically motivated crime, and innovative covert shielding using ICT. The internet plays a prominent part in both radicalisation and terrorism. The internet lives particularly among young people, and they are mutually inspired and motivated to make extremist statements. The internet is also used to gather knowledge (manuals or other operational knowledge) and mobilise people. The literature shows a trend towards publications focusing on the impact of Islamic radicalism (and other radical movements to a lesser extent). This may have a negative impact on knowledge development in a broader sense and lead to tunnel vision. As a result, important trends and indications may be neglected or overlooked. Radicals, terrorists and parties in the criminal circuit use innovative techniques to screen their communication from 'unauthorised' parties (including criminal investigation bodies). Their methods vary from smart ideas (such as continuously changing unregistered mobile telephones or using 'dead letter boxes', where draft e-mail messages can be viewed and modified by several users without actually being transmitted) to advanced concepts like encryption (encoding the content of messages), and steganography (hiding the existence of a message altogether by incorporating it into an image or digital clip, for instance). In some cases, experts are hired to perform these operations.

Illegal trade

The internet enables unlimited and virtually effort-free trade. It is a growth market in our modern economy, but it also means that illegal goods and services can be traded over the digital highway. Both national and international literature provides little insight into the illegal trade in drugs, arms and explosives, nor human trade and smuggling. Based on this study, we cannot determine whether this is indicative of the *extent* to which the internet is being used, or whether such knowledge is absent due to the lack of investigation, research and publications. For now, it seems that ICT plays a primarily *communication-oriented* role in such forms of trade. The relative anonymity of internet users and the lack of social control and face-to-face contact may in fact deter internet use among these criminal markets. However, there are phenomena in which the internet is an important economic market place and distribution channel for trading goods and services. Counterfeit brand drugs, non-prescription drugs, child pornography, stolen goods, illegal software (software piracy) and illegal gambling are all examples of such goods and services that are currently offered on a large scale. The internet is a popular and commonly used resource mainly because of the large market to which it offers access and the relatively low risk of being caught. The trade in child pornography

in particular, in which the material itself is offered in digital form, is being increasingly blocked with the help of advanced techniques.

Economic and financial crime
Economic and financial crime involves making an illegal profit by means of fraud, deception and embezzlement. Internet embezzlement in particular is a common problem that is threatening Dutch society. People are made to pay money under false pretences (advance-fee fraud), or ICT is used to obtain confidential information illegally (identify theft) that is subsequently used to commit bank and credit-card fraud. Identity fraud by means of phishing – which is a criminal tool rather than an objective – is seen as one of the fastest growing forms of non-violent crime. The literature contains less information on the other themes (fraud through market manipulation, extortion and blackmail, and money laundering). Money laundering using ICT might increase significantly in the future due to the growing virtual money flows in social and economic traffic (via online auction sites, electronic and mobile commerce). Another potential threat is the extortion of companies that depend heavily on the internet for their operations (e-commerce), or companies and citizens which receive threats that important files and data will be damaged or made publicly if they do not comply with the demands being made. We should note the close relationship between phenomena of cyber crime and computer crime in this context. Internet fraud (cyber crime), for instance, uses a variety of methods and techniques like phishing, spamming, malware and pharming (computer crime). The cyber variant of blackmail and extortion is often related to system hacking and threats of a dDoS attack that may corrupt entire systems (see also computer crime).

Illegal communication
The many uses of ICT and the internet can also be used to convey messages with *illegal content*. This mainly involves activities that actually affect public morale, or the personal life of victims (e.g. stalking, discrimination or grooming). In this report, such crimes are called illegal communication. In terms of their content, these digital behavioural crimes differ little from their variants in the 'physical world'. Discrimination (or inciting hatred) via the internet in particular, in which different groups continuously provoke each other in discussion forums and chat boxes, has become a trend. Another growing problem that is causing a lot of outrage in society is grooming, in which chat sites are used by adults with dishonourable sexual intentions to approach children. In some cases, grooming results in an actual meeting where minors are physically abused and raped. Illegal communication is also involved when third-party computer and telephone data are intercepted illegally, i.e. without authorisation (espionage). Criminals use methods and tools like hacking, spyware and malware to do this, as well as service

performers (e.g. corrupt employees). Here, too, we see a close relationship between cyber crime and computer crime. In this context, the use of spyware (software installed unnoticed on a computer that collects data and transmits it to a third party) and keyloggers (where keystrokes and mouse clicks are transmitted to a third party) in particular may expand in the future.

Computer crime

In this report, the term *computer crime* refers to all new forms of criminality that would have been impossible if ICT did not exist. ICT is used not only as a tool in such criminal activities, but also as the explicit target. In most cases, computer crime is about breaking into, disturbing, manipulating or changing systems and/or developing and providing tools and resources to do so. We distinguish four theme clusters that are described below.

Unauthorised access to ICT
There are two central elements in providing unauthorised access to ICT (in fact, breaking into systems): hackers and botnets. Hackers increasingly have criminal intentions, are increasingly often financially motivated, and engage in multifunctional activities that can be used for multiple phenomena of computer crime. They can break into secure and unsecured systems, develop tools to cause ICT failures, and provide tailor-made customisations that require a high level of expertise and technical knowledge. There is an 'underground' sub-culture that resembles the underground criminal circuit: it has its own identity, status as an important acquirement, and its own standards and values. Hackers are increasingly hired by traditional criminal networks, and, in some cases Dutchmen are also members of organised (Eastern European) criminal networks acting as service performers.[153] One of the main criminal tools that hackers can provide is a botnet. This is a collection of remote-controlled computers that is instrumental in committing several phenomena of high-tech crime, especially spamming, phishing and (extortion with the aid of) dDoS attacks.

ICT failure due to data traffic
Criminals can disturb the operation of systems (e.g. websites, e-mail services or computer networks) in several ways. (d)DoS attacks and spamming are two important phenomena that have shown enormous worldwide growth. A (distributed) Denial of Service or (d)DoS attack involves intentionally sending massive quantities of data to systems,

153 We use the term service performer to avoid confusion with the term 'service provider' (ISP).

overloading them and making them unavailable. It is a tool that is deployed to blackmail companies, for instance, but may also represent an expression of protest, revenge, competition and vandalism. Spamming in the form of mass e-mails can also cause system failures, but this is mainly a side-effect of digital marketing and advertising (e.g. for lifestyle products and non-prescription drugs), rather than a concrete objective. Internet fraud involves sending massive quantities of phishing e-mails in order to obtain confidential information from people. That information is then used to extort their money. Hackers provide support for both dDoS attacks and spamming, or execute sub-tasks with the aim of causing targeted failures.

ICT failure due to data and system manipulation
Failures can also be caused directly by the actual manipulation of (damaging, deleting, changing or destroying) data and systems. Malware is the umbrella term for dubious '*…computer programmes that run on a computer without authorisation from the owner or administrator and cause the system to do something an outsider wants it to do*' (KLPD, DNRI, 2007a: 15). Such programmes are tailor-made by experts and, entirely unnoticed, collect confidential user information, damage data and systems (the infamous viruses), or grant external access to computers (via the modern viruses called Trojan horses). It is also possible to block or change entire websites (defacing), among other things, as a way to swindle (e.g. internet fraud by means of fake websites) and extort money from people or to express one's discontent (hacktivism). Only when ICT systems that control vital infrastructures (such as transport systems, control systems in the chemical sector or important crisis and information services) are damaged for political reasons in order to cause large-scale social disruption, this report refers to a cyber-terrorist attack. While no concrete attempts have been made to date, (vengeful) insiders with knowledge of and access to the operating systems represent a significant threat in particular (see also service performers).

Service performers
The use of ICT service performers has a direct relationship to organised crime. Criminals and terrorists hire the knowledge of experts to, for instance, protect their communications against criminal investigation or develop tools to facilitate criminal or terrorist activities (such as the intentional creation, sale, distribution or availability of a technical tool, password or code to gain access to an automated system). This report distinguishes between three types of service performance: corruption of ICT personnel, infiltration by criminal ICT workers, and hiring ICT experts. People with ICT authorisations that have access to sensitive company data may render assistance (through bribery or threat) to criminal parties from inside an organisation. This is called corruption

and mutual involvement of the upper and underworlds. While the threat of corrupt IT workers seems limited in the Netherlands at this time, criminal infiltration by ICT consultants and hiring experts for certain tasks (e.g. hackers) constitute a significant security risk.

What is known about the perpetrators?

Systematically mapping perpetrator characteristics in the form of risk indicators (the prototype offender profile) is called *profiling*. In terms of development and usability, however, profiling techniques are still in their infancy. This technique does not lead directly to the identification of the perpetrator(s) of a crime, but provides a description of *combinations of properties* that perpetrators are likely to have. At this time, insufficient research data is available about the effectiveness of using risk profiles (see also Van Donselaar and Rodrigues, 2006: 43, 58). It is clear that a combination of general and specific perpetrator characteristics that are sufficiently distinctive is required.

The disadvantage of risk profiles is that they confirm prejudices about certain people and groups. Both prevention and investigation will devote a disproportionate amount of attention to known risk groups, which may lead to stigmatisation of innocents (that just happen to match the characteristics) whilst simultaneously allowing real criminals to remain 'invisible' and untouched if it just so happens that they do not match the profile. As such, the profiling technique is certainly not perfect; its use requires a certain level of caution and nuance. As a preventive and investigative tool, risk profiles must be used with great care and restraint. However, an understanding of perpetrator characteristics may offer a starting point in both the prevention and tracing of high-tech crime. Further research will have to demonstrate this. Since perpetrator characteristic mapping onto profiles is not yet supported from an empirical perspective and validated instruments are lacking at this time, this report speaks of understanding the type of people that commit high-tech crimes instead of using the term 'offender profiles'.

The lack of knowledge concerning the perpetrators in a so-called 'intelligence database' is one important reason for the failure to develop perpetrator or offender profiles. One of the aims of this study was therefore to compile an inventory of existing knowledge about people and groups that commit high-tech crimes on the basis of national and international literature. In Chapter 3 we mapped perpetrator characteristics for a selection of high-tech crime phenomena whose threat and risks to Dutch society are considered most urgent:[154] (1) radicalisation

154 The perpetrator characteristics for the other phenomena of high-tech crime are described in Annex 4.

and extremism, (2) terrorism and ideologically motivated crime, (3) child pornography, (4) grooming, (5) software piracy, (6) internet fraud, (7) money laundering, (8) cyber terrorism, (9) hacking, (10) malware, and (11) ICT service performers.

Among other things, this inventory demonstrated that *internet fraud* and *hacking* in particular are criminal phenomena that are often committed in combination with other forms of high-tech crime. Terrorism, child pornography, grooming, software piracy and internet fraud mainly involves male perpetrators. Most sexual offences (child pornography and grooming) are committed by white perpetrators, whilst terrorism and internet fraud primarily involve perpetrators of African and/or Asian descent. While a significant proportion of high-tech crimes is financially motivated, hackers and malware authors in particular have a range of motives for their criminal activities (they also do it because of the challenge, their ideology, power, revenge or vandalism). It is notable that corrupt ICT workers and criminals who are active in the field of terrorism, internet fraud, child pornography and hacking tend to have a criminal record. The diversity of phenomena and (limited) clues as to the perpetrators make it clear that it is impossible to speak of 'the' high-tech criminal, but rather of criminals that specialise in a certain field. However, because certain offences are facilitated by the same digital techniques it becomes easier for the criminal to realise larger profits by deploying the same techniques to commit multiple crimes at the same time.

We are forced to conclude, however, that fairly little knowledge on individual perpetrators of high-tech crime is available in the literature. The literature inventory offers nothing more than rough and incomplete perpetrator sketches based on a limited number of characteristics. If we compare the profile sketch with indicators such as those developed for the FBI (see also Annex 5), there is a clear lack of specific perpetrator knowledge in the literature, in terms of organisation (e.g. recruitment), execution (expertise), behaviour (including personal characteristics) as well as the resources used. Moreover, for most phenomena of high-tech crime we also lack an understanding of the criminal career of perpetrators and the overlap between the various forms of high-tech crime. The information that *is* available in the literature is generally superficial, unstructured and limited, and in some cases based on anecdote and hypotheses of which the reliability and validity are difficult or impossible to establish. In short, there is a lack of empirical scientific research into perpetrator characteristics which clarifies the distinction between the separate phenomena of high-tech crime. A more elaborate understanding of perpetrators can be achieved by means of more problem-targeted research (e.g. case studies). A literature inventory alone

is clearly not enough to make well-founded statements about people and groups that commit high-tech crimes.

Can we speak of organised high-tech crime?

There are indications that organised crime exists for some phenomena of high-tech crime. In this report, we speak of organised crime if: '…*groups focus mainly on illegal [financial or material] gain and systematically commit crimes with serious consequences for society*' (Parlementaire Enquêtecommissie Opsporingsmethoden, Annex VII, 1996; Fijnaut et al., 1998; Kleemans et al., 1998: 22-23). While little is known in the literature about perpetrator groups committing high-tech crime (the understanding of perpetrators is relatively limited), there are clues that both traditional criminal networks (such as the Russian and Eastern European mafia) are involved that hire the required expertise externally, and that new fluid high-tech (HT) criminal networks are involved in which experts (such as hackers and malware authors) perform sub-tasks and bundle their forces. The KLPD (Boerman and Mooij, 2006) speaks of a trend towards *diversification* in which various forms of crime are committed simultaneously (e.g. hacking, botnets, spamming, malware, pharming, dDoS attack, internet fraud, extortion) and a trend towards *specialisation of tasks* in which criminals deploy experts that are responsible for certain sub-tasks in committing an offence (e.g. developing the tools or creating fake websites).

An inventory was made in Chapter 4 on the involvement of organised crime in the phenomena of high-tech crime that were qualified as a threat to Dutch society (see also section 5.3). Of the phenomena prioritised in Chapter 3, child pornography, software piracy, internet fraud (advance-fee fraud and identity theft), money laundering, hacking and malware in particular, are financially lucrative fields of operation for both traditional and new fluid HT criminal networks. The profits are significant, especially when you consider the small amount of investment and risks involved. ICT service performers also increasingly have criminal intentions and become involved in organised crime. Young people with ICT knowledge are recruited at universities, computer clubs and via the internet to provide support to the malicious practices of criminals; as are graduates and IT employees. However, this does not necessarily mean that the criminal circuit itself may not possess adequate technical knowledge to commit serious crimes without outside help. Botnet trading in particular is an important market for organised crime. In the Netherlands, HT criminal networks operate mainly in the field of internet and advance-fee fraud. Moreover, the Netherlands is an important supplier of botnets (that are rented out at very high prices) and an

important target of dDoS attacks. Creators of viruses (malware and Trojan horses) in particular play a prominent part in this context to gain control of, and spy on, the systems of others. Modifying or destroying websites (defacing), and developing fake websites to which people are rerouted (pharming) are increasingly becoming crimes from which perpetrators also achieve considerable financial gain.

While in relation to radicalisation and terrorism, activities occur on a (locally) organised basis, traditional criminal networks are not involved. Nor does grooming (which is generally committed on an individual basis) involve organised high-tech crime; and no concrete cyber-terrorist activities have been detected as yet. Furthermore, KLPD research has not yielded any clues on collaboration between criminal and terrorist networks (Boerman and Mooij, 2006: 86). We should note, however, that terrorist networks *are* involved in a range of criminal activities, including high-tech crime as a means to finance their terrorist operations.

We can only conclude here that, as yet, too little can be said about organised high-tech crime based on this literature study. The inventory offers a general overview of the criminal activities (that are sometimes committed in combination), the level of expertise required, experts and service performers hired, and the transnational nature of high-tech crime with its international connections. It is expected that organised crime will increasingly move towards high-tech crime, implementing ever new trends and innovative techniques. However, specific knowledge concerning perpetrators and collaborations is lacking in the literature, and additional research (e.g. studies on criminal files and cases) is necessary to map organised crime in the field of high-tech crime more adequately.

What are the knowledge gaps concerning perpetrators?

Based on this literature inventory, we have established that little specific knowledge is available concerning perpetrators and criminal collaborations. The overview below classifies the findings in terms of current perpetrator knowledge on a scale from 1 (very limited knowledge) to 4 (very good knowledge). The prioritised high-tech crime themes are printed in bold type. The rows (from left to right) refer to the knowledge position concerning individual perpetrators; the columns (from top to bottom) list the knowledge as it relates to organized high-tech crime. As such, the overview provides a direct understanding of what is known, in the literature, of individual perpetrators and HT criminal networks for each variant.

Literature-based high-tech crime perpetrator knowledge

	Individual perpetrator characteristics			
HT criminal networks	Very limited	Moderate	Good	Very good
Very limited	**Animal rights activism** **Extreme right terrorism** **Software piracy** **Identity fraud** **Pharming (internet fraud)** **Money laundering** **Grooming** **Cyber terrorism** **Hacking** **Novice hacker** **Petty thief hacker** **Old guard hacker** **Virus writer hacker** **Professional criminal hacker** **Information warrior hacker** **Political activist hacker** **Malware** **ICT service performers** Medicine trade Arms/explosives trade Human trade Drug trade Fencing Illegal gambling Market manipulation Espionage Spamming dDoS attack Defacing	**Right-wing radicalism** **Islamic radicalism** **Islamic terrorism** **Cyberpunk hacker** **Internal hacker** Cyber stalkers Discrimination	-	-
Moderate	Shielding Extortion and blackmail	**Child pornography** **Advance-fee fraud**	-	-
Good	-	-	-	-
Very good	-	-	-	-

The overview shows that there is a *moderately good* understanding of child pornography and advance-fee fraud perpetrators (both in terms of individual perpetrators and for HT criminal networks); that there is *moderate* knowledge, for extreme-right and Islamic radical and terrorist movements, of individual perpetrator characteristics (but not HT criminal networks); and that there is also a *moderately good* understanding of individual perpetrator characteristics – but not for HT criminal networks) for several hacker variants (cyberpunk and internal hacker) and

behavioural offences (cyber stalking and discrimination).[155] While there may be some knowledge of HT criminal networks for some techniques (shielding, extortion, pharming), the individual perpetrators behind them are relatively invisible. Perpetrator knowledge is not qualified as good or very good for any of the phenomena of high-tech crime. It is notable that very limited knowledge is available in the literature on the perpetrator characteristics for most of the phenomena (the top-left cell in the table contains most of the phenomena). And for many of the phenomena characterised as a threat to Dutch society (animal rights activism, extreme right terrorism, software piracy, identity fraud, money laundering, grooming, a number of hacker types, malware creators and ICT service performers),[156] we can conclude that there is a lack of knowledge all together. This does not necessarily imply that such knowledge is unavailable to the law enforcement and intelligence services. After all, the conclusions of this report are based on a study of mostly public literature.

Expectations for the future

Increase in high-tech crime
In terms of high-tech crime, it is expected that both the number of victims and criminal profits will continue to grow over the next few years. Perpetrators change methods quickly and the trend of diversification (in which criminals focus on various activities at the same time) and task specialisation (in which specific expertise is deployed for criminal sub-tasks) will continue (NHTCC, quoted by KLPD/DNRI, 2007a: 36). It is also expected that criminal activities will focus more on specific targets (i.e. an individual or organisation); and especially on victims that have little or no technical knowledge of digital communication structures (e.g. the elderly) and have implemented inadequate security will be duped in particular (NHTCC, 2006b: 10-11).

The internet as a crime scene
Due to increased use of the internet (causing the market to grow) and the limited risk of being caught, illegal trade on and via the internet may expand further. Moreover, the increasing virtual money flows give rise to the expectation that internet fraud (and identity theft) will cause the greatest number of victims and the most important financial damage (Taylor et al, 2006: 357-383). The V-NDB2006 also described identity fraud

155 In relation to cyber stalking, collaborations are irrelevant due to the nature of the offence.
156 It is self-evident that there is no knowledge concerning the perpetrators of cyber terrorism since no such attacks have been made to date.

with the aid of phishing as going through a tumultuous development (Boerman and Mooij, 2006: 21, 30). The high ADSL density, which means that computers are connected to the internet virtually permanently, makes the Netherlands a particularly attractive area of operations for phishers. This involves not just cyber criminality but also phenomena of computer crime, such as spamming (Ianelli and Hackworth, 2005). More recently, phishing on the internet is based in part on botnets (networks of malware-infected computers that are then controlled by third parties from external locations). Botnets also play an important part in many other high-tech crime phenomena, thereby representing a significant threat (Europol, 15 June 2006). Since botnets are created on a smaller scale and focus on specific target groups, they are becoming more difficult to trace.[157]

The emergence of hackers as service performers

The deployment of ICT service performers and experts must be qualified as the most important development in the field of organised and high-tech crime. There are indications that criminal networks from Eastern Europe and Russia in particular hire hackers originating primarily in Western Europe. Through the years, hackers discovered that they can make a lot of hard, fast cash with their expertise. As a result, they have attracted attention from criminal networks and, in some cases, are likely to be members of such organisations. Many criminals who are interested in high-tech crime have an interest in botnets, for instance, putting the hackers that have access to such zombie networks in a special position. This has made hackers into important facilitators for criminal groups. They deliver a range of technical tools, such as back doors (to gain access to systems), Trojan horses and bots (to control computers externally), and complete botnets (armies of zombie computers that can be remote-controlled) to order. The multifunctional applications of *malware* and *botnets* in particular are strong drivers in the criminal market of high-tech crime: they are tailor-made and facilitate a range of criminal activities, such as dDoS attacks, phishing, spamming, internet fraud, and the distribution of child pornography. Particular causes of concern are the recruitment of young students (who are approached at universities, computer clubs and/or online forums), the corruption of highly qualified ICT personnel,[158] and the infiltration of criminals in ICT companies or e-commerce. A lack of knowledge concerning the perpetrators and the ways in which criminal groups deploy ICT in their operations cause considerable obstacles in criminal investigation and prosecution,

157 Because many botnets can be active simultaneously, their impact is not necessarily reduced.

158 Introducing a professional code for ICT workers has been a subject of discussion for several years (Rogers, 2001: 132-133).

which means that controlling this phenomenon causes serious concern (NDB2004, KLPD, DNRI).

Young people as a high-risk group
The younger generation and students with solid ICT knowledge and skills, as well as a sound understanding of the internet can be qualified as a particular high-risk group for high-tech crime. This applies especially for the possibility of being involved in organised crime, not just for criminal but also for terrorist collaborations (Europol, 2003; McAfee, 2006; Neve, 2007). Research has shown that computer crime (and some associated forms of cyber crime) perpetrators are becoming younger and are engaged in ever more complex activities (Europol, 2003: 116). Apart from the 'thrill' and the challenge, high-tech crime helps them make a lot of money. This may cause young people that may initially be qualified as part of a type of 'youth gang' to enter a criminal spiral from which it is difficult to escape.

Corruption within companies
The vulnerabilities that are created in companies when employees are careless about security measures or block or derange them intentionally is another phenomenon requiring attention. Because key processes in companies and government bodies are increasingly controlled by ICT, these organisations are forced to rely on experts with the skills and expertise to develop, manage and secure their systems. Persons with high-level ICT authorisations (engineers, system and data administrators) or access to sensitive and confidential data (e.g. customer and payment files) and employees of companies or organisations that are responsible for vital infrastructures and security (SCADA systems, criminal investigation services) represent a particular risk. This involves not just people who may be sensitive to corruption, but also vengeful (ex-)employees (internal hackers and CITIs) that can potentially cause serious damage. Companies also increasingly hire external IT consultants to build systems or software. If these people have criminal intentions or if criminals offer ICT services on the market as independent entrepreneurs, this may constitute a serious security risk.

Sub-cultures
Part of the social activities that used to be part of the 'physical world' now make use of ICT and digital technology. Virtual communities that use discussion forums, for instance, can sometimes be qualified as sub-cultures (hackers, scientists, youth gangs, paedophiles). These communities have their own identity, standards, values and interests, and in some cases even their own 'language' (the use of acronyms and symbols). This applies to young people with radical (Islamic or extreme right) ideas, for instance, as well as youngsters who have become part of the underworld of the hacker community. According to Turgeman-

Goldschmidt (2005), what starts as a form of entertainment may easily devolve and escalate into a criminal phenomenon. The increasing shift towards a digital society also means that some behaviour will result in excesses on the internet, for instance. We must devote attention to assessing a number of phenomena of high-tech crime that involve young people (radicalisation and extremism, software piracy, discrimination, hacking) in relation to sub-cultures and youth criminality. Social-psychological factors and group processes that are linked to the internet (e.g. moral development, family problems, social influence and sub-cultural group formation) are special areas of concern in this context (cf. NCTb, 2006b: 10; Yar, 2005b).

Literatuur

Internet/media nieuws en achtergronden

AD
Kinderporno Second Life 'smakeloos'
Publicatie 24 april 2007
Geraadpleegd op 4 juni 2007: www.adnl/economie/article1312939.ece

AD
Brussel wil nieuwe aanpak 'cybercrime'
Publicatie 21 mei 2007
Geraadpleegd op 22 mei 2007: www.adnl/economie/article1386553.ece

Bednarz, A.
Profiling cybercrime: A promising but immature science
Computerworld Malaysia, technology, jan/feb 2005
Geraadpleegd op 3 april 2007: www.computerworld.com.my/ShowPage.aspx?pagetype=2&articleid=280&pubid=4&issueid=32

Beek, Sj. van
Extremisme – Jihad en witte woede
Binnenlands Bestuur, jrg. 28, nr. 16, 2007: pp. 8-11

Biancuzzi, F.
Inside the Hacker's Profiling Project
Linux.com, 3 november 2006
Geraadpleegd op 8 maart 2007: http://software.newsforge.com/article.pl?sid=06/10/30/155251

Bolkestein, F.
Social engineering: van scalpel tot houwdegen
Filosofie Magazine, internetpublicatie, 2001
Laatst geraadpleegd op 13 november 2007: www.filosofiemagazine.nl/artikelDetail.lasso?ID=1917&-token.kop=ditnummer

Brein
Piraterij
Stichting Bescherming Rechten Entertainment Industrie Nederland, 2007
Laatst geraadpleegd op 18 juli 2007: http://anti-piracy.nl/piraterij/piraterij.asp

Brein
Politie pakt professionele piraat
Stichting Bescherming Rechten Entertainment Industrie Nederland, 2007b
Laatst geraadpleegd op 18 juli 2007: http://anti-piracy.nl/nieuws/bericht.asp?nieuwsberichtid=48

Business Software Alliance
Soorten Softwarepiraterij
Business Software Alliance, BSA, 2007
Geraadpleegd op 15 mei 2007: www.bsa.org/netherlands/antipiracy/types-of-piracy.cfm

Clarke, R.
Vulnerability: What are Al Qaeda's capabilities?
Internetpublicatie, 2003
Geraadpleegd op 16 mei 2007: www.pbs.org/wgbh/pages/frontline/shows/cyberwar/vulnerable/alqaeda.html

Computable
Identiteitsfraude grote kostenpost
Internetpublicatie, 16 januari 2007
Laatst geraadpleegd op 29 augustus 2007: www.computable.nl/nieuws.jsp?id=1834662

Computertaal
McAfee beschrijft volgende generatie bedreigingen in nieuwste editie van Global Threat Report
Internetpublicatie, 14 april 2007
Geraadpleegd op 14 mei 2007: www.computertaal.info/modules/news/article.php?storyid=1057

Cops
Apeldoorn: Politieacademie, Kennisnetwerk, 2007a
Reeks *Cops@cyberspace*, jrg. 11, nr. 10, 5 – 11 maart 2007

Cops
Apeldoorn: Politieacademie, Kennisnetwerk, 2007b
Reeks *Cops@cyberspace*, jrg. 11, nr. 11, 12 – 18 maart 2007

Cops
Apeldoorn: Politieacademie, Kennisnetwerk, 2007c
Reeks *Cops@cyberspace*, jrg. 11, nr. 12, 19 – 25 maart 2007

Cops
Apeldoorn: Politieacademie, Kennisnetwerk, 2007d
Reeks *Cops@cyberspace*, jrg. 11, nr. 13, 26 maart – 1 april 2007

Cops
Apeldoorn: Politieacademie, Kennisnetwerk, 2007e
Reeks *Cops@cyberspace*, jrg. 11, nr. 14, 2 – 8 april 2007

Cops
Apeldoorn: Politieacademie, Kennisnetwerk, 2007f
Reeks *Cops@cyberspace*, jrg. 11, nr. 15, 9-15 april 2007

Cops
Apeldoorn: Politieacademie, Kennisnetwerk, 2007g
Reeks *Cops@cyberspace*, jrg. 11, nr. 16, 16 – 22 april 2007

Cops
Apeldoorn: Politieacademie, Kennisnetwerk, 2007h
Reeks *Cops@cyberspace*, jrg. 11, nr. 18, 30 april – 6 mei 2007

Cops
Apeldoorn: Politieacademie, Kennisnetwerk, 2007i
Reeks *Cops@cyberspace*, jrg. 11, nr. 19, 7 – 13 mei 2007

Cops
Apeldoorn: Politieacademie, Kennisnetwerk, 2007j
Reeks *Cops@cyberspace*, jrg. 11, nr. 20, 14 – 27 mei 2007

Cops
Apeldoorn: Politieacademie, Kennisnetwerk, 2007k
Reeks *Cops@cyberspace*, jrg. 11, nr. 21, mei/juni 2007

Cops
Apeldoorn: Politieacademie, Kennisnetwerk, 2007l
Reeks *Cops@cyberspace*, jrg. 11, nr. 23, 4 – 10 juni 2007

Cops
Apeldoorn: Politieacademie, Kennisnetwerk, 2007m
Reeks *Cops@cyberspace*, jrg. 11, nr. 25, 18 – 24 juni 2007

De Tijd
800.000 euro gestolen bij fraude met internetbankieren in België
Elektronische publicatie 9 oktober 2007
Geraadpleegd op 9 oktober 2007: www.tijd.be/nieuws/ondernemingen/financien/artikel.asp?Id=3260230

De Volkskrant
'In Amsterdam zijn geen duizenden escortbureaus': De webcam-industrie wordt het volgende onderwerp van studie
Publicatie 23 augustus 2006

De Volkskrant
Gevangen in een botnet van zombies
Publicatie 25 augustus 2006

De Volkskrant
Wikipedia gebruikt om virus te verspreiden
Publicatie 6 november 2006

E-crime congress
Who's Who? Tackling Identity and Online Fraud
The fifth annual e-crime congress, Londen, 27-28 maart 2007
Laatst geraadpleegd op 29 augustus 2007:
www.e-crimecongress.org/ecrime2007/website.asp

Ejure
Extremisme op internet
Internetpublicatie, 2007
Geraadpleegd op 25 april 2007: www.ejure.nl/dossier_id=242/f_dossier/dossier.html

Elsevier
Europol gaat islamitische terreursites aanpakken
Internetpublicatie, 9 mei 2007
Geraadpleegd op 12 juni 2007:
www.elsevier.nl/nieuws/internet_en_gadgets/artikel/asp/artnr/151674/zoeken/ja/index.html

Ernst & Young
Money transfer
Internetpublicatie, 2006
Geraadpleegd op 8 mei 2007: www.ey.nl/download/overig/money_transfer.pdf

Europese Commissie
Instellingen en andere organen van de Europese Unie
Internetpublicatie, 2007
Geraadpleegd op 13 juni 2007: www.europa.eu/institutions/inst/comm/index_nl.htm

Europol
Computer crime experts gathered at Europol
Internetpublicatie, 15 juni 2006
Geraadpleegd op 14 mei 2007: www.europol.europa.eu/index.asp?page=news&news=pr060615b.htm

Fox-IT
Systeembeheerders doelwit criminelen
Internetpublicatie, 29 januari 2004
Geraadpleegd op 14 maart 2007: www.fox-it.com/content/view/338/99/lang,nl/

Fox-IT
Crimineel in de pc
Internetpublicatie, 26 februari 2004
Geraadpleegd op 14 maart 2007: www.fox-it.com/content/view/336/99/lang,nl/

G8
Meeting of G8 Justice and Home Affairs Ministers
Internetpublicatie, Washington, 11 mei 2004
Laatst geraadpleegd op 13 juni 2007: www.usdoj.gov/criminal/cybercrime/g82004/index.html

Home
Politie Delft pakt bende internetoplichters op
Internetpublicatie, 3 mei 2007
Geraadpleegd op 10 mei 2007: www.home.nl/nieuws/tech/artikel/00294049

Internetoplichting.nl
Oplichter '419-fraude' aangehouden
Internetpublicatie, 4 februari 2007
Geraadpleegd op 2 mei 2007: www.internetoplichting.nl/cgi-bin/yabb/YaBB.cgi?num=1175718367

Interpay
M-commerce services
Internetpublicatie, 2007
Geraadpleegd op 16 mei 2007: www.interpay.nl/Services_nieuw/M-commerce_Services/

Interpol
Financial and high-tech crimes
Internetpublicatie, 2007
Geraadpleegd op 14 mei 2007: www.interpol.int/Public/FinancialCrime/Default.asp

Ius mentis
Wat zegt u? Smaad op internet
Internetpublicatie, 27 oktober 2006
Laatst geraadpleegd op 4 juni 2007: www.iusmentis.com/maatschappij/smaad/

Ius mentis
De Wet computercriminaliteit: wat is computercriminaliteit?
Internetpublicatie, 6 oktober 2006
www.iusmentis.com/beveiliging/hacken/computercriminaliteit/cybercrime/

KLPD
Meldpunt cybercrime, 2007
Geraadpleegd op 29 maart 2007: www.meldpuntcybercrime.nl/

Kortekaas, J.J.C.
ICT leidt niet tot veranderingen in georganiseerde criminaliteit
Persbericht, Universiteit Leiden, 31 mei 2005
Geraadpleegd op 8 maart 2007: www.nieuws.leidenuniv.nl/index.php3?c=501

McCandless, D.
Bad trip for online drug peddlers
Internetpublicatie, 7 juni 2005
Geraadpleegd op 22 mei 2007: www.wired.com/print/medtech/health/news/2005/07/68049

Metro
Spyware op helft alle pc's
Publicatie 7 maart 2007

Metro
'Mag ik jou fotograferen in je onderbroekje?': Metro-verslaggeefster doet zich voor als 12-jarig meisje op chatsites en wordt overspoeld met oneerbare voorstellen
Publicatie 20 maart 2007

Metro
Steeds meer sites met kinderporno
Publicatie 18 april 2007

Metro
Hogere strafeisen tegen kinderporno
Publicatie 1 mei 2007

Metro
Online diefstal lucratiever dan drugsverkoop
Publicatie 9 mei 2007a

Metro
'Ik weet dat ik fout zit'
Publicatie 9 mei 2007b

Metro
Pedofiel gepakt na internetdate
Publicatie 16 mei 2007

Metro
Oudere jeugd downloadt vaakst illegale bestanden
Publicatie 27 juni 2007
Ministerie van Justitie
Kansspelen via internet
Website geraadpleegd op 14 mei 2007: www.justitie.nl/onderwerpen/opsporing_en_handhaving/kansspelen/internet_kansspelen/
MKB-net
Amerikaans grootwinkelbedrijf TJX is slachtoffer van hackers
Internetpublicatie, 7 april 2007
Geraadpleegd op 10 april 2007: http://mkbnet.nl/archief/55081
Zie ook: http://extern.mdinfo.nu/demo/?query=hackers
Netkwesties
Belegger gedaagd voor online leugens en afpersing
Internetpublicatie, 8 mei 2006
Geraadpleegd op 8 maart 2007: www.netkwesties.nl/editie144/artikel1.html
Netkwesties
Cybercrime-eenheid in de knop gebroken
Internetpublicatie, 24 augustus 2006
Geraadpleegd op 10 mei 2007: www.netkwesties.nl/editie145/artikel1.html
Nova
Shell gehackt via computers Russische geheime dienst
Publicatie 19 januari 2006
Geraadpleegd op 29 maart 2007: www.novatv.nl/index.cfm?ln=nl&fuseaction=artikelen.details&achtergrond_id=8317
NRC Handelsblad
De opmars van het hacktivisme
Publicatie 29 januari 1999
Geraadpleegd op 8 maart 2007: www.nrc.nl/W2/Lab/Beveiliging/hackers29011999.html
NRC Handelsblad
Internet: gokken
Publicatie 11 maart 1999
Geraadpleegd op 14 mei 2007: www.nrc.nl/W2/Lab/Profiel/internet99/gokken.html
NRC Handelsblad
CIA in paniek door inbraak in Lotus Notes
Publicatie 1 augustus 2000
Geraadpleegd op 8 maart 2007: www.nrc.nl/W2/Lab/Beveiliging/000801-b.html
NRC Handelsblad
De opmars van cyberprotest: hackers verminken websites met politieke boodschappen
Publicatie 25 augustus 2006

Nu.nl
Piraterij kost Amerikaanse economie jaarlijks 15 miljard euro
Publicatie 30 september 2006
Laatst geraadpleegd op 29 maart 2007: www.nu.nl/news/837650/54/Piraterij_kost_Amerikaanse_economie_jaarlijks_15_ miljard_euro.html

Nu.nl
FIOD rolt internethandel in neppillen op
Publicatie 23 november 2006
Laatst geraadpleegd op 3 oktober 2007: www.nu.nl/news/897210/50/rss/FIOD_rolt_internethandel_in_neppillen_op.html

OM
De zaak afpersing Campina
Internetpublicatie, Openbaar Ministerie, oktober 2005
Geraadpleegd op 8 maart 2007: www.om.nl/over_het_om/de_officier_van_justitie/de_zaak/21035/

OM
Bende internetoplichters opgerold
Internetpublicatie, Openbaar Ministerie, 26 september 2006
Geraadpleegd op 28 maart 2007: www.om.nl/computercriminaliteit/_computercriminaliteit_persberichten/30281/

OM
Team High Tech Crime houdt hacker van computerspellen aan
Internetpublicatie, Openbaar Ministerie, 2007
Geraadpleegd op 8 mei 2007: www.om.nl/computercriminaliteit/_computercriminaliteit_persberichten/31568/

OM
Landelijk Parket
Internetpublicatie, Openbaar Ministerie, 2007b
Geraadpleegd op 11 juni 2007: www.om.nl/parket/landelijk/

Planet internet
Politie telt 470 illegale kansspelen online
Internetpublicatie, 19 september 2005
Geraadpleegd op 14 mei 2007: www.planet.nl/planet/show/id=118880/contentid=621126/sc=190f97

Planet internet
Justitie wil links naar goksites verbieden
Internetpublicatie, 16 februari 2006
Geraadpleegd op 14 mei 2007: www.planet.nl/planet/show/id=118880/contentid=683330/sc=01569c

Planet internet
Achtergrond: rootkits
Internetpublicatie, 17 mei 2006
Geraadpleegd op 14 mei 2007: www.planet.nl/planet/show/id=112030/contentid=713079/sc=1e3edc

Politieacademie
Financieel-economische criminaliteit
Internetpublicatie, 2007
Geraadpleegd op 15 mei 2007: http://thesaurus.politieacademie.nl/word.php?id=4703

Samut, H.
Through a looking glass darkly
Alert communications, 2000
Geraadpleegd op 16 mei 2007: www.alert.com.mt/printpage.asp?p=197&l=1&i=166

Security.nl
Tweede Kamer: geen doorstart High Tech Crime Center
Internetpublicatie, 25 oktober 2006
Geraadpleegd op 14 mei 2007: www.security.nl/article/14689/1

Security.nl
Via spam aangeboden afslankpillen levensgevaarlijk
Internetpublicatie, 5 maart 2007
Geraadpleegd op 8 maart 2007: www.security.nl/article/15597/1/%22Via_spam_aangeboden_afslankpillen_levensgevaarlijk%22.html

Security.nl
Drugsdealers vinden nieuwe bestemming op internet
Internetpublicatie, 25 april 2007
Geraadpleegd op 10 mei 2007: www.security.nl/article/15945/1/%22Drugsdealers_vinden_nieuwe_bestemming_opinternet%22.html

Security.nl
Hackers namen Chinese TV over?
Internetpublicatie, 3 mei 2007
Geraadpleegd op 10 mei 2007: www.security.nl/article/15984/1

Security.nl
Politie arresteert student wegens oproep tot dDoS-aanval
Internetpublicatie, 8 mei 2007
Geraadpleegd op 10 mei 2007: www.security.nl/article/15998/1

Security.nl
Air marshals in gevaar door verloren TSA harde schijf
Internetpublicatie, 9 mei 2007
Geraadpleegd op 10 mei 2007: www.security.nl/article/16005/1

Spits
Spam is onstuitbaar
Publicatie 13 maart 2007

Spits
Pas op voor cyberseks
Publicatie 9 mei 2007

Tweakers.net
Estland beschuldigt Rusland van dDoS-aanval
Internetpublicatie, 14 mei 2007

Laatst geraadpleegd op 20 juli 2007:
http://tweakers.net/nieuws/47539/Estland-beschuldigt-Rusland-van-ddos-aanval.html

US Department of Justice
Former navy contractor sentenced for damaging navy computer system
Elektronische publicatie, 5 april 2007
Geraadpleegd op 22 mei 2007: www.cybercrime.gov/sylvestreSent.pdf

Vnunet
2007 to bring video viruses: McAfee publishes 10 security predictions for next year
Internetpublicatie, 30 november 2006
Geraadpleegd op 10 mei 2007: www.vnunet.com/vnunet/news/2169898/2007-bring-video-viruses

Walker, C.
Russian mafia extorts gambling websites
Internetpublicatie, juni 2004
Laatst geraadpleegd op 20 juli 2007: www.americanmafia.com/Feature_Articles_270.html

Webwereld
'Nederlander bedreigde 180Solutions'
Internetpublicatie, 4 november 2005
Geraadpleegd op 14 mei 2007: www.webwereld.nl/articles/38181

Webwereld
Amsterdammer ontvoerd na internetafspraak
Internetpublicatie, 8 mei 2006
Geraadpleegd op 8 mei 2007:
www.webwereld.nl/articles/41037/amsterdammer-ontvoerd-na-internetafspraak.html

Webwereld
Vierde zaak tegen botnet-hackers verdaagd
Internetpublicatie, 17 augustus 2006
Geraadpleegd op 14 mei 2007: www.webwereld.nl/ref/rss/42469

Webwereld
Celstraffen geëist tegen botnet-hackers
Internetpublicatie, 16 januari 2007
Geraadpleegd op 14 mei 2007: www.webwereld.nl/articles/44587/toxbot

Webwereld
Cyberboeven opgepakt in Amsterdam
Internetpublicatie, 12 februari 2007
Geraadpleegd op 8 mei 2007:
www.webwereld.nl/articles/45026/cyberboeven-opgepakt-in-amsterdam.html

Webwereld
Hoofdverdachte in botnet-zaak in hoger beroep
Internetpublicatie, 14 februari 2007
Geraadpleegd op 14 mei 2007: www.webwereld.nl/ref/rss/45048

ZDNet.com
Mafia insiders infiltrating firms, U.K. cops warn
Internetpublicatie, 25 april 2006
Laatst geraadpleegd op 20 juli 2007: http://news.zdnet.com/2102-1009_22-6064954.html

Wetenschappelijke bijdragen en onderzoekspublicaties

Adamsky, A.
Crimes related to the computer network. Threats and opportunities: A criminological perspective. In: M. Rogers. *A new hacker taxonomy (revised version)*
Publicatie 2000: p. 7
Geraadpleegd op 3 april 2007: http://homes.cerias.purdue.edu/~mkr/hacker.doc

AIVD
Saoedische invloeden in Nederland; verbanden tussen salafistische missie, radicaliseringsprocessen en islamitisch terrorisme (elektronische versie)
Den Haag: Algemene Inlichtingen- en Veiligheidsdienst, 2004

AIVD
Van dawa tot jihad: De diverse dreigingen van de radicale islam tegen de democratische rechtsorde
Den Haag: Algemene Inlichtingen- en Veiligheidsdienst, 2004b

AIVD
Dierenrechtenactivisme in Nederland: Grenzen tussen vreedzaam en vlammend protest (elektronische versie)
Den Haag: Algemene Inlichtingen- en Veiligheidsdienst, 2004c

AIVD
Nota 'Dierenrechtenactivisme in Nederland' (elektronische versie)
Den Haag: Algemene Inlichtingen- en Veiligheidsdienst, 2004d

AIVD
De gewelddadige jihad in Nederland: Actuele trends in de islamitisch-terroristische dreiging (elektronische versie)
Den Haag: Algemene Inlichtingen- en Veiligheidsdienst, 2006a

AIVD
Algemene Inlichtingen- en Veiligheidsdienst: Jaarverslag 2006 (elektronische versie)
Den Haag: Algemene Inlichtingen- en Veiligheidsdienst, 2006b

AIVD
Dierenrechtenactivisme in Nederland, springplank voor Europa (elektronische versie)
Den Haag: Algemene Inlichtingen- en Veiligheidsdienst, 2007

Alberdingk Thijm, Ch.A.
Kroniek van technologie en recht
Nederlands Juristenblad, nr. 13, 2007, pp. 837-847

Alexy, E.M., A.W. Burgess, T. Baker
Internet offenders: Traders, travelers, and combination trader-travelers
Journal of Interpersonal Violence, jrg. 20, nr. 7, 2005, pp. 804-812

Alison, L., C. Mclean, L. Almond
Profiling suspects. In: T. Newburn, T. Williamson, A. Wright (red.)
Handbook of Criminal Investigation
Cullompton, Devon: Willan Publishing, 2007, pp. 493-516

Amersfoort: van, L. Smit, M. Rietveld
Criminaliteit in de virtuele ruimte
Zeist, Kerckebosch, 2002
Reeks Politie en Wetenschap

Bakker, E.
Jihadi terrorists in Europe, their characteristics and the circumstances in which they joined the jihad: an exploratory study
Den Haag: Nederlands Instituut voor Internationale Betrekkingen Clingendael, 2006

Benschop, A.
CyberJihad internationaal: Waarom terroristen van internet houden
Sociosite (2001-heden), 2006
Laatst geraadpleegd op 24 juli 2007: www.sociosite.org/jihad_int.php

Benschop, A.
Cyberterrorisme: dodelijk geweld vanaf het toetsenbord
Sociosite (2001-heden), 2007
Geraadpleegd op 18 april 2007: www.sociosite.org/terrorisme.php

Benschop, A.
Cyberstalking: belaagd op het internet
Sociosite (2002-heden), 2007b
Geraadpleegd op 16 mei 2007: www.sociosite.org/cyberstalking.php

Blok-Tip, L., H. Vogelpoel, M.J. Vredenbregt, D.M. Barends, D. de Kaste
Counterfeits and imitations of Viagra® and Cialis® tablets: trends and risks to public: A survey of the analyses carried out at the Dutch National Institute for Public Health and the Environment in the time period 2000-2004
Bilthoven, RIVM rapport 267041001, 2005

Boerman, F., A. Mooij
Vervolgstudie nationaal dreigingsbeeld: Nadere beschouwing van potentiele dreigingen en witte vlekken uit het nationaal dreigingsbeeld 2004
Zoetermeer, KLPD, DNRI, 2006

Bovenkerk, F., e.a.
Bedreigingen in Nederland (elektronische versie)
Utrecht: Willem Pompe Instituut, Universiteit Utrecht, augustus 2005
Laatst geraadpleegd op 4 juni 2007: www.politieenwetenschap.nl/pdf/bedreigingen_in_nederland.pdf

Broadhurst, R.G.
International cooperation in cyber-crime research (paperpresentatie)
11th UN Congress on crime prevention and criminal justice
Thailand, Bangkok, 2005

Bruinsma, M.Y, J.A. Moors
Illegale vuurwapens: Gebruik, bezit, en handel in Nederland 2001-2003
Tilburg, IVA Beleidsonderzoek en advies, 2005

Bunt, H.G. van de, E.R. Kleemans
Georganiseerde criminaliteit in Nederland, derde rapportage op basis van de Monitor Georganiseerde Criminaliteit
Den Haag, Ministerie van Justitie-WODC / Boom Juridische uitgevers, 2007, Reeks Onderzoek en beleid, nr. 252

Burt, R.S.
Structural holes and good ideas
Americal Journal of Sociology, nr. 110, 2003, pp. 349-399

Burt, R.S.
Structural holes: The social structure of competition
Cambridge, MA: Harvard University Press, 1992

Casey, E.
Cyberpatterns: Criminal behavior on the internet. In: B.E. Turvey, *Criminal profiling: An introduction to behavioral evidence analysis*
San Diego: Academic Press, 2002, pp. 547-572

Chantler, N.
Profile of a computer hacker. In: M. Rogers, *A new hacker taxonomy (revised version)*
Internetpublicatie, 2000: 4-5
Geraadpleegd op 3 april 2007: http://homes.cerias.purdue.edu/~mkr/hacker.doc

Chau, M., J. Xu
Mining communities and their relationship in blogs: A study of online hate groups
International Journal of Human-Computer Studies, jrg. 65, 2007: 57-70

Chiesa, R., S. Ducci
Hackers Profiling Project
Internetpublicaties, 2006
Geraadpleegd op 3 april 2007: http://hpp.recursiva.org/en/index.php
Geraadpleegd op 8 maart 2007: http://hpp.isecom.org

Choo, K.K.R.
Zombies and botnets
Trends & Issues in Crime and Criminal Justice, nr. 333, 2007, pp. 1-6

Coleman, J.
Social capital in the creation of human capital
American Journal of Sociology, jrg. 94, supplement, 1988, pp. S95-S-120

Copes, H., L. Vieraitis
Identity Theft: Assessing Offenders' Strategies and Perceptions of Risk
Paper submitted to the U.S. Department of Justice
Birmingham, University of Alabama, 2007

Dijkshoorn, B.A., F.J. Erkens, S. Heij, H.M.P. Kersten, A. Ponjee
Aard en omvang verkrijgbaarheid van verboden slag-, steek- en stootwapens in Nederland
Den Haag, WODC/Ministerie van Justitie, 2007

Donselaar, J. van, P.R. Rodrigues (red.)
Monitor racisme & extremisme: zevende rapportage
Amsterdam, Anne Frank Stichting, 2006

Donselaar, J. van, W. Wagenaar
Monitor racisme & extremisme: Racistisch en extreemrechts geweld in 2006
Amsterdam, Anne Frank Stichting, 2007

Drucker, S.J., G. Gumpert
Cybercrime and punishment
Critical Studies in Media Communication, jrg. 17, nr. 2, 2000, pp. 133-158

Durkin, K.F.
Misuse of the internet by pedophiles: Implications for law enforcement and probation practice. In: E.M. Alexy, A.W. Burgess, T. Baker, Internet offenders: traders, travelers, and combination trader-travelers
Journal of Interpersonal Violence, jrg. 20, nr. 7, 2005, pp. 804-812

Europol
Computer-related crime within the EU: Old crimes new tools, new crimes old tools
Luxemburg, Office for Official Publications of the European Communities, 2003

Europol
EU Terrorism situation and trend report TE-SAT 2007 (elektronische versie)
Den Haag, Europol, 2007a
Laatst geraadpleegd op 24 mei 2007: www.europol.europa.eu/publications/TESAT/TESAT2007.pdf

Europol
EU Organised Crime Threat Assessment (OCTA) 2007 (elektronische versie)
Den Haag, Europol, 2007b
Laatst geraadpleegd op 20 juli 2007: www.europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_(OCTA)/OCTA2007.pdf

Fafinski, S.
In the back of the net: football hooliganism and the internet. In: Y. Jewkes (red.) *Crime Online*
Portland, Oregon, Willan Publishing, 2007, pp. 109-127

Fidis
D7.2: Descriptive analysis and inventory of profiling practices
Profiling, Future of identity in the information society, 29 juni 2005
Geraadpleegd op 22 mei 2007: www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.2.profiling_practices.pdf

Fijnaut, C., F. Bovenkerk, G. Bruinsma, H. van de Bunt
Organised crime in the Netherlands
Den Haag, Londen, Boston, Kluwer Law International, 1998

Furnell, S.M.
The problem of categorising cybercrime and cybercriminals
(paperpresentatie)
2nd Australian Information Warfare (IW) and Security Conference (SC)
Perth, Australië, 29-30 november 2001

Furnell, S.
Hackers: anti-heroes of the computer revolution? In: S. Furnell
Cybercrime: Vandalizing the information society
Londen, Pearson Education Limited, 2002, pp. 41-94

Gelderblom, B.
Dubieuze informatie en waren op internet. In: B. Gelderblom,
Computercrime: over stalkers, struikrovers en sluipmoordenaars op de digitale snelweg
Amsterdam, Pearson Education Benelux, 2004, pp. 89-107

Gelderblom, B.
Afpersing op internet. In: B. Gelderblom, *Computercrime: over stalkers, struikrovers en sluipmoordenaars op de digitale snelweg*
Amsterdam, Pearson Education Benelux, 2004, pp. 123-131

Gelderblom, B.
Georganiseerde misdaad op internet. In: B. Gelderblom, *Computercrime: over stalkers, struikrovers en sluipmoordenaars op de digitale snelweg*
Amsterdam, Pearson Education Benelux, 2004: 193-201

Gelderblom, B.
Internetstalkers. In: B. Gelderblom, *Computercrime: over stalkers, struikrovers en sluipmoordenaars op de digitale snelweg*
Amsterdam, Pearson Education Benelux, 2004, pp. 215-221

Goldberg, I.K.
Glossary of information warfare terms
Internetpublicatie, 5 maart 2005
Geraadpleegd op 16 mei 2007: www.psycom.net/iwar.2.html

Goodman, S.E., J.C. Kirk, M.H. Kirk
Cyberspace as a medium for terrorists
Technological Forecasting & Social Change, nr. 74, 2007, pp. 193-210

Gordon, S., R. Ford
On the definition and classification of cybercrime
Journal in Computer Virology, nr. 2, 2006, pp. 13-20

Gordon, G.R., C.D. Hosmer, C. Siedsma, D. Rebovich
Assessing technology, methods, and information for committing and combating cyber crime (elektronische versie)
Rockville, the computer forensics research & development center (CFRDC), 4 februari 2002
Laatst geraadpleegd op 23 mei 2007: www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf

Govcert
Van herkenning tot aangifte: Handleiding cybercrime
Den Haag, Govcert.nl, KLPD, 2006

Govcert
Trendrapport 2007: Cybercrime in trends en cijfers (elektronische versie)
Den Haag, Govcert.nl, 11 juni 2007
Laatst geraadpleegd op 13 juni 2007: www.govcert.nl/render.html?it=156

Grabosky, P.
The global dimension of cybercrime
Global Crime, jrg. 6, nr. 1, 2004, pp. 146-157

Grabosky, P.
Computer crime: a criminological overview (paperpresentatie)
10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders
Wenen, Oostenrijk, 15 april 2000
Laatst geraadpleegd op 24 mei 2007: www.aic.gov.au/conferences/other/grabosky_peter/2000-04-vienna.pdf

Granovetter, M.S.
The strength of weak ties
American Journal of Sociology, jrg. 78, nr. 6, 1973, pp. 1360-1380

Helmus, S., A. Smulders, F. van der Zee
ICT Veiligheidsbeleid in Nederland – Analyse en overwegingen bij herijking
TNO rapport nr. 035.31231, 2006

Higgins, G.E.
Digital piracy, self-control theory, and rational choice: An examination of the role of value
International Journal of Cyber Criminology, jrg. 1, nr. 1, 2007, pp. 33-55

Higgins, G.E.
Can low self-control help with the understanding of the software piracy problem?
Deviant Behavior, nr. 26, 2005, pp. 1-24

Hollinger, R.
Computer hackers follow a guttman-like progression. In: M. Rogers, *A new hacker taxonomy*, revised version, 2000 (elektronische versie: pp. 3-4)
Geraadpleegd op 3 april 2007: http://homes.cerias.purdue.edu/~mkr/hacker.doc

Holt, T.J., D.C. Graves
A qualitative analysis of advance fee fraude e-mail schemes
International Journal of Cyber Criminology, jrg. 1, nr. 1, 2007, pp. 137-154
Ianelli, N., A. Hackworth
Botnets as a vehicle for online crime
Pittsburgh PA, CERT Coordination Center, International High Technology Crime Investigation Association (HTCIA), 2005
Geraadpleegd op 14 mei 2007: www.htcia.org
Inspectie voor de Gezondheidszorg
Handel in geneesmiddelen via internet (elektronische publicatie)
Den Haag, augustus 2004
Geraadpleegd op 26 september 2007:
www.igz.nl/32414/2004-08-handel_in_geneesmid1.pdf
Jewkes, Y., C. Andrews
Internet child pornography: International responses. In: Y. Jewkes (red.) *Crime Online*
Portland, Oregon, Willan Publishing, 2007, pp. 60-80
Jolls, C., C.R. Sunstein, R.H. Thaler
A behavioral approach to law and economics
Stanford Law Review, nr. 50, pp. 1471-1550
Jordan, T.: Taylor
A sociology of hackers
The Sociological Review, jrg. 46, nr. 4, 1998, pp. 757-780
Khong, D.W.K.
An economic analysis of spam law
Erasmus Law and Economics Review, jrg. 1, vol. 1, 2004, pp. 23-45
Kleemans, E.R., E.A.I.M. van den Berg, H.G. van de Bunt
Georganiseerde criminaliteit in Nederland: Rapportage op basis van de WODC-monitor
Den Haag, WODC, 1998
Kleemans, E.R., M.E.I. Brienen, H.G. van de Bunt, R.F. Kouwenberg, G. Paulides, J. Barensen
Georganiseerde criminaliteit in Nederland, tweede rapportage op basis van de WODC-monitor
Den Haag, Ministerie van Justitie-WODC / Boom Juridische uitgevers, 2002
Reeks Onderzoek en beleid, nr. 198
KLPD, DNR
Criminaliteitsbeeld 2005 (elektronische versie)
Driebergen, 2005
Laatst geraadpleegd op 24 juli 2007: www.om.nl/files/file.php5?id=383
KLPD, DNRI
Nationaal dreigingsbeeld zware of georganiseerde criminaliteit: een eerste proeve
Zoetermeer, Dienst Nationale Recherche Informatie, 2004

KLPD, DNRI
Identiteitsfraude met behulp van phishing op internet: verslag van een onderzoek voor de vervolgstudie NDB (intern rapport)
Zoetermeer, Dienst Nationale Recherche Informatie, 2007a

KLPD, DNRI
Afpersing door middel van (dreigen met) een dDoS-aanval: verslag van een onderzoek voor de vervolgstudie NDB (intern rapport)
Zoetermeer, Dienst Nationale Recherche Informatie, 2007b

KLPD, DNRI
Corruptie van ICT-personeel: verslag van een onderzoek voor de Vvervolgstudie NDB (intern rapport)
Zoetermeer, Dienst Nationale Recherche Informatie, 2007c

Kohlmann, E.F.
The real online terrorist threat
Foreign Affairs / Council on Foreign Relations, jrg. 85, nr. 5, 2006, pp. 115-124

Kortekaas, J.J.C.
Risicoanalyse georganiseerde criminaliteit. Uitwerking instrumentarium en toepassing op de ICT-ontwikkelingen
's-Gravenhage, Elsevier Overheid, 2005

Krone, T.
High tech crime brief: concepts and terms (elektronische versie)
Australian institute of criminology, high tech crime centre (AHTCC), nr. 1, 2005
Geraadpleegd op 1 mei 2007: www.aic.gov.au/publications/htcb/htcb001.pdf

Lau, E.K.
Factors motivating people toward pirated software
Qualitative Market Research: an International Journal, jrg. 9, nr. 4, 2006: 404-419

Landreth, B.
Out of the inner circle. In: M. Rogers *A new hacker taxonomy (revised version)*, 2000, pp. 2-3.
Geraadpleegd op 3 april 2007: http://homes.cerias.purdue.edu/~mkr/hacker.doc

Leeuw, F.L.
Over beleidsonderzoek en sociologie in de toekomst. In: G. Engbersen en J. de Haan (red.), *Balans en toekomst van de sociologie*, Amsterdam, Pallas Publications, 2006, pp. 263-274

Limayem, M., M. Khalifa, W.W. Chin
Factors motivating software piracy: A longitudinal study
IEEE Transactions on Engineering Management, jrg. 51, nr. 4, 2004, pp. 414-425

Lin, N.
Building a network theory of social capital
Connections, jrg. 22, nr. 1, 1999, pp. 28-51

Loza, W.
The psychology of extremism and terrorism: A Middle-Eastern perspective
Aggression and Violent Behavior, nr. 12, 2007: 141-155

Lunnemann, K., S. Nieborg, M. Goderie, R. Kool, G. Beijers
Kinderen beschermd tegen seksueel misbruik (elektronische versie)
Utrecht, Verwey-Jonker Instituut, 2006
Laatst geraadpleegd op 10 mei 2007:
www.verwey-jonker.nl/images/dynamisch/D6443492_def.pdf

Mann, D., M. Sutton
Netcrime: more change in the organisation of thieving. In: S. Morris
The future of netcrime now: Part 1 – threats and challenges
UK home office, online report nr. 62/04
Laatst geraadpleegd op 16 april 2007: www.homeoffice.gov.uk/rds/pdfs04/rdsolr6204.pdf

Mann, D., M. Sutton, R. Tuffin
The evolution of hate: social dynamics in white racist newsgroups
Internet Journal of Criminology, 2003, pp. 1-32
Laatst geraadpleegd op 24 mei 2007: www.internetjournalofcriminology.com/Evolution%20of%20Hate%20(updated).pdf

McAfee
Georganiseerde misdaad en het internet
McAfee, december 2006

McCusker, R.
Transnational organised cyber crime: distinguishing threat from reality
Crime Law and Social Change, nr. 46, 2006: 257-273

McFarlane, L.: Bocij
An exploration of predatory behaviour in cyberspace: towards a typology of cyberstalkers (elektronische versie)
First monday, jrg. 8, nr. 9, september 2003
Laatst geraadpleegd op 30 augustus 2007: http://firstmonday.org/issues/issue8_9/mcfarlane/index.html

McLaughlin, J.F.
Cyber child sex offender typology
Internetpublicatie, 2000
Laatst geraadpleegd op 24 mei 2007: www.ci.keene.nh.us/police/Typology.html

MessageLabs
Bedrijven in de frontlinie
Internetpublicatie, 2005
Geraadpleegd op 23 mei 2007: www.nl.messagelabs.com/emailthreats/intelligence/reports/monthlies/January05/default.asp#t1

Mheen, D. van de (red.): Gruter (red.): Kruize, B. Rovers, M. Stoele (2007)
Helingpraktijken onder de loep: impressies van helingcircuits in Nederland
Den Haag, Ministerie van Justitie-WODC / Boom Juridische uitgevers, 2007
Reeks Onderzoek en beleid, nr. 251

Molenaar, D.R.
De digitale jungle: wie houdt toezicht?
Tijdschrift voor Consumentenrecht en Handelspraktijken, nr. 2, 2007, pp. 44-51

Mooij, A., J. van der Werf
Cybercrime
Zoetermeer, KLPD, DNRI, 2002
KLPD rechercherapport nr. 22/2002

Morris, S.
The future of netcrime now: Part 1 – threats and challenges
UK home office online report nr. 62/04, 2004
Laatst geraadpleegd op 16 april 2007: www.homeoffice.gov.uk/rds/pdfs04/rdsolr6204.pdf

NCTb
Internetgebruik door jihadisten: fenomeenstudie (vertrouwelijk rapport)
Den Haag, NCTb/DKA, november 2006a

NCTb
Jihadisten en het internet (elektronische versie)
Den Haag, Nationaal Coördinator Terrorismebestrijding, december 2006b
Geraadpleegd op 25 april 2007: www.nctb.nl/Images/Jihadisten%20en%20het%20internet_tcm111-139397.pdf

NCTb
Radicalisering en rekrutering
Internetpublicatie, 2007b
Geraadpleegd op 25 april 2007: www.nctb.nl/wat_is_terrorisme/inleiding/radicalisering_en_rekrutering/

NCTb
Het dreigingsbeeld terrorisme Nederland (DTN8) van maart 2007
Den Haag, Nationaal Coördinator Terrorismebestrijding, 2007c

NCTb
Zesde voortgangsrapportage terrorismebestrijding (elektronische versie)
Den Haag, Nationaal Coördinator Terrorismebestrijding, 4 juni 2007d
Laatst geraadpleegd op 30 augustus 2007: www.nctb.nl/Images/Zesde%20voortgangsrapportage_tcm111-152857.pdf

Neve, R.
Misbruik van ICT (cybercrime): aanzet voorstudie Nationaal Dreigingsbeeld 2008 (interne notitie)
Zoetermeer, Dienst Nationale Recherche Informatie, 2007

Neve, R., L. Vervoorn, F. Leeuw, S. Bogaerts
Eerste inventarisatie van contraterrorismebeleid: Duitsland, Frankrijk, Italië, Spanje, het Verenigd Koninkrijk en de Verenigde Staten; research in progress
Den Haag, Ministerie van Justitie-WODC, 2006
WODC-Cahier, 2006-3

Newman, G.R., M.M. McNally
Identity Theft Literature Review
Paper prepared for the U.S. Department of Justice
United States, University of Albany, Rutgers University Newark, 2005

NHTCC, NPAC
Ontwerp 'Nationale Infrastructuur Bestrijding Cybercrime' (elektronische versie)
Den Haag, National HighTech Crime Center/NPC-project Aanpak Cybercrime, maart 2006a
Laatst geraadpleegd op 28mei 2007: www.minez.nl/dsc?c=getobject&s=obj&objectid=133892&!dsname=EZInternet&isapidir=/gvisapi/

NHTCC
Verantwoording Project High Tech Crime: *bijlage bij het Ontwerp 'Nationale Infrastructuur Bestrijding Cybercrime'* (elektronische versie), maart 2006b
Laatst geraadpleegd op 28mei 2007: www.minez.nl/dsc?c=getobject&s=obj&objectid=133891&!dsname=EZInternet&isapidir=/gvisapi/

NIJ
Special report: investigations involving the internet and computer networks (elektronische versie)
U.S. Department of Justice, National Institute of Justice, januari 2007
Laatst geraadpleegd op 10 april 2007: www.ncjrs.gov/pdffiles1/nij/210798.pdf

Nykodym, N., R. Taylor, J. Vilela
Profiling of cyber crime: criminal profiling and insider cyber crime
Computer Law & Security Report, nr. 21, 2005, pp. 408-414

Parker, D.
Fighting computer crime: a new framework for protecting information.
In: M. Rogers *A new hacker taxonomy (revised version)*, 2000, pp. 5-6
Geraadpleegd op 3 april 2007: http://homes.cerias.purdue.edu/~mkr/hacker.doc

Parlementaire Enquêtecommissie Opsporingsmethoden (PEO)
Inzake opsporing: Enquête opsporingsmethoden
Den Haag, SDU Uitgevers, 1996

Post
Computer crime
Londen, The Parliamentary Office of Science and Technology (POST), 2006
Postnote, nr. 271

Power, R.
Current in future danger. In: M. Rogers *A new hacker taxonomy (revised version)*, 2000, p. 5
Geraadpleegd op 3 april 2007: http://homes.cerias.purdue.edu/~mkr/hacker.doc

Rogers, M.
A new hacker taxonomy (revised version) (elektronische versie)
Internetpublicatie, 2000
Geraadpleegd op 3 april 2007: http://homes.cerias.purdue.edu/~mkr/hacker.doc

Rogers, M.K.
A social learning theory and moral disengagement analysis of criminal computer behavior: an exploratory study
University of Manitoba, Winnipeg, 2001 (proefschrift)

Rogers, M.
A two-dimensional circumplex approach to the development of a hacker taxonomy
Digital Investigation, nr. 3, 2006: 97-102

Rogers, M.K., N. Smoak, J. Liu
Self-reported criminal computer behaviour: a big-5, moral choice and manipulative exploitive behavior analysis
Deviant Behavior, nr. 27, 2006a, pp. 1-24

Rogers, M.K., K. Seigfried, K. Tidke
Self-reported computer criminal behaviour: a psychological analysis
Digital Investigation, nr. 3S, 2006b, pp. S116-S120

Siegel, D.
Nigeriaanse madams in de mensenhandel in Nederland
Justitiële Verkenningen, jrg. 33, nr. 7, pp. 39-49

Shaw, E.D.
The role of behavioral research and profiling in malicious cyber insider investigations
Digital Investigation, jrg. 3, 2006, pp. 20-31

Shaw, E.D., K.G. Ruby, J.M. Post
The insider threat to information systems: the psychology of the dangerous insider
Security Awareness Bulletin, jrg. 2, 1998, pp. 1-10
Laatst geraadpleegd op 7 augustus 2007 op www.pol-psych.com/sab.pdf

Smit, M., M. Boot
Het begrip mensenhandel in de Nederlandse context
Justitiële Verkenningen, jrg. 33, nr. 7, pp. 10-22

Spapens, A.C., M.Y. Bruinsma
Illegale vuurwapens in Nederland: smokkel en handel
Apeldoorn/Zeist: Uitgeverij Kerkebosch bv., 2004
Reeks Politiewetenschap, nr. 18

Speer, D.L.
Redefining borders: the challenges of cybercrime
Crime, Law and Social Change, nr. 34, 2000: 259-273

Stohl, M.
Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?
Crime, Law and Social Change, nr. 46, 2006: 223-238

Stokkom, B.A.M. van, H.J.B. Sackers, J.P. Wils
Haatuitingen en –incidenten in Nederland: enkele kerngegevens.
In: Van Stokkom e.a., *Godslastering, discriminerende uitingen wegens godsdienst en haatuitingen: een inventariserende studie*
Den Haag, Boom Juridische uitgevers, 2007: 185-197

Stol, W.Ph.
Trends in cybercrime
Justitiële Verkenningen, nr. 8, 2004, pp. 76-94

Stol, W.Ph.
Kinderporno op internet (elektronische publicatie)
Den Haag: Ministerie van Justitie, WODC, 2001
Geraadpleegd op 2 mei 2007:
www.wodc.nl/publicatie/aanpakcriminaliteit/criminaliteitsproblemen/Kinderporno_internet/#

Stratix
Onderzoek inzake Artikel 11.3 Tw: concept dreigingsbeeld
Hilversum, Stratix Consulting, 2007

Sullivan, C.
Internet traders of child pornograhpy: Profiling research
New Zealand, the department of internal affairs, 2005, pp. 1-9
Geraadpleegd op 4 april 2007:
www.lgc.govt.nz/pubforms.nsf/URL/Profilingupdate2.pdf/$file/Profilingupdate2.pdf

Sullivan, C.
Internet traders of child pornograhpy: Profiling research – update
New Zealand, the department of internal affairs, 2007, pp. 1-7
Geraadpleegd op 4 april 2007:
www.dia.govt.nz/Pubforms.nsf/URL/Profilingupdate3.pdf/$file/Profilingupdate3.pdf

Taylor, R.W., T.J. Caeti, D.K. Loper, E.J. Fritsch, J. Liederbach
Digital crime and digital terrorism: The criminology of computer crime
New Jersey, Pearson Prentice Hall, 2006, pp. 36-65

Tompsett, B.C., A.M. Marshall, N.C. Semmens
Cyberprofiling: Offender profiling and geographic profiling of crime on the internet (paperpresentatie)
Annual meeting of the American Society of Criminology
Royal York, Toronto, Canada, 5 oktober 2005
Laatst geraadpleegd op 28 mei 2007: http://cprof.tees.ac.uk/~amm/cyberprofilingieee.pdf

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

Verrest, P.A.M.
De strafbaarstelling van witwassen
Justitiële Verkenningen, nr. 2, 2006, pp. 41-53

Vries, U.R.M.Th. de, H. Tigchelaar, M. van der Linden, A.M. Hol
Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen
Utrecht, Departement rechtsgeleerdheid, Universiteit Utrecht (in opdracht van het WODC), 2007

Wall, D.
Crime and the Internet
New York, Routledge, 2001

Weimann, G.
Cyberterrorism: The sum of all fears?
Studies in Conflict & Terrorism, nr. 28, 2005, pp. 129-149

Weimann, G.
Virtual disputes: The use of the internet for terrorist debates
Studies in Conflict & Terrorism, nr. 29, 2006, pp. 623-639

Werf, J. van der
Cybercrime, deel 2: Een verkennende analyse
Zoetermeer, KLPD, DNRI, 2003
KLPD rechercherapport nr. 28/2003

Williams, P.
Organized crime and cybercrime: Synergies, trends, and responses
Global Issues, Transnational Crime, augustus 2001 (elektronische publicatie)
Laatst geraadpleegd op 20 juni 2007: http://usinfo.state.gov/journals/itgic/0801/ijge/gj07.htm

Williams, P.
Russian organized crime, Russian hacking, and US security
(paperpresentatie)
Fourth Information Survivability Workshop (ISW-2001/2002)
'Impediments to Achieving Survivable Systems'
CERT Coordination Center, Vancouver, Canada, 2002

Woodruff, C., S. Gregory
Profile of internet gamblers: Betting on the future
UNLV Gaming Research & Review Journal, jrg. 9, nr. 1, 2005, pp. 1-14

Wykes, M.
Constructing crime: Stalking, celebrity, 'cyber' and media. In: Y. Jewkes (red.) *Crime Online*
Portland, Oregon, Willan Publishing, 2007, pp. 128-143

Yar, M.
The novelty of 'Cybercrime': An assessment in light of Routine Activity Theory
European Journal of Criminology, jrg. 2, nr. 4, 2005a, pp. 407-427
Yar, M.
Computer hacking: Just another case of juvenile delinquency?
The Howard Journal, jrg. 44, nr. 4, 2005b, pp. 387-399

Overige notities en publicaties

Brief aan de Tweede Kamer
AIVD vervolgonderzoek 'Lonsdale'-jongeren (17 januari 2006) (elektronische versie)
Laatst geraadpleegd op 29 augustus 2007: www.aivd.nl/contents/pages/54647/aivdvervolgonderzoeklonsdale-jongeren.pdf
BZK
'Lonsdale-jongeren' in Nederland: feiten en fictie van een vermeende rechts-extremistische subcultuur (elektronische versie)
Den Haag, Ministerie van Binnenlandse Zaken, AIVD-nota nr. 2381145, 2005
Geraadpleegd op 21 mei 2007: www.minbzk.nl/contents/pages/43317/lonsdalenotavoorburgemeestersgeregistreerd.pdf
Europese Commissie
Naar een algemeen beleid voor de bestrijding van cybercriminaliteit
Mededeling van de commissie aan het Europees Parlement, de Raad en het Europees Comité van de regio's (COM2007, 267 final), 22 mei 2007a
Brussel: Europese Commissie
Europese Commissie
Impact assessment report
Bijlage bij de mededeling van de commissie aan het Europees Parlement, de Raad en het Europees Comité van de regio's (SEC2007, 642), 22 mei 2007b
Brussel: Europese Commissie
EZ
Aanbieding eindadvies van de projecten NPAC en NHTCC (elektronische versie)
Den Haag, Ministerie van Economische Zaken, 18 mei 2006
Laatst geraadpleegd op 4 juni 2007: www.hetccv.nl/binaries/ccv/dossiers/ondernemen/actieplan-vo/eindadvies_npac_nhtcc.pdf
Gemeente Amsterdam
Beleidskader van de gemeentelijke informatiehuishouding radicalisering (elektronische versie)
Amsterdam, Gemeente Amsterdam, 24 oktober 2006
Geraadpleegd op 21 mei 2007: www.hetccv.nl/binaries/ccv/dossiers/samenleven-en-wonen/radicalisering/amsterdam_informatiehuishouding_radicalisering.pdf

Kwint
Voorlichtingsmateriaal (potentiële) computercriminelen
Internetpublicatie, mei 2003
Geraadpleegd op 29 maart 2007: www.ecp.nl/download/Voorlichtingsmateriaal_tbv_(potentiele)_computercriminelen.pdf?PHPSESSID=fff3049e448ec91860

MvJ
Aanpak bestrijding van kansspelen via internet (elektronische versie)
Den Haag, Ministerie van Justitie, 25 juli 2006
Geraadpleegd op 14 mei 2007: www.justitie.nl/images/Aanpak%20KVI_tcm34-9460.pdf

OM
Aanpak van georganiseerde misdaad: de strafrechtelijke aanpak van georganiseerde misdaad in Nederland 2005-2010
Den Haag, Openbaar Ministerie, 2004

PCA
Parliamentary joint committee on the Australian crime commission: Cybercrime
Parliament of the Commonwealth of Australia, 2004
Laatst geraadpleegd op 23 mei 2007: www.aph.gov.au/senate/committee/acc_ctte/completed_inquiries/2002-04/cybercrime/report/report.pdf

Raad van Europa
Cybercrimeverdrag / Convention on Cybercrime
Budapest, 23 november 2001
Geraadpleegd op 26 maart 2007: http://conventions.coe.int/treaty/EN/Treaties/html/185.htm

Tweede Kamer der Staten-Generaal
Nationaal Actieplan Mensenhandel
Kamerstukken II, vergaderjaar 2004-2005, 28 638 nr. 13

Tweede Kamer der Staten-Generaal
Terrorismebestrijding: Nota radicalisme en radicalisering
Kamerstukken II, vergaderjaar 2004-2005, 29 754 nr. 26

Tweede Kamer der Staten-Generaal
Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II); Brief staatssecretaris over het eindadvies van het project National High Tech Crime Center (NHTCC) en het NPC-project Aanpak Cybercrime (NPAC)
Kamerstukken II, vergaderjaar 2005-2006, 26 671 nr. 24

Tweede Kamer der Staten-Generaal
Naar een veiliger samenleving
Kamerstukken II, vergaderjaar 2005-2006, 28 684 nr. 85

Tweede Kamer der Staten-Generaal
Voortgangsbericht bestrijding georganiseerde criminaliteit
Kamerstukken II, vergaderjaar 2005-2006, 29 911 nr. 4

Tweede Kamer der Staten-Generaal
Wijziging van de Wet op de kansspelen houdende tijdelijke bepalingen met betrekking tot kansspelen via internet
Kamerstukken II, vergaderjaar 2005-2006, 30 362 nr. 2

Tweede Kamer der Staten-Generaal
Vaststelling van de begrotingsstaten van het Ministerie van Justitie (VI) voor het jaar 2007
Kamerstukken II, vergaderjaar 2006-2007, 30 800 hoofdstuk VI nr. 2

Tweede Kamer der Staten-Generaal
Voorstel van wet van het lid Waalkens houdende strafbaarstelling van het plegen van seksuele handelingen met dieren en pornografie met dieren (verbod seks met dieren)
Kamerstukken II, vergaderjaar 2006-2007, 31 009 nr. 1

Tweede Kamer der Staten-Generaal
Naar een veiliger samenleving
Kamerstukken II, vergaderjaar 2007-2008, 28 684 nr. 119

Bijlage 1
Begeleidingscommissie

Dhr. S. van der Geer	Ministerie van Justitie, Directie Rechtshandhaving & Criminaliteitsbestrijding, Afdeling Criminaliteit & Veiligheid
Dr. Z. Geradts	Nederlands Forensisch Instituut (NFI), Afdeling Digitale Expertise
Dr. B. van Gestel	Ministerie van Justitie, Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)
Dhr. H. van Hezik	Landelijk Parket Rotterdam, Openbaar Ministerie (opvolger van Mr. dr. H. Moerland)
Dhr. J. van Oss	Europol, Serious Crime Department
Dr. A. Sey	Korps Landelijke Politiediensten (KLPD), Concerndienst Beleidsondersteuning & Control Strategische Organisatieontwikkeling (opvolger van Dhr. J. van Oss)
Dr. W. Ph. Stol	Noordelijke Hogeschool Leeuwarden, Thorbecke Academie, Lectoraat Integrale Veiligheid
Drs. M.R. Vollenbroek	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Afdeling Politieel Veiligheidsbeleid, Directie Politie (opvolger van drs. M.A. Seijlhouwer)
Dhr. J. Wester	Ministerie van Economische Zaken, Directie ICT en Toepassing
Mevr. A. van Zantvoort	Ministerie van Justitie, Directie Rechtshandhaving & Criminaliteitsbestrijding, Afdeling Criminaliteit & Veiligheid

Bijlage 2
Begrippenlijst

Adware	Computersoftware waarmee op andermans computer zonder toestemming kan worden ingebroken.
BBS	Bulletin board services: computersysteem met software waarmee gebruikers via een telefoonlijn kunnen inbellen en vervolgens functies kunnen worden uitgevoerd zoals het down- en uploaden van software en data, het lezen van nieuws, en het uitwisselen van berichten met andere gebruikers. Wordt beschouwd als de voorloper van het WorldWideWeb (Wikipedia).
Bot	Een programma dat geautomatiseerd werk kan uitvoeren (zoals wormen, Trojaanse paarden en backdoors) en bijvoorbeeld andere computers zelfstandig kan besmetten.
Botnet	Een leger aan zombiecomputers die zijn besmet met bots die zichzelf aansturen en zonder medeweten van de eigenaren worden ingezet voor dDoS-aanvallen.
Bulletin board	Virtueel prikbordsysteem waarop mensen berichten kunnen achterlaten en waarop zij discussies met elkaar voeren. Andere termen die ook worden gebruikt zijn: online forum, webforum, discussion board. Het toevoegsel forum verwijst doorgaans naar een internetgemeenschap die zich met een specifiek en zelfde onderwerp bezighouden.
Chatroom	Virtuele ruimte op het internet waar mensen met elkaar communiceren.
Clickfraude	Vorm van oplichting waarbij gebruikers van het internet door clicken op zogenoemde pop-ups (reclamevensters) worden omgeleid naar websites die dure belkosten in rekening brengen. Aangezien adverteerders vaak een vergoeding per klik betalen aan de beherende zoeksystemen, kunnen ook zij op kosten worden gejaagd wanneer online advertenties massaal worden aangeklikt via geautomatiseerde commando's (verspreid via botnets).
Computercriminaliteit	Alle criminele activiteiten waarbij ICT als instrument wordt gebruikt én waarbij ICT expliciet doelwit is van de criminele activiteiten.
Cracking	Hacking met de bedoeling criminele activiteiten te ontplooien.

Cybercriminaliteit	Alle (traditionele) criminele activiteiten waarbij ICT als instrument wordt gebruikt zonder dat ICT expliciet doelwit is van de criminele activiteiten.
Cyberstalking	Verzamelnaam voor het stelselmatig en op dwangmatige wijze online lastigvallen (en soms zelfs bedreigen) van een persoon door provocerende uitspraken te doen en/of berichten te plaatsen via online forums, bulletin boards en chat rooms, de ander via spyware te bespioneren, of door het voortdurend ongevraagd verzenden van e-mail en spam.
Cyberterrorisme	Politiek gemotiveerde en beraamde aanvallen van subnationale groepen of clandestiene actoren tegen gegevens, informatiesystemen en computerprogramma's (bijvoorbeeld de virtuele infrastructuur van het internet of andere kritieke infrastructuren in bijvoorbeeld energie, transport en communicatie) die resulteren in geweld tegen niet-strijdende doelwitten (Europol, 2003: 42).
Dawa	Zendingsopdracht in naam van God om het islamitisch geloof te verkondigen.
Defacing	Een vorm van vandalisme door het zonder toestemming wijzigen, vervangen of verminken van een website en/of het doorgeleiden van internetverkeer naar een andere website (Wikipedia).
Discriminatie	Het ongegrond onderscheid maken tussen mensen.
DoS-aanval	Denial of Service-aanval: actie waarbij wordt geprobeerd een computer, een systeem of netwerk zo te belasten dat deze wordt uitgeschakeld en niet meer beschikbaar is (het wordt als het ware plat gelegd).
dDoS-aanval	Een distributed Denial of Service (dDoS) attack is een aanval op een computer of netwerk waarbij met behulp van een botnet een aantal computers (vaak vanaf meerdere plaatsen op de wereldwijd) die vanaf een centraal punt worden bestuurd zoveel verbindingsverzoeken naar de server van een of meer sites verstuurd worden, dat de service ervan tijdelijk niet beschikbaar is of de server zelfs crasht (Wikipedia).

E-commerce	Bedrijven en organisaties die handel bedrijven (goederen kopen en verkopen) door gebruik te maken van digitale communicatie en transacties (Europol, 2003: 65).
Encryptie	Vorm van afgeschermde communicatie door het omzetten van informatie in voor buitenstaanders en onbevoegden onleesbare taal en codes.
Extremisme	Een term die veelal wordt gebruikt om (politieke) ideeën en gedragingen van (groepen) anderen te beschrijven die men als extreem ervaart. Op het moment dat radicalisering overgaat tot daadwerkelijke mobilisering of gebruik van geweld gericht tegen bevolkingsgroepen of tegen de overheid als geheel is er sprake van extremisme.
Google-bom	Poging om het zoekresultaat van Google te beïnvloeden en zo een bepaalde pagina hoog op de resultatenlijst van de zoekmachine te laten verschijnen.
Grooming	Het lokken van kinderen via chatsites.
Haatzaaien	Het oproepen tot discriminatie en geweld.
Hacking	Ongeautoriseerd toegang verschaffen tot een computer.
Hacktivist	Hackers met politieke of sociale bedoelingen (zie hacktivisme).
Hacktivisme	Hacken van computersystemen uit vaak politiek gemotiveerde overwegingen waarbij men protest uit door bijvoorbeeld websites te blokkeren of systemen door massale e-mail te overbelasten (Europol, 2003: 42, 52-53).
High-tech crime	Het gebruik van ICT voor het plegen van criminele activiteiten tegen personen, eigendommen, organisaties of elektronische communicatienetwerken en informatiesystemen.
Identiteitsdiefstal	Identiteitsdiefstal is een vorm van oplichting. Door zich voor te doen voor iemand anders kan men dingen verwerven op naam van iemand anders (Wikipedia).
Information warfare	Het inzetten van informatie en computer (processen en systemen) om de informatie en computer (processen en systemen) van de tegenstander te exploiteren, te vervalsen of te vernietigen en dat van zichzelf te beschermen zodat men competitief voordeel heeft op militaire of zakelijke opponenten (Goldberg, 2005).

IP-adres	Internet Protocol adres: een uniek identificerend nummer van met internet verbonden apparaten.
Islamisme	Verzameling van politieke ideologieën die gebaseerd is op een conservatieve, letterlijke interpretatie van de Koran (het heilige boek van de moslims) en de Hadieth (islamitische overleveringen over de profeet Mohammed). Aanhangers zijn principieel tegen de scheiding van geloof en staat (Wikipedia).
Islamistisch	Verwijst naar een radicale stroming binnen de islam met een duidelijk politieke agenda. Islamisten streven ernaar om de samenleving een weerspiegeling te laten zijn van de 'zuivere' islam (gebaseerd op een conservatieve, letterlijke interpretatie van de Koran en de Hadieth). Het islamisme kent gewelddadige, niet-gewelddadige en democratische varianten (AIVD, 2006b: 13).
Islamitisch	Refereert aan alles betreffende de islam als religie.
Jihad	Begrip uit de islamitische godsdienst wat 'strijd' betekent. Er zijn twee soorten: enerzijds de eigen innerlijke strijd om allerlei verleidingen te weerstaan (ook wel grote strijd genoemd), anderzijds de strijd tegen degenen die de islam of de verwezenlijking van een moslimsamenleving en heerschappij bedreigen (ook wel kleine strijd genoemd).
Jihadistisch	Refereert aan een extreem politieke ideologie dat zich beroept op de islam en zich kenmerkt door een streven om via een gewelddadige 'heilige oorlog' tegen alle ongelovigen te voldoen aan de als goddelijke ervaren plicht om de islam over de wereld te verspreiden (NCTb, 2007).
Keylogging	Keystroke logging (of keylogging) is een spyware diagnose-instrument dat bijhoudt wat er op een computer via het toetsenbord wordt ingetypt. Het kan zowel in software als in hardware worden ingebouwd en biedt de mogelijkheid om andermans activiteiten te bespioneren en bijvoorbeeld (versleutelde) passwords op beveiligde systemen te verkrijgen (Wikipedia). De softwareversie kan met een virus worden

	verspreid of via een Trojaans paard ongemerkt worden geïnstalleerd op de computer.
Malware	Afkorting van malicious software: computersoftware waarmee andermans computer zonder toestemming kan worden beschadigd (bijvoorbeeld virussen, wormen en Trojaanse paarden).
Message boards	Virtueel prikbordsysteem waarop mensen berichten kunnen achterlaten. Communicatie komt tot stand via het internet.
Nieuwsgroep	Een publiekelijk toegankelijke discussieruimte op het internet waarin mensen met elkaar kunnen discussiëren, computerfiles verspreiden, adverteren en berichten kunnen achterlaten die door iedereen gelezen kan worden en waarop men kan reageren.
Nigerian scam	Ook wel 'advance fee fraud' (voorschotfraude) of '419-fraude' genoemd: grootschalige oplichtingspraktijken die veelal door Nigerianen worden gepleegd. Slachtoffers worden via misleidende digitale informatie (bijvoorbeeld spam e-mail) overgehaald om een financieel voorschot te verlenen (om belangrijke anderen te helpen of om een grote geldprijs te incasseren die in het vooruitzicht wordt gesteld).
PBX-fraude	Private Branche Exchange: fraude met bedrijfstelefooncentrales waarbij op kosten van een bedrijf internationale gesprekken worden gevoerd door buitenstaanders (Boerman en Mooij, 2006; KLPD, DNRI, 2004: 88).
PDA (personal digital assistant)	PDA staat voor Personal Digital Assistant en is een klein draagbaar toestel vaak uitgerust met een minitoetsenbord of een aanraakscherm (touch screen) dat computer-, telefonie-, fax- en netwerkfuncties combineert. Door veel mensen gebruikt als mobiele telefoon en persoonlijke organiser.
PGP (pretty good privacy)	Vercijferingsmethode (vorm van cryptografie) die veel wordt gebruikt op het internet.
Pharming	Vorm van digitale oplichting waarbij een internetgebruiker bij het invoeren van het adres van een website op een andere pagina terechtkomt (men wordt omgeleid naar een nepsite waar vervolgens d.m.v. phishing om persoonlijke gegevens wordt gevraagd).

Phishing	Vorm van digitale oplichting waarbij een internetgebruiker een vervalste e-mail ontvangt, meestal van een gerenommeerde bron (bijvoorbeeld een financiële) instelling en waarbij mensen om persoonlijke gegevens wordt gevraagd.
P2P (peer to peer)	Technologie waarbij een groep internetgebruikers (peers) een deel van de eigen computer openstelt voor anderen (sharing) en zo onder meer muziek- en videobestanden met elkaar uitwisselt zonder tussenkomst van een server (men heeft direct toegang tot andermans computer).
Radicalisering	Een proces in de sociale sfeer waarin individuen door beïnvloeding vanuit de omgeving worden aangezet zich te ontwikkelen in een gewelddadige richting (NCTb, 2007b).
Rootkit	Stuk software dat een hacker na een succesvolle inbraak achterlaat, om de volgende keer gemakkelijk via een 'achterdeur' binnen te komen.
Script kiddies	Mensen (voornamelijk tieners) die computers kraken, informatie wissen en websites defacen zonder echte technische kennis (men maakt gebruik van de vindingen van hackers). Valt onder de categorie crackers.
Skimming	Het kopiëren van pinpas- en creditcardgegevens. De bijbehorende pincodes worden vaak achterhaald met gebruik van miniatuurcamera's, spiegels en neptoetsenborden en vervolgens worden de betreffende rekeningen geplunderd.
SMiShing	Phishing via SMS tekstberichten in plaats van e-mail.
Sniffing	Het bekijken van netwerkverkeer en onderscheppen van passwords, e-mail en andere vertrouwelijke informatie.
Social engineering	Het onder valse voorwendselen verkrijgen van vertrouwelijke informatie of ongeoorloofd een bedrijf binnenkomen waarbij de menselijke betrokkenheid (tactieken) van belang zijn bij het verkrijgen van gevoelige informatie (bijvoorbeeld door werknemers binnen een bedrijf te bespelen) (NCTb, 2007).
Spam	Stupid Pointless Annoying Messages: het versturen van ongewenste e-mail of reclame.

Spoofing	Identiteitsvervalsing waarbij de bron zich voordoet als iets of iemand anders (bijv. door het verwijderen van het IP-adres).
Spyware	Verzamelnaam van programma's die het computergedrag van gebruikers bespioneren (zoals adware, malware en keyloggers).
Telecomfraude	Misbruik van een telecommunicatievoorziening waardoor de integriteit van de infrastructuur wordt aangetast, dan wel het verrichten van frauduleuze handelingen waardoor financieel nadeel ontstaat voor de telecommunicatieve dienstverlening (Boerman en Mooij, 2006: 35).
Terrorisme	Het plegen van, of dreigen met, op mensenlevens gericht geweld dan wel het toebrengen van ernstige maatschappij ontwrichtende schade met als doel maatschappelijke veranderingen te bewerkstelligen of politieke besluitvorming te beïnvloeden (NCTb, 2007: 17).
Trojaans paard	Een Trojaans paard (genoemd naar de Griekse soldaten die de stad Troje binnenkwamen om de stad van binnenuit aan te vallen) is een programma of stukje software dat ongewenst meekomt met een programma dat door de computergebruiker wordt geïnstalleerd (onder andere via bijlagen in e-mails). Het nestelt zich in het besturingssysteem op de harde schijf en zorgt ervoor dat de computer wordt opengezet voor andere gebruikers. Schending van de privacy van de gebruiker (achterhalen van wachtwoorden en gebruikersnamen) en schade aan computergegevens (anderen die bestanden inzien, wijzigen of verwijderen) zijn mogelijke gevolgen. Ook kan een besmette computer worden ingezet bij een dDoS-aanval (Wikipedia).
Virus	Een zichzelf vermenigvuldigend en verspreidend computerprogramma. Een computervirus is een vorm van schadelijke software (ook wel malware genoemd) dat zich ongemerkt in een bestand kan nestelen (bijvoorbeeld in bestanden van een besturingssysteem). Zij nemen schijfruimte en computertijd in beslag en in ernstige gevallen kunnen ze in de computer schade aanrichten zoals het wissen en verspreiden van (gevoelige) gegevens (Wikipedia).

VoIP (Voice over IP)	Telecomdiensten via internet.
Warez	Illegaal gekopieerde software.
Web sit-in	Vorm van hacktivisme waarbij door een groot aantal deelnemers herhaaldelijk informatie wordt opgevraagd bij een website waardoor deze overbelast raakt en buiten werking komt te staan.
Zombie	Een computer die zonder toestemming van de eigenaar deel uitmaakt van een botnet.
0900-fraude	Vorm van fraude waarbij onwetende internetgebruikers worden omgeleid naar dure (0900-beltarief) websites (KLPD, DNRI, 2004: 88).

Bijlage 3
De aanpak van high-tech crime

De acht democratische, industriële grootmachten Canada, Duitsland, Frankrijk, Groot-Brittannië, Italië, Japan, Rusland, en de Verenigde Staten (G8) hebben zich in 2004 expliciet uitgesproken over de bestrijding van high-tech crime, onder meer in relatie tot terrorisme en georganiseerde misdaad (G8, 2004). Uit de G8 Lyon-groep[159] ontstonden vijf subgroepen die zich op specifieke subthema's van georganiseerde misdaad richtten. Eén daarvan is ingericht op de preventie, opsporing en vervolging van high-tech crime (de G8 Lyon-Roma High-Tech Crime Group) en richt zijn aandacht expliciet op de bestrijding van terrorisme en de bescherming van vitale infrastructuren (in dit rapport cyberterrorisme). Onlangs werd high-tech crime door de Europese Commissie (EC) opnieuw op de internationale agenda gezet met de intentie meer geld vrij te maken voor opbouw van expertise en bestrijding van wat men noemt 'internetmisdaad' of 'cybercrime'[160,161] (AD, 21 mei 2007; EC, 22 mei 2007).

Uit onderzoek van TNO is gebleken dat het ICT-veiligheidsbeleid in Nederland is versnipperd en overlap kent in activiteiten, bevoegdheden en verantwoordelijkheden (zie Helmus e.a., 2006). Tot op heden was het ICT-veiligheidsbeleid in Nederland meer gericht op de niet-strafrechtelijke aanpak (bewustwording, voorlichting en kennisoverdracht) dan op de strafrechtelijke aanpak (toezicht en handhaving) van high-tech crime. Binnen het nieuwe veiligheidsprogramma van de Nederlandse overheid (tot 2010) is high-tech crime (cq. cybercrime) als speerpunt geformuleerd voor het aanpakken van criminaliteit. Dit komt onder meer tot uitdrukking via de prestatiecontracten 2007-2008 met de Politie (TK 2005-2006, 28 684, nr. 85). We geven onderstaand een korte toelichting op context en initiatieven van zowel de niet-strafrechtelijke als de strafrechtelijke aanpak van high-tech crime in Nederland.

Niet-strafrechtelijke aanpak

In het kader van het nieuwe Veiligheidsprogramma is het Nederlandse regeringsbeleid gericht op een intensivering van de bestrijding en opsporing van high-tech crime. Zo werd er in Nederland gewerkt aan de ontwikkeling van een '*Nationale Infrastructuur ter bestrijding van Cyber Crime*' (NICC). Dit programma heeft tot doel om de informatie-uitwisseling, samenwerking en coördinatie tussen de verschillende betrokken partijen op het gebied van high-tech crime in Nederland te bevorderen (denk

159 Oorspronkelijk opgericht (1995) door experts ter bestrijding van grensoverschrijdende georganiseerde misdaad

160 Uit praktische overwegingen hanteert de commissie de term 'cybercrime' (zie ook hoofdstuk 2 van dit rapport).

161 Het Zevende Kaderprogramma voor Onderzoek en Technologische Ontwikkeling (7KP) van de Europese Commissie, dat loopt van 2007 tot 2013, vormt daarbij een belangrijk instrument.

aan de politie, aan overheidsdiensten zoals Govcert, aan toezichthouders zoals OPTA, en aan het bedrijfsleven zoals MKB, telecommunicatie, bankwereld, software-industrie, en internet service providers). Het NICC werd mede voorbereid door de projectgroep National High Tech Crime Center (NHTCC)[162] en het NPC-Project Aanpak Cyber Crime (NPAC) van het Nationaal Platform Criminaliteitsbestrijding (NPC).[163] Beide projecten hebben een gezamenlijk eindadvies opgeleverd dat door het Ministerie van Economische Zaken (EZ), mede namens het Ministerie van Justitie (MvJ) en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), werd aangeboden aan de Tweede Kamer op 18 mei 2006 (TK 2005-2006, 26 671, nr. 24). De coördinerende taken van het NPC voor de verdere doorontwikkeling van het NICC-programma berusten inmiddels geheel bij EZ.

Strafrechtelijke aanpak

Wat betreft de opsporing en vervolging van high-tech crime zijn de taken op nationaal niveau (met name voor de zwaardere vormen van georganiseerde criminaliteit) belegd binnen het nieuwe Team High-Tech Crime (THTC) van de Nationale Recherche, onderdeel van het Korps Landelijke Politiediensten (KLPD).[164] Het team is formeel sinds 1 januari 2007 operationeel en houdt zich (samen met de bestaande groep Digitale Recherche[165]) landelijk bezig met strafrechtelijk onderzoek en de bestrijding van high-tech crime, in het bijzonder waar het gaat om zware, georganiseerde criminaliteit en om innovatieve vormen van high-tech crime of incidenten met een belangrijke internationale component (TK 2005-2006, 26 671, nr. 24). Ook levert de unit informatie aan de Dienst Nationale Recherche Informatie (DNRI) met het oog op het Nationaal Dreigingsbeeld (NDB) (Netkwesties, 24 augustus 2006). Ter ondersteuning van de regionale politiekorpsen in Nederland houden zeven interregionale Bureaus Digitale Expertise (BDE's) zich bezig met het opsporen van high-tech crime, waarbij iedere BDE zijn eigen expertise kent[166] (zie Molenaar 2007). In Europees verband worden de krachten gebundeld bij Europol om de internetactiviteiten van onder andere (moslim)terroristen

162 Een initiatief van het KLPD en BZK, EZ en MvJ (oktober 2004 – eind 2005) gericht op proactief ingrijpen van de overheid en met name het bestrijden van high-tech crime vanuit de politie.
163 Het Nationaal Platform Criminaliteitsbestrijding (NPC) coördineert de samenwerking met bedrijfsleven (waaronder VNO-NCW, MKB Nederland, banken en verzekeraars) op het gebied van de niet-strafrechtelijke bestrijding van high-tech crime (NHTCC, 2006a: 39).
164 De politie wordt op haar beurt landelijk weer aangestuurd door het Landelijk Parket (LP) van het Openbaar Ministerie (OM) (zie ook Molenaar, 2007). Het LP houdt zich bezig met de strafrechtelijke handhaving op het gebied van georganiseerde misdaad en heeft tevens tot taak expertise te ontwikkelen op het gebied van high-tech crime. Voor alle rechtshandhaving die niet gerelateerd is aan openbare orde, wordt de politie landelijk aangestuurd door BZK.
165 De groep Digitale Recherche richtte zich voorheen vooral op computerinbraken, kinderporno, fraude en grote financiële transacties in bijvoorbeeld drugssmokkel (Fox-IT, 26 februari 2004).
166 Rechercheteam Noord is bijvoorbeeld verantwoordelijk voor de aanpak van telecomfraude.

te onderzoeken en te bestrijden (Elsevier, 9 mei 2007). Ten slotte wordt in de landelijke prestatieafspraken met de politie en in het Coalitieaccoord aandacht besteed aan de verdere versterking van de opsporing en vervolging van high-tech crime.[167]

Ook burgers worden betrokken in de strafrechtelijke aanpak en bestrijding van high-tech crime: zij kunnen terecht bij de politie voor het doen van aangiftes. In maart 2006 is het Meldpunt Cybercrime (MCC) in gebruik genomen door de politie (in maart 2007 werd de nieuwe website gelanceerd). Burgers kunnen er terecht voor het melden van kinderporno en grooming (het seksueel benaderen van kinderen via het internet) en als zij radicale en terroristische uitingen op het internet tegenkomen (MCC, 2007). Het MCC is vooralsnog gericht op de bestrijding van kinderporno en terrorisme maar zal naar verwachting op termijn worden uitgebreid voor aangiftes van andere vormen van high-tech crime.

167 Men noemt het cybercrime.

Bijlage 4
Vormen van radicalisme

Het internet is bij uitstek geschikt voor het ontmoeten van gelijkgestemden om extreme opvattingen mee te delen. Radicale groeperingen en personen met extreme opvattingen maken dan ook intensief gebruik van websites en chatboxen. Zij voeren propaganda, bedreigen opponenten, roepen op tot geweld en bereiden acties voor (TK 2004-2005, 29 754, nr. 26: 9; Van Stokkom e.a., 2007: 189). In hoofdstuk 2 werden drie vormen van radicalisme onderscheiden die een concrete bedreiging vormen voor de Nederlandse samenleving: het dierenrechtenactivisme, het rechts-extremisme en het islamistisch radicalisme. In deze bijlage geven we een korte toelichting op deze radicale stromingen.

Dierenrechtenactivisme

Het dierenrechtenactivisme kenmerkt zich door een sterke ideologie en strijd voor de rechten en het welzijn van dieren. Er is geen sprake van een achterliggende doctrine: de ideologische achtergrond van betrokken individuen lopen sterk uiteen, variërend van extreem-links tot extreem-rechts (TK 2004-2005, 29 754, nr. 26: 37). Vreedzame activisten hebben tot doel om via demonstraties en het uitdelen van pamfletten de politiek en de samenleving te attenderen op dierenleed. Dit gaat soms echter gepaard met illegale en gewelddadige acties (blokkades, vernieling, brandstichting, bedreiging, intimidatie, het vrijlaten van dieren uit fokkerijen) waarbij geweld tegen personen niet wordt geschuwd. Deze acties zijn vooral gericht tegen de vlees- en vee-industrie, tegen organisaties die zich bezighouden met dierproeven, en tegen mensen die actief zijn op het gebied van de jacht (AIVD, 2004c). Volgens de AIVD (2004d) is er sprake van '*…een toenemende professionalisering in de acties, die vaak plaatsvinden in georganiseerd verband en in toenemende mate een relatie met buitenlandse radicale groeperingen hebben*'. De AIVD neemt een verschuiving waar van verdergaande radicalisering en de impliciete bereidheid om ook mensenlevens op het spel te zetten. Dit politiek gewelddadig activisme, die overigens beperkt is tot een kleine kern activisten (de overgrote meerderheid is meer gematigd), schuift dan feitelijk op in de richting van terroristisch geweld (AIVD, 2004c; 2007).

Rechts-extremisme

Het rechts-extremisme kenmerkt zich door sterk nationalistische en racistische denkbeelden. Bekende voorbeelden van een extreem-rechtse groeperingen zijn de Ku Klux Klan (KKK) en Stormfront, die tot op de dag van vandaag actief zijn in onder meer de Verenigde Staten (maar ook op het internet) (Gelderblom, 2004: 69). Verschillende extreem-rechtse discussiefora (bijvoorbeeld van Nieuw Rechts en van de Nationale

Alliantie maar ook Polinco) zijn recentelijk uit de lucht gehaald. Van het Nederlandstalige deel van het internationale Stormfront-forum zijn de afgelopen jaren enkele deelnemers vanwege hun extremistische uitingen vervolgd en veroordeeld. Een ander webforum dat sinds 2003 in de lucht is en waarop extreem-rechtse gabbers actief zijn is Holland Hardcore. Volgens Van Donselaar en Rodrigues (2006: 131) zijn extreem-rechtse webforums '*… een verzamelplaats van radicale strafbare uitingen, oproepen tot geweld en haatzaaierij*'. In Nederland worden skinheads, gabbers en Lonsdale-jongeren (zogenoemde jeugd-subculturen) met regelmaat als risicogroep aangewezen. Kenmerkend voor bijvoorbeeld Lonsdale-jongeren zijn de frustraties ten aanzien van de multiculturele samenleving. De daaruit voortvloeiende gevoelens van nationalisme leiden regelmatig (onder invloed van drank en drugs) tot gewelddadige confrontaties met allochtonen. Uit onderzoek van de AIVD blijkt dat er geen sprake is van een landelijke Lonsdale-organisatie en dat er ook binnen deze beweging een kleine kern is van neo-nazi's die er expliciet rechts-radicale gedachten op na houdt en een veel grotere groep met meer '*burgerlijk rechtse opvattingen*' (MvJ, 2005: 37). Volgens de AIVD heeft de rechts-extremistische jongerencultuur nergens een zodanige vlucht genomen als in Nederland. Hoewel sprake is van een voortschrijdende radicalisering, is er vooralsnog geen sprake van een concrete dreiging voor de samenleving uit deze hoek (DTN8, maart 2007).

Islamistisch radicalisme

Het islamistisch radicalisme wordt door de AIVD (2004b: 7) omschreven als: '*…Het politiek-religieuze streven om, desnoods met uiterste middelen, een samenleving tot stand te brengen die een zo zuiver mogelijke afspiegeling is van hetgeen men meent dat gesteld wordt in de oorspronkelijke bronnen van de islam*'. Er zijn verschillende islamistische stromingen met dezelfde geloofsbeleving en puriteinse, intolerante en anti-westerse sympathieën, maar de doelen en middelen die worden gepropageerd verschillen. Waar de één vooral de radicaal-islamistische ideologie uitdraagt als zendingsopdracht in naam van god om het islamitisch geloof te verkondigen (*dawa*) is de ander daadwerkelijk gewelddadig en roept op tot de gewapende strijd (*jihad*). Aanhangers van de dawa hanteren een langetermijnstrategie van continue indoctrinatie en beïnvloeding. Bijvoorbeeld door de moslimbevolking ervan te overtuigen dat niet-moslims vijandig staan tegenover de islam en dat deze religie in het Westen wordt onderdrukt als de moslimbevolking er niets aan doet, of door de moslimbevolking ervan te overtuigen dat de Westerse normen en waarden verderfelijk zijn en niet stroken met de islam. Binnen de laatste categorie vallen ook *salafisten*: radicaal-islamistische puriteinen die terug willen naar de zuivere islam van de salaf (de eerste volgelingen van Mohammed) (AIVD, 2004b: 26, 42).

Aanhangers van de jihad zijn bereid om elke bedreiging van de islam met geweld te bestrijden. Jihad is een begrip uit de islamitische godsdienst en betekent 'strijd'. De grote strijd refereert aan de eigen innerlijke strijd om allerlei verleidingen te weerstaan. De kleine strijd is gericht tegen iedereen die de islam of de verwezenlijking van een moslimsamenleving en heerschappij bedreigt. Wanneer in de media wordt gesproken van jihad wordt doorgaans de kleine strijd (of heilige oorlog) bedoeld. De AIVD spreekt in het laatste geval ook wel van *jihadisme*[168] en ziet steeds vaker individuen en groepen jongeren die uit zichzelf (en niet door rekrutering of formele sturing 'van bovenaf') radicaliseren en tot gewelddadige actie willen overgaan.

Volgens de AIVD (2004: 8-12; 2004b: 43) lijkt de radicalisering naar het jihadisme zich behalve naar kleine moskeeën en huiskamers in toenemende mate te verplaatsen naar internetsites en chatrooms waar discussies met gelijkgestemden worden gevoerd (de '*virtuele dawa*'). Het verspreiden van propaganda via het internet (met zijn grote bereik en relatief weinige weerwoord) vindt op steeds professionelere wijze plaats. Bij onderlinge communicatie wordt gebruikgemaakt van codewoorden en *encryptie* en andere vormen van afscherming (AIVD, 2006a: 48; NCTb, 2006a, 2006b: 8-10). Er wordt gericht aansluiting gezocht bij de taal, cultuur, mentaliteit en belevingswereld van de doelgroep (NCTb, 2006b: 64, 70). Vooral jongere moslims in westerse niet-moslimlanden kampen met levensvragen en religieuze vragen en zijn op zoek naar hun identiteit en positionering in de samenleving. Zij zoeken antwoorden en een gevoel van saamhorigheid die zij in de maatschappij doorgaans missen. Dit brengt hen in een omgeving die zij goed kennen, namelijk het internet, waar zij behalve veel (eenzijdige, radicale) uitleg van de islam krijgen[169] ook onderdeel kunnen gaan uitmaken van een virtuele gemeenschap[170,171] (NCTb, 2006b: 93-95). Juist de mogelijkheden die het internet biedt voor herhaling (het continue herhalen van berichten, preken en video's) is effectief om te kunnen indoctrineren. Evenals voor de andere radicale stromingen geldt ook voor het islamistisch radicalisme dat de harde kern relatief klein is met daaromheen een grotere groep sympathisanten (vaak familieleden of mensen met wie men een etnisch/religieuze verwantschap heeft) (TK 2004-2005, 29 754, nr. 26: 39). De AIVD benadrukt dat het van belang is om radicale moslimjongeren die de gewelddadige jihad aanhangen te onderschei-

168 *Jihadisme* is een extreem politieke ideologie en radicale interpretatie van de islam die gekenmerkt wordt door een streven om via een 'heilige oorlog' tegen alle ongelovigen te voldoen aan de als goddelijk ervaren plicht om de islam over de wereld te verspreiden (NCTb, 2007).

169 Bijvoorbeeld via websites van radicale schriftgeleerden waar gepredikt wordt over jihad en martelaarschap.

170 Binnen deze subcultuur van (veelal Marokkaanse) jongeren 'infecteert' men zichzelf en elkaar als het ware met een steeds verdergaande radicaal-islamistische ideologie (AIVD, 2006a: 57 en 2006b: 49).

171 Hoewel het proces van radicalisering zich in eerste instantie kan beperken tot het internet is het een reële voorstelling van zaken dat dit zich voortzet buiten het internet (bijvoorbeeld in gevangenissen, scholen en moskeeën) (AIVD, 2004b: 44).

den van moslimjongeren die door middel van uiterlijkheden en extreme uitspraken hun sociale identiteit vorm proberen te geven (AIVD, 2006b: 20). Met name onder moslimjongeren lijkt de concrete dreiging recentelijk gestabiliseerd en is sprake van een zekere gelatenheid (NCTb, 2007d).

Bijlage 5
Terrorisme en internet

Het internet biedt vanuit terroristisch oogpunt belangrijke voordelen (NCTb, 2006a: 16; Weimann, 2005, 2006: 624): het is gemakkelijk toegankelijk, relatief voordelig (men heeft een computer en een online verbinding nodig), relatief anoniem (de pakkans is gering), er is sprake van beperkte censuur, het heeft een wereldwijd bereik zonder fysieke barrières (geen landsgrenzen te overbruggen), informatie kan snel worden verspreid, communicatie is interactief, en gecombineerde multimediatoepassingen zijn mogelijk (gebruik van tekst, beeld én audio). Terroristen zijn zich van dergelijke gebruiksvoordelen goed bewust. Zo noemt Al Qaeda het bijvoorbeeld de 'heilige plicht' van iedere moslim om informatie over de jihad zo snel mogelijk te verspreiden via *nieuwsgroepen*[172] op het internet, internetfora en websites (NCTb, 2006b: 70). Daarbij wordt gebruikgemaakt van het feit dat video-uitzendingen, digitale magazines, animaties, strijdliederen en losse berichten nauwelijks (kunnen) worden gereguleerd of gecensureerd.[173] Er is door Al Qaeda zelfs een model ontwikkeld voor zogeheten 'virtuele jihadistische verzetsbrigades' die worden geacht de jihadistische boodschap te verspreiden (via literatuur, onderzoek, publicaties, vertalingen), leden te werven voor de jihad, en zich aan te sluiten bij het front (NCTb, 2006b: 51-52). Kennis van ICT behoort dus tot de basisuitrusting van iedere strijder.

Benschop (2006) beschrijft uitvoerig het type informatie dat door Al Qaeda en aanverwante organisaties op internet wordt aangeboden. Het internet wordt gebruikt als ideologische inspiratiebron, operationele kennisbron, katalysator voor netwerkvorming en voor het in stand houden van radicale, extremistische en terroristische contacten (zie ook hoofdstuk 2 onder radicalisering). Daarnaast gebruiken terroristen het internet om (zie ook Europol, 2003: 41; Goodman e.a., 2007; Handelingen 2006-2007, nr. 33, TK, pp. 2191-2193; Kohlmann, 2006; NCTb, 2006b; Stol, 2004; Weimann, 2006):

– *de vijand te beïnvloeden (psychologische oorlogsvoering)*
  Terwijl propaganda is gericht op het indoctrineren van de eigen (potentiële) achterban, gaat het bij psychologische oorlogsvoering om het aanjagen van angst ter beïnvloeding van (het politieke klimaat van) de vijand (NCTb, 2007: 68).

172 Een nieuwsgroep is een publiekelijk toegankelijke discussieruimte op het internet waarin mensen met elkaar kunnen discussiëren, computerfiles verspreiden, adverteren en bijvoorbeeld berichten kunnen achterlaten die door iedereen gelezen kunnen worden en waarop men kan reageren. Geplaatste berichten worden over het algemeen na enkele weken verwijderd. De nieuwsgroepen hebben veelal een specifiek thema en naar schatting waren er in 2003 in aantal 35.000 wereldwijd (Mann e.a., 2003).

173 De propaganda is steeds meer verfijnd, van betere kwaliteit en wordt op professionelere wijze tot stand gebracht. Er is een toename in het gebruik van de Engelse taal om een zo groot mogelijk publiek te bereiken (Europol, 2007: 3, 25).

– *virtuele trainingskampen te organiseren*
Het gebruik van internet voor trainingsdoeleinden vormt volgens de NCTb (2006a: vi) een belangrijke terroristische dreiging. Zo zijn er talloze websites beschikbaar met informatie over het voorbereiden van aanslagen. Het gaat hier om allerhande operationele kennis die op het internet rondzwerft, waaronder gedetailleerde satellietfoto's maar ook handleidingen (bijvoorbeeld militaire handboeken) en instructievideo's waarin methodes worden uitgelegd voor het maken van bijvoorbeeld explosieven, het veilig onderling communiceren, het ontdekken van infiltranten, het doen van ontvoeringen en gijzelingen, en wat te doen bij arrestaties (Kohlmann, 2006; NCTb, 2006b: 76-87).

– *(afgeschermd) te communiceren bij het plannen, mobiliseren en coördineren van activiteiten*
In een oudere Al Qaeda-publicatie werd bijvoorbeeld het gebruik van de 'dead box' als veilig communicatiemedium aangeprezen:[174] instructies en dergelijke werden op een onopvallende geheime plaats gelegd, waar ze door medeterroristen (die de afzender niet hoeven te kennen) weer konden worden opgehaald. Een moderne variant is het gebruik van een Hotmail-account door meerdere personen, die zo berichten kunnen doorgeven zonder ze ooit daadwerkelijk via het internet te verzenden.

– *activiteiten te financieren (bijvoorbeeld door verkoop van producten en diensten via het internet) en fondsen te werven*
Het kan gaan om openlijke fondsenwerving (soms via kettingbrieven) waarin wordt opgeroepen geld te doneren voor het bekostigen van wapens, omkoping, zorg voor (gezinsleden van) martelaren en liefdadigheidsinstellingen, maar ook om niet-vrijwillige bijdragen die zijn gegenereerd door online creditcardfraude, phishing en pharming (NCTb, 2006b: 79-80) (zie voor een nadere toelichting op deze vormen van cybercriminaliteit hoofdstuk 2).

– *zelfmoordterroristen te werven (rekrutering)*
In Nederland gaat volgens de NCTb (2006b: 50-51, 82) vooral dreiging uit van lokale, autonome netwerken die een interactieve vorm van propaganda bedrijven, elkaar inspireren en kopiëren. Vooral bij de rekrutering speelt het internet een belangrijke rol. Zo maakt men bijvoorbeeld gebruik van postings op websites en nieuwsgroepen die verwijzen naar een bepaalde website waarop via chatprogramma's kan worden gediscussieerd over (geloofs)zaken. Van de aanvankelijk open wijze van communicatie worden gaandeweg op meer vertrouwelijke wijze één-

174 Volgens Benschop (2006) vormt het internet voor terroristische groeperingen één grote digitale 'dead box'.

op-één chatsessies georganiseerd met potentiële rekruten. De virtuele netwerken die ontstaan, worden door de NCTb (2006b: 10, 64) gekarakteriseerd als een '*…informele pool van bereidwilligen voor de jihad die in wisselende combinaties met elkaar of individueel geweldsactiviteiten kunnen ontplooien*'.

Vooral het gebruik van internet voor propaganda (radicalisering), de vorming van virtuele netwerken en trainingsdoeleinden (terrorisme) vormt een dreiging (NCTb, 2006b: 96). In samenwerking met het OM, het KLPD en de AIVD ontwikkelt de NCTb een aanpak voor het bestrijden van internetgebruik voor radicale en terroristische doeleinden (TK 2006-2007, 30 800 hoofdstuk VI, nr. 2).

Bijlage 6
Daderkenmerken high-tech crime

Van de geprioriteerde thema's van high-tech crime werd op grond van de literatuur geïnventariseerd wat er bekend is over de daders ervan (hoofdstuk 3) en in hoeverre kan worden gesproken van georganiseerde high-tech crime of HT-CSV's (hoofdstuk 4). In deze bijlage vatten we de resultaten van deze inventarisatie samen voor de niet-geprioriteerde thema's van high-tech crime. Een overzicht van de subthema's die aan bod komen, is weergegeven in schema B1[175] (zie voor een indeling naar clusters ook schema 2 van hoofdstuk 2).

Schema B1 Overzicht van niet-geprioriteerde subthema's van high-tech crime

Cybercriminaliteit
- afscherming met behulp van ICT
- illegale handel in drugs
- illegale handel in geneesmiddelen
- illegale handel in vuurwapens en explosieven
- heling
- mensenhandel en -smokkel
- illegale kansspelen
- marktmanipulatie
- afpersing en chantage
- cyberstalking
- discriminatie
- spionage

Computercriminaliteit
- (d)DoS-aanval
- spamming
- defacing (pharming)
- (h)acktivisme

Legale communicatie en afscherming

Afscherming met behulp van ICT
Over individuele daderkenmerken en HT-CSV's die gebruikmaken van afschermingstechnieken met behulp van ICT zijn weinig concrete kenmerken in de literatuur te vinden. Wel is uit onderzoek gebleken dat traditionele CSV's (groothandelaren in drugs en vuurwapens) gebruikmaken van afgeschermde communicatiemiddelen zoals IRC, ICQ ('I seek you'-protocollen) en versleutelde e-mail, en van contrastrategieën zoals

175 Van de subthema's 'ongeautoriseerde toegang tot ICT' en 'dienstverleners' worden de verschijningsvormen van high-tech crime als prioriteit aangemerkt (zie hoofdstuk 2).

het plaatsen van bugs en het gebruik van sweeping apparatuur (Hynds, aangehaald door McCusker, 2006; KLPD, DNRI, 2004). Volgens Europol (2003: 33) worden daarvoor ook in Nederland computerspecialisten ingeschakeld. Door de verbeterde technische mogelijkheden om de eigen communicatienetwerken af te schermen zou de behoefte aan spionage voor dergelijke criminele netwerken afnemen (KLPD, DNRI, 2004: 115, 121).

Illegale handel

Wat betreft illegale handel (in drugs, geneesmiddelen, vuurwapens en explosieven, gestolen goederen, mensenhandel en -smokkel en illegale kansspelen) zijn er doorgaans minimaal twee typen daders te onderscheiden, namelijk de aanbieders (producenten, vervaardigers, dealers) en de afnemers (eindgebruikers). We beperken ons in deze bijlage tot de eerste categorie: de *aanbieders* van illegale handel. Over de individuele daderkenmerken en HT-CSV's met betrekking tot het aanbod van illegale handel op het internet zijn er weinig tot geen bijzonderheden te vinden in de literatuur. We beschrijven per subthema onze (summiere) bevindingen.

Drugs
Van de handel in drugs kan algemeen worden vastgesteld dat Nederland een belangrijk doorvoer- en distributiecentrum is van Zuidwest-Aziatische heroïne (bijvoorbeeld Afghanistan). Volgens Europol zijn het vooral Turkse CSV's die deze handel domineren en worden de winsten in onroerend goed in Nederland geïnvesteerd (TK 2005-2006, 29 911 nr. 4: 5). Ook voor de handel in cocaïne (afkomstig uit Venezuela, de Nederlandse Antillen, Suriname, Brazilië en Peru) vormt Nederland een belangrijk distributieknooppunt naar andere Europese landen. De productie en handel in synthetische drugs (XTC) ligt in handen van een beperkt aantal Nederlanders in het zuidwesten van het land, al is er een trend waarneembaar dat de productie zich verplaatst naar België en dat ook Chinese CSV's zich zijn gaan toeleggen op deze handel (TK 2005-2006, 29 911 nr. 4: 6). Het daadwerkelijk aanbieden van illegale drugs via het internet is waarschijnlijk beperkt door de zichtbaarheid ervan voor de opsporing. Wel worden overigens (chemische) grondstoffen en benodigdheden voor de productie van synthetische drugs op het internet aangeboden (NDB2004: 44-45, 116-177). Over de aanbieders van de illegale handel op internet zijn in de literatuur geen bijzonderheden bekend. Interessant detail is wel dat volgens onderzoek van de FBI drugsdealers in de VS zich steeds meer zijn gaan richten op identiteitsfraude (zie ook hoofdstuk 4).

Geneesmiddelen
Over de illegale handel in geneesmiddelen via het internet worden geen specifieke daderkenmerken beschreven in de literatuur.

Vuurwapens en explosieven
Wat betreft de handel in vuurwapens zijn er in Nederland geen omvangrijke CSV's actief (KLPD, DNR, 2005: 79; TK 2005-2006, 29 911 nr. 4: 8).

Heling
Uit recent onderzoek naar helingpraktijken in Nederland (Van de Mheen e.a., 2007) kwam naar voren dat het voor de helft van de geregistreerde helingzaken gaat om auto's, fietsen en geld (witwassen) en voor de helft om goederen als elektronica, kleding, sieraden, genotsmiddelen en voeding. Populaire distributiekanalen hiervoor zijn niet alleen de zwarte markt (bijvoorbeeld Beverwijk) maar ook het internet. Als belangrijkste redenen voor het internetgebruik worden de grootte van de afzetmarkt genoemd en het feit dat het relatief veilig is (risico's zijn klein) om gestolen goederen langs deze weg te verkopen. Daders blijken ook betrokken bij creditcardfraude en witwaspraktijken (Europol, 2003: 31). In hoeverre sprake is van echte georganiseerde handel op het internet blijft enigszins onduidelijk.

Mensenhandel en -smokkel
Verdachten van mensensmokkel (niet specifiek als high-tech crime) blijken vaak de Nederlandse, Turkse, Chinese, of Nigeriaanse nationaliteit te hebben (Siegel, 2007; TK 2005-2006, 29 911 nr. 4). Een groot deel van de CSV's die betrokken zijn bij mensenhandel blijken ook betrokken te zijn bij vermogensdelicten, drugs- en wapenhandel (TK 2005-2006, 29 911 nr. 4: 7).

Illegale kansspelen
Aanbieders van illegale kansspelen via het internet (waarbij uitnodigingen tot kansspelen worden gericht aan het Nederlandse publiek) zijn voor het overgrote deel van Nederlandse (45%) en Canadese (19%) nationaliteit (KLPD, 2003; Planet internet, 19 september 2005). In hoeverre dit georganiseerd plaatsvindt is niet bekend.

Geconcludeerd kan worden dat er slecht zicht is op de individuele daders achter de illegale handel die schuilgaat op het internet. Wat vooral van de traditionele CSV's (drugs, vuurwapens, mensenhandel) HT-CSV's zou kunnen maken is voornamelijk het gebruik van ICT als communicatiemiddel en niet het internet als handelsplaats als zodanig (zie ook Hynds, aangehaald door McCusker, 2006; Kortekaas, 2005; NDB2004). Uitzonderingen hierop kunnen zijn de illegale handel in geneesmiddelen, gestolen goederen en illegale kansspelen, omdat daarvoor het grote bereik naar afnemers toe (het internettende publiek) bepalend is voor de criminele winsten die er gemaakt worden. Nader onderzoek op dit gebied kan hierover uitsluitsel geven.

Financieel-economische criminaliteit

Marktmanipulatie
Over de individuele daderkenmerken van financieel-economische criminaliteit in relatie tot high-tech crime zijn er op het gebied van marktmanipulatie geen bijzonderheden te vinden in de literatuur. Uit onderzoek van de FBI in de jaren negentig is wel gebleken dat Amerikaanse en Russische HT-CSV's betrokken waren bij zogenoemde 'pump and dump'-technieken (Williams, 2001). Het internet werd hierbij gebruikt voor het verspreiden van (des)informatie om aandelenprijzen kunstmatig op te drijven.

Afpersing en chantage
Bij afpersing en chantage zijn hackers betrokken die hun technische expertise voor financieel gewin of uit wraak (bijvoorbeeld in geval van ontslagen ex-werknemers[176]) inzetten voor het plegen van misdrijven (KLPD, DNRI, 2007b: 2, 13-16). Meestal gebeurt dit in de vorm van het dreigen met het platleggen van systemen door een dDoS-aanval. Daarvoor is enerzijds de technische expertise nodig voor het ontwikkelen en uitvoeren van de aanval, maar anderzijds zijn ook vaardigheden nodig voor het daadwerkelijk afpersen van doelwitten en het innen van gelden. Deze onderwereldactiviteiten vereisen specifieke vaardigheden die hackers niet per definitie op het lijf geschreven staan. Volgens het KLPD (KLPD, DNRI, 2007b: 15) is het dan ook aannemelijk dat de technische en de meer actiegerichte taken door verschillende personen wordt uitgevoerd, en dat hackers zich laten inhuren door HT-CSV's. Hackers zijn bijvoorbeeld ook betrokken bij phishing via het internet, identiteitsdiefstal en het schrijven en verspreiden van malware. De hackers worden op het internet geworven en op grond van hun deskundigheid (bijvoorbeeld botnets) als dienstverleners ingehuurd (KLPD, DNRI, 2007b: 14). De georganiseerde misdaad heeft zich altijd al ingelaten met afpersingspraktijken. Met de voortschrijdende ontwikkelingen op het gebied van ICT zal dit zich volgens Europol (2003: 44) steeds meer verplaatsen naar het virtuele domein. Volgens de politie is er sprake van samenwerking tussen hackers uit West-Europese landen en traditionele CSV's uit Rusland en Oost-Europa (Boerman en Mooij, 2006; KLPD, DNRI, 2007b: 23). Uit gegevens van Europol (2003: 51) blijkt dat vermeende Russische CSV's in de VS online goksites tijdelijk uit de lucht haalden (met een DoS-aanval) waarna de webeigenaren een bedrag moesten betalen aan de afpersers om te voorkomen dat de hele website zou worden vernield (Europol, 2003: 51). Hoewel er in de VS meerdere gevallen van afpersing door dDoS-dreiging is gemeld lijkt het in Nederland tot op heden om een zeldzaam fenomeen te gaan (Boerman en

176 Ook in de zaak van de Tilburgse hackers die een Amerikaans bedrijf afpersten onder dreiging van een dDoS-aanval bleek een van de verdachten door het bedrijf te zijn ontslagen (Webwereld, 4 november 2005).

Mooij, 2006). De daadwerkelijke omvang van het probleem in Nederland zou echter groter kunnen zijn dan uit de registraties naar voren komt, bijvoorbeeld omdat bedrijven bang zijn voor imagoschade en niet in het nieuws willen brengen dat zij ingaan op de eisen van afpersers om losgeld te betalen (KLPD, DNRI, 2007b: 6).

Illegale communicatie

Cyberstalking
Uit onderzoek naar fysieke stalkers worden motieven genoemd als verzoening, wraak, eenzaamheid of de behoefte aan macht, en niet zelden is sprake van een psychiatrische aandoening (Baas, 2003; Zona e.a. 1993, Mullen e.a. 1999, aangehaald door McFarlane en Bocij, 2003: 4; Taylor e.a., 2006: 180). Volgens Gelderblom (2004: 216) zijn fysieke stalkers extreem jaloers, snel boos, manipulatief (spelen in op andermans schuldgevoelens), gefascineerd door geweld, overdreven vriendelijk, geven zij anderen onverwacht ongepaste cadeaus, bieden ongevraagd hulp aan en accepteren geen nee. Er zijn overeenkomsten en verschillen tussen traditionele fysieke stalkers en cyberstalkers (McFarlane en Bocij, 2003; Taylor e.a., 2006: 182). In beide gevallen gaat het vaak om blanke, alleenstaande mannen die eerder met justitie in aanraking zijn geweest (bijvoorbeeld voor diefstal, wapenbezit, fysiek geweld). Zij hebben de behoefte om dicht bij het slachtoffer te komen en willen het slachtoffer controleren of straffen. Om dit te bereiken vertoont men obsessief gedrag (Benschop, 2007b). In sommige gevallen heeft de dader een liefdes- of datingrelatie met het slachtoffer of zijn dader en slachtoffer bijvoorbeeld collega's van elkaar. Over het algemeen zijn stalkers psychisch of emotioneel labiel (zij beelden zich bijvoorbeeld in dat het slachtoffer een liefdesrelatie met hen wenst).

Specifiek voor cyberstalkers is dat zij gebruikmaken van e-mail, intranet en discussiegroepen op het internet (zoals bulletin boards en chatrooms) om anderen lastig te vallen. Door de relatieve anonimiteit zijn zij brutaler en schaamtelozer in hun gedrag dan fysieke stalkers (Taylor e.a., 2006: 180-182). Hoewel cyberstalkers door de aard van het contact zich niet per se in de fysieke nabijheid van het slachtoffer hoeven op te houden, blijkt dat dit wel vaak het geval is: daders wonen veelal dicht bij het slachtoffer (Wykes, 2007: 138). Cyberstalkers opereren vaak individueel en

Daderkenmerken cyberstalking:
Sociaal-demografische kenmerken:
– man
– blank
– alleenstaand en alleenwonend
– woont in fysieke nabijheid van het slachtoffer
(Technische) kennis en vaardigheden:
– virtueel actief via e-mail, intranet, discussieforums
– redelijk goede computervaardigheden
Primaire motivatie:
– macht (behoefte om het slachtoffer te controleren of te straffen)
– wraak (aanleiding kan een uit de hand gelopen, triviale discussie zijn)
– affectie (is eenzaam en zoekt een partner)
Sociaal-psychologisch profiel:
– bekende van het slachtoffer (ex-geliefde, e-datingpartner, collega)
– psychisch of emotioneel labiel
– obsessief
– gebrek aan invoelingsvermogen en sociale vaardigheden
– brutale en schaamteloze taal via chatrooms
– bedreigt, intimideert, is extreem jaloers, manipulatief, snel boos
– fascinatie voor geweld
Criminele carrière:
– mogelijk strafblad (diefstal, offline stalking, wapenbezit, fysiek geweld)
Verschijningsvormen van high-tech crime:
– spamming
– e-mail bommen
– identiteitsfraude

richten hun activiteiten meestal tegen andere individuen (of organisaties). Er is dus geen sprake van HT-CSV's. Aan de hand van interviews met *slachtoffers* van cyberstalking onderscheiden McFarlane en Bocij (2003) vier typen daders:[177]
– de wraakzuchtige stalker: heeft een psychiatrische stoornis, handelt uit wraak (bijvoorbeeld na een uit de hand gelopen, triviale discussie), stalkt het slachtoffer ook fysiek, en heeft mogelijk een strafblad;
– de beheerste stalker: wil het slachtoffer daadwerkelijk kwellen of irriteren (is niet uit op een relatie met het slachtoffer) en heeft ook mogelijk een strafblad;
– de collectieve stalker: doet het domweg om anderen te intimideren en maakt gebruik van geavanceerde technologieën (zoals spam, e-mail bommen en identiteitsfraude);

177 De auteurs interviewden 24 slachtoffers (waarvan 22 vrouwen) uit het Verenigd Koninkrijk, de VS, Canada en Nieuw-Zeeland. De geringe onderzoekspopulatie (N=24) maakt de resultaten van dit onderzoek echter niet zonder meer generaliseerbaar.

– de intieme stalker: vraagt vooral aandacht en affectie van het slachtoffer (mogelijk een ex-partner).

Discriminatie
In tegenstelling tot cyberstalking komt discriminatie juist vaak voor in groepsverband en is dit ook meestal gericht tegen groepen. Wanneer dit gepaard gaat met oproepen tot geweld, is er sprake van haatzaaien (of 'hate crime'). Levin en McDevitt (aangehaald door Mann e.a., 2003) onderscheiden vier motieven voor zogenoemde hate crime. Men kan anderen discrimineren:
– voor de lol (om indruk te maken op vrienden);
– als waarschuwingssignaal (om anderen te overtuigen iets te doen of te laten);
– als vergeldingsactie (dat kan escaleren tot een grootschalig groepsconflict);
– als missie (waarbij men het als een taak ervaart om doelwitten aan te vallen).

Uit onderzoek blijkt dat in Nederland in de meeste gevallen Marokkanen, Afrikanen, moslims en joden doelwit zijn van discriminerende, haatzaaiende en tot geweld oproepende uitingen (Landelijk Expertisecentrum Discriminatie, 2004; Meldpunt Discriminatie Internet: MDI, 2005). Daders zijn veelal extreem-rechts maar ook een aanzienlijk deel is zelf van Turkse of Marokkaanse afkomst. Kenmerkend voor de meeste 'haatcriminelen' op het internet is dat de betrokkenen erg jong zijn. In bijna de helft van de gevallen is er sprake van jongeren onder de 19 jaar (Van Stokkom e.a., 2007: 194). Volgens Chau en Xu (2007: 60) is dit te verklaren uit het gegeven dat juist deze groep zeer actief is op het internet. Voor een groot deel worden discriminerende en haatzaaiende uitingen gedaan op interactieve websites (webforums en weblogs). Van Stokkom en anderen (2007: 197) concluderen op grond van gegevens van het MDI dat er een 'virtuele burgeroorlog' wordt gevoerd tussen voornamelijk extreem-rechtse en radicale moslimsites (en weblogs). Er lijkt sprake te zijn van jeugd-subculturen waarbinnen het vooral 'stoer' is om zich op deze manier te profileren naar de buitenwereld (zie ook radicalisering: hoofdstukken 2 en 3). Het gaat om min of meer hechte virtuele gemeenschappen, met een gedeelde collectieve identiteit en een relatief kleine kern van invloedrijke individuen (personen van wie de weblog[178] met grote regelmaat door anderen wordt bezocht). De zogenoemde 'hate crimes' ontberen feitelijk echter enige vorm van planning en de haatgroepen zijn ook niet zo goed georganiseerd om zich te laten typeren

178 Een blog of weblog is een persoonlijke website waarop mensen een logboek bijhouden door dagelijks nieuwe informatie toe te voegen. Bezoekers kunnen over het algemeen reacties achterlaten op de weblog.

als HT-CSV (Schafer, 2003). Een probleem binnen de opsporing en vervolging is dat verdachten vaak 'nicknames' gebruiken en de websites veelal worden gehost op buitenlandse servers (Meldpunt Discriminatie Internet, 2 mei 2006).

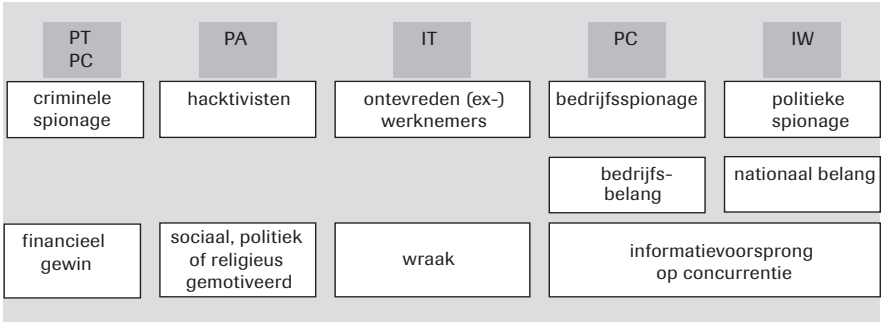
> Een indrukwekkende studie van 28 racistische 'anti-black' haatgroepen (en 820 bloggers[179]) op het internet (op www.xanga.com) is die van Chau en Xu (2007). In dit onderzoek werd gebruikgemaakt van sociale netwerkanalyse van internetverkeer en -contacten waarin expliciete haatdragende en racistische uitspraken werden gedaan over mensen van Afrikaanse afkomst. De meeste bloggers binnen de 28 onderzochte haatgroepen waren mannelijke Amerikanen. Uit analyse van de berichten die werden achtergelaten via de blogs kwam naar voren dat de haatgroepen geclusterd waren: dezelfde personen die over en weer met elkaar communiceren, zijn vaak te vinden op meerdere webforums.

Spionage
Wat betreft spionage zijn er volgens Morris (2004: 16) vijf dadercategorieën te onderscheiden:
- ontevreden werknemers (die handelen uit wraak);
- bedrijfsspionnen (die voor de concurrent werken);
- criminele spionnen (die gevoelige informatie stelen en doorverkopen);
- hacktivisten (met sociaal, politieke of religieuze motieven);
- politieke spionnen die handelen in het nationale belang (bijvoorbeeld militaire of veiligheidsdiensten).

Concrete daderkenmerken zijn in de literatuur niet voorhanden. Binnen de taxonomie van Rogers (2000, 2001, 2006) (zie hoofdstuk 3) worden spionnen als hackers beschouwd (zie ook schema B2). Vergelijken we bovenstaande indeling van Morris met de hackertaxonomie van Rogers, dan kunnen de ontevreden werknemers als 'internal' (IT) worden aangemerkt, de bedrijfsspionnen als 'professional criminal' (PC), de criminele spionnen als 'petty thief' (PT) of 'professional criminal' (PC), de hacktivisten als 'political activist' (PA), en de politieke spionnen als 'information warrior' (IW). Voor nadere informatie over de daderkenmerken van deze hackers verwijzen we naar paragraaf 3.2.9.

179 Bezoekers van een weblog.

Schema B2 Vijf typen van spionage (naar Morris, 2004) en hacker-categorieën (naar Rogers, 2006)



(PT: petty thief, PC: professional criminal, PA: political activist, IT: internal, IW: information warrior)

Ongeautoriseerde toegang tot ICT

De subthema's binnen dit cluster (hacking en botnets) zijn beschreven in de hoofdstukken 3 en 4.

ICT-storing door gegevensverkeer

(d)DoS-aanval
Het veroorzaken van ICT-storingen vindt bewust plaats wanneer sprake is van een (d)DoS-aanval. Bij een (d)DoS-aanval wordt een website door massale verzending van gegevens (met behulp van botnets) zodanig overbelast dat deze niet meer beschikbaar is. Motieven kunnen zijn financieel gewin (zie ook afpersing met behulp van een dDoS-aanval); petty thiefs of professional criminals), maar ook wraak (internals), protest (political activists) of vandalisme (cyberpunks) (de verwijzingen tussen haakjes refereren aan de hackertaxonomie van Rogers, zie paragraaf 3.2.9). Volgens het NCIS (2002, aangehaald in Van der Werf, 2003: 28) blijken daders niet zelden afvallige of ontevreden werknemers. Op basis van Nederlandse HKS gegevens over 2001-2002 concludeerde Van der Werf (2003: 29) dat het in Nederland vooral om autochtone mannen gaat. In een recent rapport concludeerden Boerman en Mooij (2006) dat het ook om hackers gaat (virus writers) die ontdekt hebben dat ze geld kunnen verdienen met hun expertise (met name op het gebied van botnets, maar hackers zijn ook betrokken bij identiteitsfraude met behulp van phishing). In het deelrapport voor de Vervolgstudie over dDoS-aanvallen (KLPD/DNRI, 2007b) blijft het de vraag of sprake is van 'georganiseerde criminaliteit' volgens de gehanteerde definitie. Op grond van theoretische overwegingen gaat het om een nieuw type HT-CSV's waarvoor een sociale basis en onderling

vertrouwen tussen de betrokkenen minder van belang is dan bij de traditionele CSV's. Anderzijds lijkt ook dat traditionele CSV's zich meer gaan toeleggen op high-tech crime, en voor de technische know-how mensen gericht inhuren.[180]

Spamming
ICT-systemen kunnen als gevolg van spamming overbelast en daardoor verstoord raken, wat doorgaans niet het doel maar eerder een nevenproduct is. In sommige gevallen gaat het om activiteiten van de 'cyberpunk' uit de hackertaxonomie van Rogers. Uit de literatuur is geen concrete informatie te herleiden naar daderkenmerken van spammers.

ICT-storing door manipulatie van data en gegevens

Defacing
ICT-storingen kunnen ook ontstaan door het bewust manipuleren van gegevens. Bij defacing worden websites aangepast of vernield. Daders die zich hieraan schuldig maken, kunnen ideologische motieven hebben (politieke activisten: zie ook hacktivisme) of handelen om andere persoonlijke redenen (bijvoorbeeld uit vandalisme). Volgens de hackertaxonomie van Rogers (2000, 2001, 2006) zijn defacers vooral 'cyberpunks' die onnodig schade aanrichten aan websites.

(H)acktivisme
Hacktivisme (zie ook spionage) wordt in de literatuur beschouwd als een subcategorie van hacking. Er zijn weinig bijzonderheden over deze variant van high-tech crime bekend. We verwijzen daarom ook hier voor meer informatie naar de hackertaxonomie (political activist) van Rogers (paragraaf 3.2.9).

Dienstverleners

Voor de subthema's binnen dit cluster verwijzen we naar hoofdstukken 3 en 4.

Conclusie

Ook de inventarisatie van daderkenmerken en HT-CSV's voor de niet-geprioriteerde thema's laat zien dat er erg weinig concrete informatie te vinden is in de literatuur. We vatten de bevindingen, net als in hoofdstuk 4,

180 Botnets worden door hackers verhuurd of verkocht maar hackers worden soms ook ingehuurd voor het in opdracht uitvoeren van dDoS-aanvallen (Boerman en Mooij, 2006: 32).

samen in schema B3. Onder diversificatie staat in het eerste deel van het schema de overlap tussen de niet-geprioriteerde verschijningsvormen van high-tech crime, met overige criminele activiteiten schuingedrukt. Ook hieruit blijkt de belangrijke multifunctionele rol van hacking voor het plegen van high-tech crime. Ook sociaal-demografische kenmerken, motieven, toegepaste technieken, vereiste kennis en vaardigheden, criminele achtergrond, en de wijze van organisatie (rekrutering, internationale connecties) zijn in het schema weergegeven.[181] Aan de hand daarvan zien we bijvoorbeeld dat de meeste (niet-geprioriteerde) vormen van high-tech crime worden gepleegd uit financieel oogpunt en/of wraak. Met name de illegale handel in drugs, mensenhandel en -smokkel, en illegale kansspelen is sprake van internationale connecties. Over cyberstalking en discriminatie is relatief het meest bekend in de literatuur in tegenstelling tot de overige verschijningsvormen. Opnieuw concluderen we dat er veel gebrek is aan kennis over daders en dadergroepen van high-tech crime.

Schema B3 Kenmerken van daders en HT-CSV's voor niet-geprioriteerde thema's van high-tech crime

	Afscherming	Drugs	Geneesmiddelen	Vuurwapens explosieven	Heling	Mensenhandel/smokkel	Illegale kansspelen	Marktmanipulatie	Afpersing en chantage	Cyberstalking	Discriminatie	Spionage	(d)DoS-aanval	Spamming	Defacing	(H)acktivisme
Diversificatie																
Afscherming																
Drugs	x															
Geneesmiddelen																
Vuurwapens en explosieven	x															
Heling																
Mensenhandel en -smokkel		x		x												
Illegale kansspelen																
Marktmanipulatie																
Afpersing en chantage																
Cyberstalking																
Discriminatie																
Spionage																
(d)DoS-aanval																
Spamming																

181 Informatie over uitvoering (planning, expertise, methoden, specialisatie), netwerken (structuren, kwetsbaarheden) en hulpbronnen (training, materiaal, steun) ontbreken en zijn weggelaten uit het schema.

Schema B3 (Vervolg)

	Afscherming	Drugs	Geneesmiddelen	Vuurwapens explosieven	Heling	Mensenhandel/smokkel	Illegale kansspelen	Marktmanipulatie	Afpersing en chantage	Cyberstalking	Discriminatie	Spionage	(d)DoS-aanval	Spamming	Defacing	(H)acktivisme
Defacing																
(H)acktivisme												x			x	
Hacking	x								x			x	x	x		x
Onroerend goed		x														
Identiteitsfraude		x														
Witwassen					x											
Internetfraude														x		
Creditcardfraude					x											
dDoS-aanvallen									x							
Sociaal-demografisch																
Man										x			x			
Blank										x	x		x			
< 19 jaar											x					
Marokkaans											x					
Turks											x					
Alleenstaand										x						
Dichtbij slachtoffer										x						
ZW-Nederland		xtc														
Amerika								x								
Rusland								x								
Motieven																
Financieel gewin		x	x	x	x	x	x	x	x			x	x	x	x	
Wraak									x	x	x	x	x			
Verzoening										x						
Macht										x						
Stoer doen / vandalisme											x		x		x	
Waarschuwing											x					
Missie											x					
Extreem-rechtse sympathieën											x					
Radicaal-islamistische sympathieën											x					
Ideologie / protest												x	x		x	

Schema B3 (Vervolg)

	Afscherming	Drugs	Geneesmiddelen	Vuurwapens explosieven	Heling	Mensenhandel/smokkel	Illegale kansspelen	Marktmanipulatie	Afpersing en chantage	Cyberstalking	Discriminatie	Spionage	(d)DoS-aanval	Spamming	Defacing	(H)acktivisme
Technieken																
Botnets													x			
E-mail										x						
Intranet										x						
Discussiegroepen										x	x					
Weblogs											x					
Nicknames											x					
Kennis/vaardigheden																
Computerervaring																
Programmeerervaring																
Criminele carrière																
Diefstal										x						
Wapenbezit										x						
Fysiek geweld										x						
Organisatie																
Organisatie																
Rekrutering / aantrekkingskracht																
Internet									x							
Sociale affiliatie																
Internationale connecties																
Rusland									x							
Oost-Europa									x							
West-Europa									x							
Azië																
Turkije		x				x										
België		x														
China		x				x										
Canada							x									

Onder diversificatie staat in het eerste deel van het schema de overlap tussen de niet-geprioriteerde verschijningsvormen van high-tech crime, met overige criminele activiteiten schuingedrukt. Ook hieruit blijkt de belangrijke multifunctionele rol van hacking voor het plegen van high-tech crime. Ook sociaal-demografische kenmerken, motieven, toegepaste technieken, vereiste kennis en vaardigheden, criminele achtergrond, en de wijze van organisatie (rekrutering, internationale connecties) zijn in het schema weergegeven.[182] Aan de hand daarvan zien we bijvoorbeeld dat de meeste (niet-geprioriteerde) vormen van high-tech crime worden gepleegd uit financieel oogpunt en/of wraak. Met name de illegale handel in drugs, mensenhandel en -smokkel, en illegale kansspelen is sprake van internationale connecties. Over cyberstalking en discriminatie is relatief het meest bekend in de literatuur in tegenstelling tot de overige verschijningsvormen. Opnieuw concluderen we dat er veel gebrek is aan kennis over daders en dadergroepen van high-tech crime.

182 Informatie over uitvoering (planning, expertise, methoden, specialisatie), netwerken (structuren, kwetsbaarheden) en hulpbronnen (training, materiaal, steun) ontbreken en zijn weggelaten uit het schema.

Bijlage 7
Voorbeeld van een profiel

De Computer Crime Adversarial Matrix (Icove, 1995) van de FBI (uit Casey, 2002: 552-554)

	Crackers		Spionage	Fraude
	Groep	Individu		
Organisatie				
Organisatie	(Tegen)subcultuur	Loners	Vijandige intelligence-diensten	Klein netwerk of alleen
Rekrutering / aantrekkingskracht	Peer group	Intellectuele uitdaging	– financieel gewin – ideologie – aandacht	– financieel gewin – macht
Internationale connecties	Contacten met andere groepen wereldwijd	Lid van journals en bulletin boards	Via hacking wereldwijd toegang	Gebruik van money-transfers
Uitvoering				
Planning	In detail	Voorstudie	In detail	In detail
Niveau expertise	Hoog	Gemiddeld tot hoog (ervaring wisselt uit via netwerken)	Hoog	Gemiddeld tot hoog (meer ervaring fraude dan high-tech crime)
Methoden	– computer-vredebreuk	– trial and error – wisselt informatie uit met andere hackers	Cracker als dienstverlener om info te verkrijgen	Gebruikt basale methoden (bijv. afluisteren)
Gedrag				
Motivatie	– intellectuele uitdaging – peer group fun – ideologie	– intellectuele uitdaging – probleem op te lossen – macht – financieel gewin – ideologie	– financieel gewin – informatie	– financieel gewin – persoonlijk voordeel – macht
Persoonlijke kenmerken	– intelligente mensen – (tegen)subcultuur	Gemiddeld tot hoog intelligent	Crackers (in groep of zelfstandig)	Zoals iedere fraudeur
Kwetsbaarheden	Praat openlijk over activiteiten	Houdt aantekeningen bij	Kan te gretig en onvoorzichtig worden om informatie te bemachtigen	Kan te gretig en onvoorzichtig worden
Resources				
Training	Expertise door veel informele training	Expertise door ervaring	Niveau van expertise verschilt	Sommigen hebben programmeerervaring
Materiaal	Computer en internetaansluiting	Computer en internetaansluiting	– computer en internetaansluiting – geavanceerde ICT	Computer en internetaansluiting
Steun	Peer group	Via informatie uitwisseling	Intelligence-diensten	Peer group of criminele organisatie

WODC-rapporten

Om zo veel mogelijk belanghebbenden te informeren over de onderzoeksresultaten van het WODC wordt een beperkte oplage van de rapporten kosteloos verspreid onder functionarissen, werkgroepen en instellingen binnen en buiten het Ministerie van Justitie. Dit gebeurt aan de hand van een verzendlijst die afhankelijk van het onderwerp van het rapport opgesteld wordt. De rapporten in de reeks Onderzoek en beleid (O&B) worden uitgegeven door Boom Juridische uitgevers en zijn voor belangstellenden die niet voor een kosteloos rapport in aanmerking komen, te bestellen bij Boom distributiecentrum, postbus 400, 7940 AK Meppel, tel.: 0522-23 75 55, via e-mail: bdc@bdc.boom.nl.
Een complete lijst van de WODC-rapporten is te vinden op de WODC-site (www.wodc.nl). Daar zijn ook de uitgebreide samenvattingen te vinden van alle vanaf 1997 verschenen WODC-rapporten. Volledige teksten van de rapporten (vanaf 1999) zullen met terugwerkende kracht op de WODC-site beschikbaar komen. Hieronder volgen de titelbeschrijvingen van de vanaf 2002 verschenen rapporten.

Kamphorst, P.A., G.J. Terlouw
Van vast naar mobiel; Een evaluatie van het experiment met elektronisch huisarrest voor minderjarigen als modaliteit voor de voorlopige hechtenis
2002, O&B 195

Moolenaar, D.E.G., F.P. van Tulder, G.L.A.M. Huijbregts, W. van der Heide
Prognose van de sanctiecapaciteit tot en met 2006
2002, O&B 196

Bokhorst, R.J., C.H. de Kogel, C.F.M. van der Meij
Evaluatie van de Wet BOB; Fase 1: de eerste praktijkervaringen met de Wet bijzondere opsporingsbevoegdheden
2002, O&B 197

Kleemans, E.R., M.E.I. Brienen, H.G. van de Bunt, m.m.v.
R.F. Kouwenberg, G. Paulides, J. Barendsen
Georganiseerde criminaliteit in Nederland; Tweede rapportage op basis van de WODC-monitor
2002, O&B 198

Voert, M. ter, J. Kuppens
Schijn van partijdigheid rechters
2002, O&B 199

Daalder, A.L.
Het bordeelverbod opgeheven; Prostitutie in 2000-2001
2002, O&B 200

Klijn, A.
Naamrecht
2002, O&B 201

Kruissink, M., C. Verwers
Jeugdreclassering in de praktijk
2002, O&B 202

Eshuis, R.J.J.
Van rechtbank naar kanton; Evaluatie van de competentiegrensverhoging voor civiele handelszaken in 1999
2002, O&B 203

Meijer, R.F., M. Grapendaal, M.M.J. van Ooyen, B.S.J. Wartna, M. Brouwers, A.A.M. Essers
Geregistreerde drugcriminaliteit in cijfers; Achtergrondstudie bij het Justitieonderdeel van de Nationale Drugmonitor: Jaarbericht 2002
2003, O&B 204

Tak, P.J.J.
The Dutch criminal justice system; Organization and operation – second revized edition
2003, O&B 205

Kromhout, M., M. van San
Schimmige werelden; Nieuwe etnische groepen en jeugdcriminaliteit
2003, O&B 206

Kogel, C.H. de, C. Verwers
De longstay afdeling van Veldzicht; Een evaluatie
2003, O&B 207

Moolenaar, D.E.G., G.L.A.M. Huijbregts
Sanctiecapaciteit 2007; Een beleidsneutrale prognose
2003, O&B 208

Eshuis, R.J.J.
Claims bij de rechtbank
2003, O&B 209

Combrink-Kuiters, L., E. Niemeyer, M. ter Voert, m.m.v. N. Dijkhoff, M. van Gammeren-Zoeteweij, J. Kuppens
Ruimte voor Mediation
2003, O&B 210

Heide, W. van der, A.Th.J. Eggen (red.)
Criminaliteit en rechtshandhaving 2001; Ontwikkelingen en samenhangen
2003, O&B 211

European Sourcebook
European Sourcebook of Crime and Criminal Justice Statistics – 2003
2003, O&B 212

Smit, P.R., F.P. van Tulder, R.F. Meijer, P.P.J. Groen
Het opheldering spercentage nader beschouwd
2003, O&B 213

Dijksterhuis, B.M., M.J.G. Jacobs, W.M. de Jongste
De competentiegrens van enkelvoudige kamers in strafzaken
2003, O&B 214

Bunt, H.G. van de, C.R.A. van der Schoot
Prevention of Organised Crime; A situational approach
2003, O&B 215

Wartna, B.S.J., N. Tollenaar
Bekenden van Justitie
2004, O&B 216

Moolenaar, D.E.G., P.P.J. Groen, A.G. Mein, B.S.J. Wartna, M. Blom
Wegenverkeerswet 1994
2004, O&B 217

Faber, W., A.A.A. van Nunen
Uit onverdachte bron
2004, O&B 218

Velthoven, B.C.J. van, M.J. ter Voert, m.m.v. M. van Gammeren-Zoeteweij
Geschilbeslechtingsdelta 2003; Over verloop en afloop van (potentieel) juridische problemen van burgers
2004, O&B 219

Leuw E., R.V. Bijl, A. Daalder
Pedoseksuele delinquentie; Een onderzoek naar prevalentie, toedracht en strafrechtelijke interventies
2004, O&B 220

Leertouwer, E.C., G.L.A.M. Huijbregts
Sanctiecapaciteit 2008
2004, O&B 221

Beijer, A., R.J. Bokhorst, M. Boone, C.H. Brants, J.M.W. Lindeman
De wet bijzondere opsporingsbevoegdheden – eindevaluatie
2004, O&B 222

Moors, J.A., M.Y.W. von Bergh, S. Bogaerts, J.W.M.W. van Poppel, A.M. van Kalmthout
Kiezen voor delen?
2004, O&B 223

Adriaanse, J.A.A., N.J.H. Huls, J.G. Kuijl: Vos
Informele reorganisatie in het perspectief van surseance van betaling, WSNP en faillissement
2004, O&B 224

Jong, P.O. de, M. Herweijer
Alle regels tellen
2004, O&B 225

Kogel, C.H. de, C. Verwers, V.E. den Hartogh
'Blijvend delictgevaarlijk' – empirische schattingen en conceptuele verheldering
2004, O&B 226

Wartna, B.S.J., N. Tollenaar, M. Blom
Recidive 1997; Een cijfermatig overzicht van de strafrechtelijke recidive van volwassen en jeugdige daders
2005, O&B 227

Wartna, B.S.J., N. Tollenaar, A.A.M. Essers
Door na de gevangenis; Een cijfermatig overzicht van de strafrechtelijke recidive onder ex-gedetineerden
2005, O&B 228

Wartna, B.S.J., S. el Harbachi, A.M. van der Laan
Jong vast; Een cijfermatig overzicht van de strafrechtelijke recidive van ex-pupillen van justitiële jeugdinrichtingen
2005, O&B 229

Wartna, B.S.J., S. el Harbachi, L.M. van der Knaap
Buiten behandeling; Een cijfermatig overzicht van de strafrechtelijke recidive van ex-terbeschikkinggestelden
2005, O&B 230

Lünnemann, K.D., M.Y. Bruinsma
Geweld binnen en buiten; Aard, omvang en daders van huiselijk en publiek geweld in Nederland
2005, O&B 231

Erp, J.G. van, M.D. van Ewijk
Werklast bestuurlijke boete; Determinanten van de werkbelasting in de bestuursrechtspleging
2005, O&B 232

Broeksteeg, J.L.W., E.M.J. Hardy, S. Klosse, M.G.W.M. Peeters, L.F.M. Verhey
Zicht op wetgevingskwaliteit; Onderzoek naar de wetgevingsadvisering van de Raad van State
2005, O&B 233

Gritter, E., G. Knigge, N.J.M. Kwakman
De WED op de helling; Een onderzoek naar de wenselijkheid de Wet op de economische delicten te herzien
2005, O&B 234

Rovers, G.B., E. de Vries Robbé
Interne criminaliteit in de logistieke sector
2005, O&B 235

Kogel, G.H. de, V.E. den Hartogh
Contraire beëindiging van de TBS-maatregel; Aantal, aard en verband met recidive
2005, O&B 236

Eggen, A.Th.J., W. van der Heide (red.)
Criminaliteit en rechtshandhaving 2004; Ontwikkelingen en samenhangen
2006, O&B 237

Bruin, D.E. de, C.J.M. Meijerman, F.R.J. Leenders, R.V. Braam
Verslingerd aan meer dan een spel; Een onderzoek naar de aard en omvang van kansspelproblematiek in Nederland
2006, O&B 238

Knaap, L.M. van der, L.T.J. Nijssen, S. Bogaerts
Geweld verslagen? Een studie naar de preventie van geweld in het publieke en semi-publieke domein
2006, O&B 239 (239a, *Violence Defied?*)

Kogel, C.H. de, M.H. Nagtegaal, E. Neven, G. Vervaeke
Gewelddadige delinquenten met een psychische stoornis
2006, O&B 240

Martin Killias, Marcelo Fernando Aebi, Kauko Aromaa, Bruno Aubusson de Cavarlay, Gordon Barclay, Beata Gruszczyñska, Hanns von Hofer, Vasilika Hysi, Jörg – Martin Jehle, Paul Smit, Cynthia Tavares
European Sourcebook of Crime and Criminal Justice Statistics
2006, O&B 241

Faure, M.M.G., C.A.R. Moerland
Griffierechten; Een vergelijkende beschrijving van griffierechten- en vergelijkbare stelsels in een aantal landen van de Europese Unie
2006, O&B 242

Sikkel, D., P.G.M. van der Heijden, G. van Gils
Methoden voor omvangschattingen van verborgen populaties, met name illegalen
2006, O&B 243

Ferwerda, H.B., I.M.G.G. van Leiden, N.A.M. Arts, A.R. Hauber
Halt: Het Alternatief? De effecten van Halt beschreven
2006, O&B 244

Laan, A.M. van der, M. Blom
Jeugddelinquentie: risico's en bescherming; Bevindingen uit de WODC Monitor Zelfgerapporteerde Jeugdcriminaliteit 2005
2006, O&B 245

Poot, C.J. de, E.W. Kruisbergen
Kringen rond de dader; Grootschalig DNA-onderzoek als instrument in de opsporing
2006, O&B 246

Ewijk, M.D. van, M.J. ter Voert
Trendrapportage Gerechtsdeurwaarders 2006; Toegankelijkheid, continuïteit en kwaliteit van de ambtelijke dienstverlening
2006, O&B 247

Sackers, H.J.B., B.A.M. van Stokkom, J.-P. Wils
Godslastering, discriminerende uitingen wegens godsdienst en haatuitingen; Een inventariserende studie
2007, O&B 248

Daalder, A.L.
Prostitutie in Nederland na opheffing van het bordeelverbod
2007, O&B 249

Jennissen, R.P.W., J. Oudhof (red.)
Ontwikkelingen in de maatschappelijke participatie van allochtonen
2007, O&B 250

Mheen, D. van de, P. Gruter (red.)
Helingpraktijken onder de loep; Impressies van helingcircuits in Nederland
2007, O&B 251

H.G. van de, E.R. Kleemans
Georganiseerde criminaliteit in Nederland; Derde rapportage op basis van de Monitor Georganiseerde Criminaliteit
2007, O&B 252

Struiksma, N., J. de Ridder, H.B. Winter
De effectiviteit van bestuurlijke en strafrechtelijke milieuhandhaving
2007, O&B 253

Eshuis, R.J.J.
Het recht in betere tijden; Over de werking van interventies ter versnelling van civiele procedures
2007, O&B 254

Heide, W. van der, A.Th.J. Eggen (red.)
Criminaliteit en rechtshandhaving 2006; Ontwikkelingen en samenhangen
2007, O&B 255

Tollenaar, N., R.F. Meijer, G.L.A.M. Huijbrechts, M. Blom, S. el Harbachi
Monitor Veelplegers; Jeugdige en zeer actieve veelplegers in kaart gebracht
2007, O&B 256

Dijk, J. van, J. van Kesteren: Smit
Criminal Victimisation in International Perspective. Key findings from the 2004-2005 ICVS en EU ICS
2007, O&B 257

Spapens, A.C.M., H.G. van de Bunt, L. Rastovac
De wereld achter de wietteelt
2007, O&B 258

Koeter, M.W.J., M. Bakker
Effectevaluatie van de Strafrechtelijke Opvang Verslaafden (SOV)
2007, O&B 259

Kunst, M.J.J., S. Schweizer, S. Bogaerts, L.M. van der Knaap
Onderlinge agressie en geweld, posttraumatische stress en arbeidsverzuim in penitentiaire inrichtingen
2007, O&B 260 (260a, *Aggression and violence, posttraumatic stress, and absenteeism among employees in penitentiaries)*

Voert, M.J. ter, S.L. Peters
Trendrapportage advocatuur 2006; Toegankelijkheid, continuïteit en kwaliteit van de dienstverlening
2007, O&B 261

Boom, A. ten, K.F. Kuijpers, m.m.v. M.H. Moene
Behoeften van slachtoffers van delicten; Een systematische literatuurstudie naar behoeften zoals door slachtoffers zelf geuit
2008, O&B 262

C.H. de Kogel, M.H. Nagtegaal
Toezichtprogramma's voor delinquenten en forensisch psychiatrische patiënten; Effectiviteit en veronderstelde werkzame mechanismen
2008, O&B 263

Hulst, R.C. van der, R.J.M. Neve
High-tech crime, soorten criminaliteit en hun daders; Een literatuur-inventarisatie
2008, O&B 264