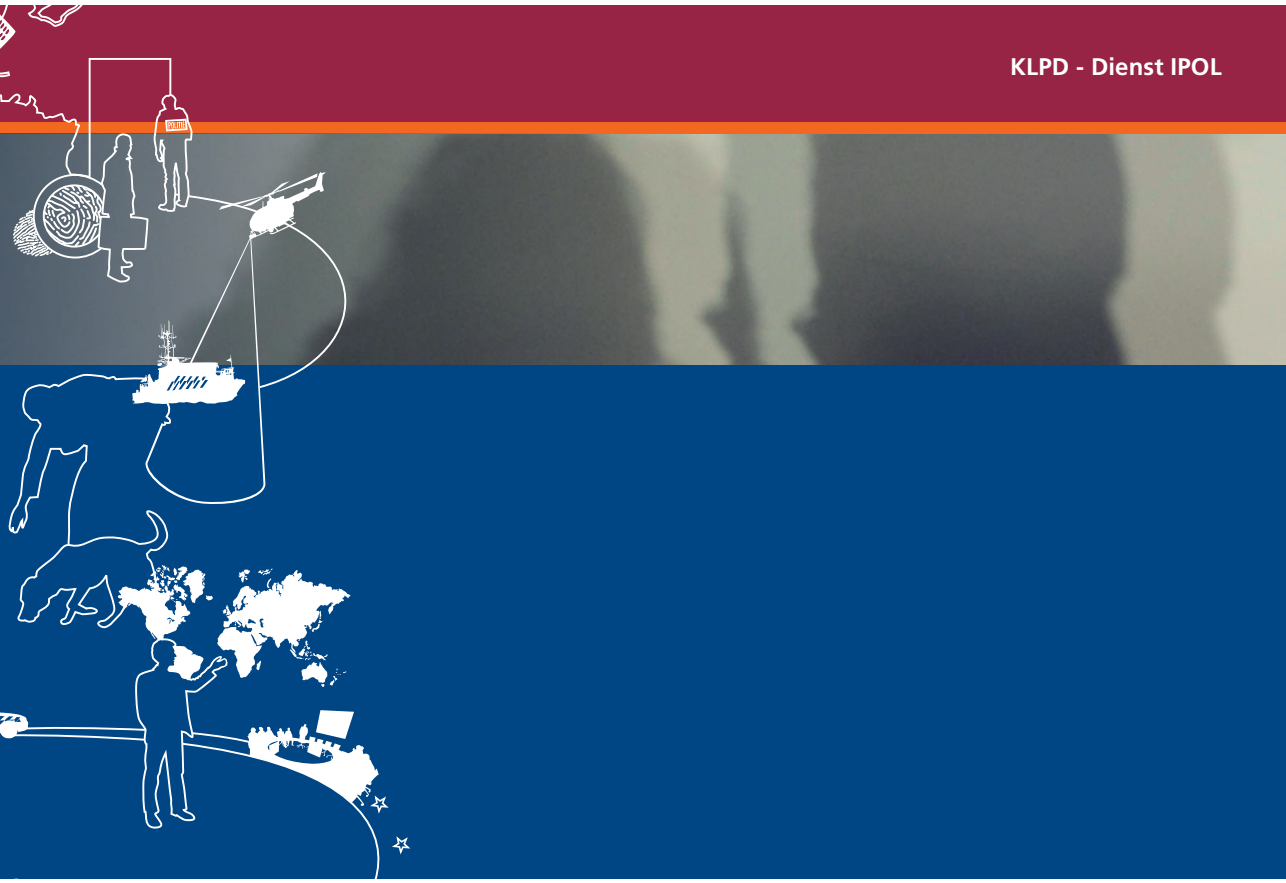
Actualisering van dreigingen uit 2004

Verslag van een onderzoek voor het Nationaal dreigingsbeeld 2008

KLPD - Dienst IPOL



«waakzaam en dienstbaar»

POLITIE
Korps landelijke politiediensten

Actualisering van dreigingen uit 2004

Verslag van een onderzoek voor het Nationaal dreigingsbeeld 2008

KLPD - Dienst IPOL

«waakzaam en dienstbaar»

POLITIE
Korps landelijke politiediensten

Uitgave

Korps landelijke politiediensten (KLPD)
Dienst IPOL
Postbus 3016
2700 KX Zoetermeer

Zoetermeer, oktober 2008

IPOL nummer 31-2008

Colofon

Tekst Rudie Neve, Rick van den Berg, Dominique Roest, Melvin Soudijn en Simone van der Zee
Vormgeving Het Lab - grafisch ontwerpers BNO, Arnhem
Foto omslag Goos van der Veen, Hollandse Hoogte
Druk Thieme MediaCenter, Rotterdam

Inhoud

Samenvatting

In dit deelrapport zijn de resultaten neergelegd van de actualisering van de kennis omtrent een aantal vormen van criminaliteit die in het NDB 2004 als (voorwaardelijke) dreiging zijn aangeduid. Voor elk thema is een beperkte gegevensverzameling uitgevoerd en is de literatuur die sinds het NDB 2004 is verschenen verwerkt. Daarnaast is voor enkele hoofdstukken (vooral het deel over geweld) gebruik gemaakt van informatie die is verzameld voor andere projecten in het kader van het NDB. Een groot deel van wat hier gerapporteerd wordt betreft dan ook 'zachte' informatie: het is veelal slechts gebaseerd op een beperkt aantal interviews met betrokkenen uit de opsporing. Voor het doen van harde en meer onderbouwde uitspraken zou meer diepgravend onderzoek op zijn plaats zijn. Hieronder worden de bevindingen uit de volgende hoofdstukken samengevat.

Ambtelijke corruptie

Dit thema is beperkt tot corruptie bij de opsporingsdiensten die zich bezighouden met de georganiseerde criminaliteit. Uit eerder onderzoek is gebleken dat de in Nederland actieve criminele samenwerkingsverbanden (csv's) zich vooral bezighouden met *transit crime*, waarbij het corrumperen van het bestuur als zodanig minder voor de hand ligt. Wel zijn csv's zich bewust dat ze onderwerp kunnen zijn van opsporingsonderzoek en om die reden is het van belang om zich zo goed mogelijk op de hoogte te stellen van de ontwikkelingen die daarin plaatsvinden. Uit journalistieke bronnen is wel het idee ontstaan dat criminelen grote bedragen beschikbaar houden voor het omkopen van opsporingsambtenaren, om hen zo te bewegen om informatie over op handen zijnde politie–acties te laten lekken of om een onderzoek op een dwaalspoor te zetten. Respondenten zijn het er echter over eens dat lekkende opsporingsambtenaren als regel maar bescheiden bedragen overhouden aan de schending van hun geheimhoudingsplicht. De meeste gevallen van lekken hebben niets te maken met omkoping, maar eerder met slordigheid en loslippigheid. Als iemand eenmaal op een verzoek is ingegaan, waarbij het veelal in eerste instantie om iets ogenschijnlijk 'onschuldigs' gaat, kan iemand in de greep komen van criminele contactpersonen. Een risicofactor die door meerdere respondenten is genoemd, is dat een te grote kring van collega's tot in detail op de hoogte is van de stand van zaken in opsporingsonderzoeken. Hierdoor wordt het ook heel moeilijk om vermoedens van lekken te verifiëren. Er wordt gepleit voor een vorm van georganiseerde controle in rechercheteams om het risico op het uitlekken van informatie uit politieonderzoeken te minimaliseren.

Als wordt geconstateerd dat een opsporingsambtenaar informatie heeft gelekt, dan blijkt het vaak zeer moeilijk om te bewijzen dat hier een tegenprestatie voor ontvangen is. Daarom worden interne onderzoeken op dit terrein vaak afgedaan als 'schending van het ambtgeheim', een lichter delict. Wat betreft de vervolging van corruptie en schending van het ambtsgeheid wordt opgemerkt dat het geregeld voorkomt dat de prioriteit wordt gegeven aan het verwijderen van de 'rotte appel' boven het rond krijgen van een intern dan wel strafrechtelijk onderzoek. Als iemand bijvoorbeeld verdacht wordt van lekken, maar ook drugs gebruikt, dan kan deze persoon op grond van drugsgebruik worden ontslagen, waarmee ook het integriteitsprobleem op korte termijn is opgelost.

De omvang van het lekken van informatie is niet met harde cijfers in beeld te brengen. Hoewel er een toename is in bepaalde categorieën interne onderzoeken die mogelijk gerelateerd zijn aan de georganiseerde criminaliteit, moet bedacht worden dat de laatste jaren veel capaciteit is ingezet in de bestrijding, bijvoorbeeld door de oprichting van Bureaus Integriteit. Naarmate er meer moeite wordt gedaan, worden er ook meer zaken gevonden. Het feit dat er bepaalde organisaties zijn waar geen enkel geval van corruptie wordt gemeld, geeft volgens respondenten te denken over de hoeveelheid energie die aan de bestrijding van normafwijkend gedrag wordt besteed in deze organisaties. Wel wordt gesteld dat corrupte contacten waarbij criminelen over cruciale informatie kunnen beschikken, zoals volgens het OM in een nog lopende zaak van een Amsterdamse rechercheur, maar zelden voorkomen.

Wat betreft de dreiging van corruptie in de nabije toekomst wordt alom verwacht dat deze dreiging zal blijven bestaan. Criminelen hebben belang bij opsporingsinformatie en zullen de kans om deze te verkrijgen, aangrijpen. Dit zal de komende jaren niet veranderen.

Corruptie bij grensoverschrijding

Soms zijn toezichthouders betrokken bij overschrijding van de landsgrenzen voor criminele doeleinden, zoals drugs– en mensensmokkel. Het betreft dan medewerkers van de douane en de marechaussee die tegen betaling mensen door laten gaan. Ook komt het voor dat toezichthouders daadwerkelijk betrokken zijn bij criminele activiteiten, zoals drugssmokkel. Voor zover bekend, beperkt de omvang hiervan zich tot enkele gevallen per jaar.

Corruptie bij mensen in het bedrijfsleven die betrokken zijn bij grensoverschrijding van mensen en goederen komt veelvuldiger voor. Bekend uit eerdere rapporten is de bagageafhandeling op Schiphol. Er zijn verschillende mogelijkheden om drugs en andere smokkelwaar over de grens te krijgen via de bagage. Al vele jaren lopen

er voortdurend onderzoeken naar drugssmokkel, waarbij telkens weer arrestaties worden verricht. De gepakte medewerkers worden echter snel weer vervangen door anderen. Ook bij andere bedrijvigheid komt corruptie voor. Criminelen proberen belang te verwerven in expeditiebedrijven die de grensformaliteiten voor opdrachtgevers afhandelen. Het komt ook voor dat dergelijke bedrijven worden gekocht door personen die verbonden zijn met criminele samenwerkingsverbanden. De positie in de markt en de expertise die binnen deze bedrijven voorhanden is, zijn aantrekkelijk voor criminelen. Dit geldt vooral voor een deel van de expeditiebedrijven, de douane–expediteurs die werken op basis van een vergunning van de douane. Vooral kleinere bedrijven zouden kwetsbaar zijn voor criminele bemoeienis. Door de invoering van de irisscan op Schiphol en het geheel afschaffen van ongecontroleerde poorten is het niet meer mogelijk voor medewerkers om hun pas uit te lenen of iemand mee te laten lopen. Mensensmokkel waarbij de gesmokkelden via de luchthaven het land binnenkomen is hierdoor sterk bemoeilijkt, wat zich uit in een vermindering van het aantal zaken dat zich heeft voorgedaan. Smokkel via Schiphol naar andere landen kan zo echter niet worden tegengegaan. In de haven speelt corruptie vooral een rol bij ladingdiefstal uit containers. Voor smokkel via containers is corruptie niet nodig. De verdergaande beveiliging van containerterminals zou kunnen leiden tot een toename van ladingdiefstal op andere plaatsen, zoals parkeerterreinen langs de snelwegen. Bij ladingdiefstal gaat het soms om kostbare, maar gemakkelijk af te zetten lading, zoals consumentenelectronica. Het komt echter ook voor dat lading wordt gestolen die alleen voor professionele afnemers interessant is, zoals grondstoffen of metalen. Dit duidt volgens respondenten op een verwevenheid van onder– en bovenwereld. Een blinde vlek wat betreft de betrokkenheid van personeel bij smokkelpraktijken is de sector van de koeriersbedrijven. De beschikbare cijfers laten niet toe om uitspraken te doen over stijging of daling in de omvang van corruptie bij grensoverschrijding. Naar verwachting van respondenten zal de druk op medewerkers vanuit de criminaliteit verder toenemen door voortgaande technische beveiliging. Tot op heden is het voor criminele elementen nog betrekkelijk eenvoudig om via het bedrijfsleven binnen te komen in de haven of op Schiphol en dat zal voorlopig wel zo blijven, is de verwachting.

Corruptie van vrijberoepsbeoefenaars

Hoewel harde cijfers ontbreken, lijkt het aantal vrijberoepsbeoefenaars en accountants dat zich in Nederland inlaat met criminaliteit beperkt. De mogelijke schade die een enkeling kan veroorzaken moet echter niet worden onderschat: enerzijds kan deze enkeling diverse zware criminelen bedienen en anderzijds kan het over zeer grote volumes gaan. Diverse respondenten hebben aangegeven dat het hier mogelijk om het ‘topje van de ijsberg’ gaat.

Als er sprake is van verwijtbaar betrokken dienstverleners gaat het in de meeste gevallen over het witwassen van crimineel geld dat afkomstig is uit de zware georganiseerde misdaad. De bijzondere expertise, in combinatie met diverse privileges, maakt de zich laakbaar gedragende dienstverlener zeer aantrekkelijk (en soms onontbeerlijk) voor criminele samenwerkingsverbanden. Naast betrokkenheid bij witwassen komen ook andere vormen van betrokkenheid bij criminaliteit voor. Zo fungeren advocaten soms tevens als liaison met de buitenwereld voor cliënten die in beperking vastgehouden worden en daardoor zelf geen contacten kunnen leggen.

Aan de kant van de opsporing is bijzondere expertise nodig om corrupte dienstverleners met succes aan te kunnen pakken. De opsporing heeft nog steeds een achterstand in te halen op het gebied van de financiële recherche.

Advocaten, notarissen en accountants spelen een belangrijke rol bij het binnendringen van crimineel geld en dus van criminelen in de 'bovenwereld'. De diensten van vrijberoepsbeoefenaars zullen naar verwachting in de nabije toekomst even onontbeerlijk blijven als zij de afgelopen jaren al waren. Tegelijk wordt een toename verwacht in de prioriteit die aan financieel opsporingsonderzoek wordt gegeven en wordt er geïnvesteerd in expertise.

Geweld, intimidatie en bedreiging door criminele samenwerkingsverbanden

Anders dan in de legale economie kunnen criminelen bij conflicten niet terugvallen op de rechter die een oordeel velt. Als bemiddeling door een persoon die beide partijen vertrouwen geen uitkomst biedt, zullen de krachtsverhoudingen bepalend zijn. Hierbij is geweld nooit ver weg. In dit rapport worden verschillende aspecten van geweldsgebruik door csv's behandeld. Geweld speelt een rol bij de binding en disciplinering van leden van de groep. Voorkomen moet worden dat mensen de groep ontrouw worden door bijvoorbeeld met de CIE te gaan praten of door de opbrengst van activiteiten in eigen zak te steken. Leden binden aan de groep kan door positieve prikkels, zoals beloningen. Er zijn dan ook csv's aangetroffen waar geweld binnen de groep weinig voorkomt. Bij veel csv's bestaan echter sancties voor leden die zich misdragen tegenover de leiders van de groep of op een andere manier te kort schieten. Er worden soms boetes opgelegd en daarnaast wordt dreiging met en toepassing van geweld gebruikt om betrokkenen in het gareel te houden.
Een bijzondere vorm van disciplinerend geweld is het geweld tegenover hulpkrachten. Zo werd melding gemaakt van bedreiging van mensen in de hennepteelt om ruimte ter beschikking te stellen, al wordt dit in de meeste gevallen gedaan voor financieel gewin.

Geweld tussen csv's komt veelvuldig voor, ook al geven veel criminelen er de voorkeur aan om met elkaar handel te drijven en vreedzaam samen te werken. Maar conflicten die ontstaan zullen uiteindelijk beslecht moeten worden. Daarbij komt dat geweld niet altijd op rationele wijze wordt toegepast: in de criminaliteit zijn personen met 'korte lontjes' oververtegenwoordigd. Geweld wordt toegepast bij conflicten over leveringen en betalingen, ripdeals en – minder frequent maar het komt voor – bij afpersing en het eisen van protectiegeld. In de drugshandel komt geweld voor om conflicten over betalingen of leveringen te beslechten, waarbij zwaar geweld, zoals mishandeling, ontvoering en moord niet wordt geschuwd. Het aantal liquidaties is de laatste jaren echter wel verminderd. Bij politiemensen in de zuidelijke regio's leeft het idee dat verschillende moorden van de laatste jaren te maken hebben met hennepteelt. Het intimideren en bedreigen van getuigen door csv's komt eveneens voor. Het risico wordt soms vergroot doordat advocaten informatie naar buiten brengen over wanneer getuigen gehoord worden. Getuigen hoeven niet concreet bedreigd te worden om zich bedreigd te voelen. Het gewelddadige imago van grotere criminelen heeft soms hetzelfde effect. Bedreiging van medewerkers van politie en justitie komt eveneens voor, maar niet veelvuldig. Concrete bedreigingen komen veelal van kleinere criminelen en worden soms impulsief geuit, waardoor het voor betrokkenen moeilijk is om in te schatten in hoeverre de bedreiging serieus genomen moet worden. Sommige medewerkers van justitie en politie worden beveiligd. Dit wordt meestal niet gedaan naar aanleiding van concrete bedreigingen, maar op basis van risicoanalyses door de politie.

Geweld bij autodiefstal

Bij geweld bij autodiefstal gaat het in dit rapport over *carjacking* en *homejacking*. In beide gevallen wordt het slachtoffer door middel van dreiging met geweld gedwongen de sleutel van de auto af te staan. Bij carjacking gebeurt dit op de weg, bij homejacking in huis. Beide fenomenen komen in zuivere vorm zeer weinig voor in Nederland. Wel komt het voor dat bij een woninginbraak ook de auto wordt gestolen, soms als extra buit en soms om te vluchten. Bij overvallen in huis waarbij ook de auto wordt buitgemaakt, komt wel excessief geweld voor. Dit delict komt enkele tientallen keren per jaar voor, volgens het Landelijk Overvallen en Ramkraken Systeem (LORS).

In het vorige NDB werd de verwachting uitgesproken dat de verbeteringen in de beveiliging van auto's tegen diefstal zou leiden tot meer car– en homejackings, maar tot nu toe is daar niets van gebleken. Enerzijds zijn criminelen in staat sommige beveiligingsmaatregelen te omzeilen, anderzijds zijn er nog veel auto's die minder goed beveiligd zijn. Voor de doelen waarvoor veel auto's worden gestolen, zoals kortstondig goedkoop vervoer, voor het plegen van andere

delicten en voor joyriding, zijn die net zo geschikt. Een andere reden om te verwachten dat er in Nederland meer carjackings zouden komen, was dat dit delict zich vrij vaak voordoet in buurland België. Ook al kunnen we het verschil tussen beide landen niet verklaren, er is op dit moment geen reden om te verwachten dat het aantal carjackings in Nederland zal toenemen.

ICT– piraterij

Gebleken is dat ICT–piraterij in Nederland op grote schaal voor komt. Hierbij dient onderscheid gemaakt te worden in hardcopy– en softcopypiraterij. De laatstgenoemde variant (het kopiëren en uitwisselen van louter digitale bestanden via sharingsites) speelt zich in Nederland op grote schaal af: er zijn enkele miljoenen gebruikers. De beheerders van websites die gelegenheid bieden voor het uitwisselen van illegale *content* verdienen niet direct geld aan de piraterij zelf, maar aan de verkoop van reclame op de sites. Gegeven de grote aantallen gebruikers kan er veel geld worden verdiend met softcopypiraterij. Niets wijst er op dat in Nederland de zware georganiseerde misdaad zich in deze markt heeft gemengd. Een reden zou kunnen zijn dat voor het faciliteren van dergelijke websites specifieke technische kennis noodzakelijk is. Daarnaast heeft nieuwe regelgeving (door voornamelijk rechterlijke uitspraken) er voor gezorgd dat men op succesvolle wijze, veelal op privaatrechtelijke grond, de Nederlandse beheerders van illegale sharingsites kan bestrijden.

In de hardcopypiraterij kan geld verdiend worden met de verkoop van auteursrechtelijk beschermde (veelal net uitgebrachte) dvd's en cd's. Uit het onderzoek is gebleken dat hier in Nederland nauwelijks sprake van is. Voor gebruikers is het aantrekkelijker om zelf thuis (met grote snelheid en goede kwaliteit) muziek en films te downloaden. De winstmarge per dvd/cd is ook vrij laag. Bovendien is er sprake van een behoorlijke inzet van opsporingsinstanties die zich in bepaalde gevallen kunnen bedienen van civielrechtelijke dwangmiddelen. Zo is de boete per cd aanzienlijk, wat een afschrikwekkend effect zou kunnen hebben. Ook in het geval van hardcopy's is van inmenging van criminele samenwerkingsverbanden niets gebleken. Wel is in het buitenland betrokkenheid van de georganiseerde criminaliteit gemeld. Zo zou de Camorra, de Napolitaanse maffia, zich met deze vorm van piraterij bezighouden. Deze illegale kopieën komen als regel niet in Nederland op de markt. Er is geen reden om te verwachten dat in Nederland criminele samenwerkingsverbanden zich op deze markt zullen begeven.

Phishing

In het NDB 2004 werd phishing gedefinieerd als een werkwijze waarbij gebruik wordt gemaakt van een misleidende website. Heden ten dage wordt deze

werkwijze beschouwd als een traditionele vorm van phishing. Andere type vistechnieken zijn gangbaar waarbij geen misleidende website meer nodig is. Onder phishing wordt daarom verstaan:

> het met behulp van digitale activiteiten wederrechtelijk toeeigenen en/of gebruiken van (delen van) de identiteitsgegevens van een internetgebruiker met het doel om een strafbaar feit te begaan waarvan de internetgebruiker het slachtoffer is.

De traditionele vormen van phishing komen steeds minder voor, onder andere doordat internetgebruikers zich steeds bewuster worden van het bestaan van misleidende e–mails. Tegenwoordig bestaat phishing vooral uit het besmetten van de computer met *malware*, waardoor er voor de gebruikers nauwelijks nog mogelijkheden zijn om dit te ontdekken.

Uit ons onderzoek komt naar voren dat het aantal aangiftes voor phishing, misleidende websites en meldingen bij internetbeveiligingsbedrijven de laatste jaren sterk is toegenomen. De groei van het internet en het aantal (financiële) diensten dat hierop aangeboden wordt, heeft een zekere aantrekkingskracht op criminelen. Gezien de complexiteit en het aantal te verrichten handelingen die nodig zijn voor het plegen van een phishingaanval, ligt het voor de hand te verwachten dat phishers zich organiseren en taken verdelen.

Uit de huidige opsporingsonderzoeken van het Team High Tech Crime blijkt dat de grote phishingaanvallen vaak gepleegd worden door Oost–Europese (oud) IT–studenten. Verwacht wordt dat de Oost–Europese betrokkenheid bij phishing nog zal toenemen. De expertise is aanwezig onder jonger IT–ers en voor sommigen van hen is het aanlokkelijk om op een snelle en gemakkelijke manier geld te verdienen. Momenteel zijn er nog geen phishingaanvallen gevonden die naar Azië leiden. Gezien de economische en technische ontwikkelingen in onder andere China is dit zeker een regio om in de toekomst rekening mee te houden.

De directe schade die door phishing wordt veroorzaakt lijkt tot nu toe mee te vallen. De indirecte schade waarmee de banken worden geconfronteerd is echter aanzienlijk. Aangezien verwacht wordt dat het aantal phishingaanvallen in de toekomst zal toenemen, kan verwacht worden dat zowel de directe als de indirecte schade zullen stijgen.

Het aantal breedbandaansluitingen neemt in de wereld nog steeds toe, waarbij Nederland een koppositie inneemt. Dit maakt het voor phishers makkelijker maakt om *botnets* te gebruiken of *malware* op computers te plaatsen.

Elektronisch winkelen en internetbankieren zullen nog meer gemeengoed worden. Ook deze criminaliteitsrelevante factoren die van belang zijn voor phishing zullen in de nabije toekomst niet veranderen.

Andere technische ontwikkelingen zoals het gebruik van *VoIP*, *wifi*, *smartphones* en *MMOG's* zullen in de toekomst steeds meer ingeburgerd raken en nieuwe technieken zullen hun intrede doen. De digitale wereld zal zich steeds verder uitbreiden waardoor nieuwe phishingtechnieken zullen worden ontwikkeld. Zo spraken verschillende respondenten de verwachting uit dat uiteindelijk de hele wereld met elkaar via internet verbonden zal zijn. Voor phishers die hier misbruik van willen maken biedt dit veel mogelijkheden. Duidelijk is echter dat phishing in de toekomst een niet te onderschatten vorm van criminaliteit zal zijn.

Bezit van ondernemingen

Voor de eerste versie van het Nationaal Dreigingsbeeld is in 2002 uitgebreid onderzoek gedaan naar criminele afscherming en verweving. Een van de indicatoren voor de verwevenheid van boven– en onderwereld was toen de zeggenschap die criminelen hadden over ondernemingen. Om te voorkomen dat criminele samenwerkingsverbanden zeggenschap hebben over ondernemingen en om ander misbruik van ondernemingen te voorkomen, heeft de overheid een aantal preventieve overheidsmaatregelen genomen:

Verklaring van geen bezwaar

Iedereen die in Nederland een besloten of naamloze vennootschap of societas europea (Europese NV) wil oprichten of de statuten van een opgericht vennootschap wil wijzigen, moet een verklaring van geen bezwaar (VVGB) bij de minister van Justitie aanvragen. Deze maatregel voldoet niet, omdat alles wat in de periode na de oprichting aan wijzigingen wordt doorgevoerd aan het zicht wordt onttrokken. Het ministerie van Justitie ontwikkelt daarom in het project 'Herziening Toezicht Rechtspersonen' (HTR) een nieuwe systematiek van toezicht op rechtspersonen. Hierbij wordt een permanente screening geïntroduceerd. Met deze permanente screening wordt beoogd het misbruik van rechtspersonen te kunnen signaleren en tegen te gaan.

Verklaring Omtrent Gedrag voor rechtspersonen (VOGrp)

Met deze VOGrp kunnen rechtspersonen hun integriteit tonen aan partners, bedrijven en overheden. De VOGrp is een verklaring van de minister van Justitie dat, voor het doel waarvoor de VOGrp is aangevraagd, hem niet is gebleken van bezwaren tegen de betreffende rechtspersoon.

Wet Bevordering Integriteitsbeoordelingen door het Openbaar Bestuur (Wet BIBOB)

De Wet BIBOB moet voorkomen dat de overheid, door het verlenen van vergunningen of het verstrekken van subsidies of het gunnen van overheidsopdrachten, onbedoeld criminele activiteiten faciliteert. Ten tijde van het NDB 2004 verkeerde de Wet BIBOB nog in de opstartfase en waren veel gemeenten nog bezig met het ontwikkelen van een BIBOB–beleid. Inmiddels hebben veel gemeenten een BIBOB–beleid vastgesteld. Tussen 2003 en 2006 heeft het bureau BIBOB in totaal 193 adviezen uitgebracht.

Bovengenoemde preventieve overheidsmaatregelen zijn erop gericht om misbruik van ondernemingen tegen te gaan. De vraag rijst in welke mate leden van criminele samenwerkingsverbanden toch in de gelegenheid zijn om ondernemingen voor criminele doeleinden te benutten. Bekeken is of de leden van de criminele samenwerkingsverbanden uit de EU–inventarisatie voor 2006 formeel betrokken waren bij ondernemingen. Van de 2273 personen uit de EU–inventarisatie stonden 577 personen in totaal 1516 maal ingeschreven bij de Kamer van Koophandel. Dit komt neer op 25,4 procent. In 2004 was dit 27,5 procent. Deze personen waren betrokken bij 1136 unieke ondernemingen. Net als in 2004 voeren de BV's de boventoon, gevolgd door de eenmanszaken en stichtingen. Deze ondernemingen zijn vooral in te delen bij de financiële instellingen, overige zakelijke dienstverlening en groothandels. Kijken we naar het aantal criminele samenwerkingsverbanden dat één of meer leden heeft dat actief is binnen een onderneming dan valt op dat bijna driekwart van de bij de politie bekende csv's leden heeft die ingeschreven staan bij de Kamer van Koophandel.

Dat leden van csv's ingeschreven zijn in het register van de Kamer van Koophandel toont nog niet aan dat ze de ondernemingen waarover ze zeggenschap hebben ook daadwerkelijk gebruiken bij het ontplooien van hun criminele activiteiten. Om hierover duidelijkheid te krijgen zou nader onderzoek verricht moeten worden.

Desinformatie als contrastrategie

Onder desinformatie wordt verstaan dat criminelen via de media of anderszins informatie in omloop brengen om de werkzaamheden van politie en justitie te ontregelen. Het kan hierbij gaan om beschuldigingen jegens personen die een belangrijke rol spelen in opsporingsonderzoeken, zoals officieren van justitie of teamleiders van de politie. Desinformatie kan een concreet onderzoek vertragen, maar kan er ook op gericht zijn om het vertrouwen in politie en justitie in bredere zin te ondermijnen. Hiertoe wordt valse informatie in omloop gebracht,

bijvoorbeeld over corruptie of het gebruik van 'verboden onderzoeksmethoden' door de politie. Door de beschikbaarheid van nieuwe media en 'kliklijnen', zoals Meld Misdaad Anoniem wordt het gemakkelijker dan voorheen om dergelijke informatie in omloop te brengen. In potentie is desinformatie mogelijk en schadelijk, maar concrete gevallen waarin een verband is met de georganiseerde criminaliteit zijn er zeer weinig.

Een recent geval waarbij een vals proces–verbaal aan de pers werd toegespeeld, laat zien dat zelfs in een dergelijk geval waarbij de vervalsing snel kon worden aangetoond, veel moeite moet worden gedaan om het beeld dat in de publiciteit is gecreëerd, weer te corrigeren. De meeste bekende gevallen hebben echter niets te maken met georganiseerde criminaliteit, maar worden uitgevoerd door rancuneuze individuen die bepaalde politiemensen een hak willen zetten. Bij beschuldigingen aan het adres van politiemensen kan er vaak niet aan worden ontkomen dat de Rijksrecherche een onderzoek instelt, waardoor de betreffende persoon op non–actief komt te staan. In het eerste NDB werd de verwachting uitgesproken dat journalisten zich meer direct tot criminelen zouden gaan wenden, nu de Orde van Advocaten de mogelijkheden om processtukken naar buiten te brengen aan banden gelegd heeft. Hier is tot nu toe echter niets van gebleken, mede omdat journalisten nog altijd vrij gemakkelijk procesinformatie kunnen krijgen via advocaten.

Naar verwachting zullen zich in de toekomst af en toe gevallen van desinformatie voordoen, maar of de georganiseerde criminaliteit vaker naar dit middel zal grijpen, is niet te zeggen. Goede en open communicatie vanuit de overheid zou er toe kunnen bijdragen dat de schadelijke gevolgen van desinformatie verminderen.

Documentvervalsing

Het begrip 'documenten' is hier gebruikt in beperkte zin. Het gaat om Nederlandse identiteitsdocumenten, met name paspoorten, rijbewijzen en verblijfsvergunningen. Het gebruik van valse of vervalste buitenlandse documenten en vervalsingen van andere documenten, zoals vrachtbrieven, valt dus buiten het kader van dit rapport.

Criminelen maken vaak gebruik van valse identiteitsdocumenten, niet alleen om te reizen, maar ook voor allerlei andere zaken die het criminele bedrijf faciliteren, zoals het huren van auto's, woningen en bedrijfsruimtes, het afsluiten van leningen en het inschrijven van bedrijven bij de Kamer van Koophandel. Er bestaan verschillende manieren om wederrechtelijk aan een Nederlands identiteits-document te komen. Het document kan geheel vals gekocht worden en er kan

een andere foto of houderpagina aan een echt document worden toegevoegd. Daarnaast bestaat de mogelijkheid om een echt document aan te vragen dat echter door een onbevoegde gebruikt zal gaan worden. De omvang van het probleem is uit de beschikbare gegevens niet goed op te maken en er is dus ook niet veel te zeggen over eventuele trends die zich daarin hebben voorgedaan.

De verwachting is dat de vraag naar valse en vervalste identiteitsdocumenten in de toekomst zeker niet zal afnemen. Mocht Nederland er in slagen het lang verwachte 'onvervalsbare' paspoort te ontwikkelen, dan is te verwachten dat criminelen zullen uitwijken naar paspoorten van andere landen die gemakkelijker na te maken zijn.

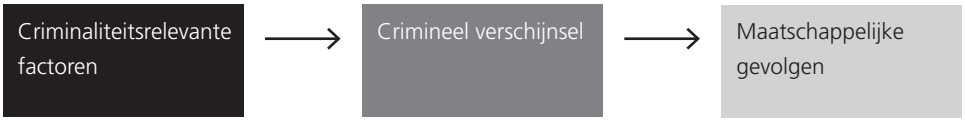
1 Inleiding

1.1 Het Nationaal dreigingsbeeld

Dit rapport is een verslag van een onderzoek voor het Nationaal dreigingsbeeld (NDB). Het NDB beoogt inzicht te verschaffen in de criminaliteit met een georganiseerd karakter waarmee Nederland heden ten dage kampt en in de nabije toekomst zal worden geconfronteerd.

In 2004 verscheen het eerste Nationaal dreigingsbeeld (DNRI, 2004a). Dit dreigingsbeeld was de eerste poging om de georganiseerde criminaliteit en haar dreigingen voor de Nederlandse samenleving in kaart te brengen sinds de Parlementaire Enquêtecommissie uit de jaren negentig. In 2006 is in opdracht van de Raad van Hoofdcommissarissen een vervolgstudie verschenen waarin nader werd ingegaan op enkele specifieke criminele verschijnselen die in het eerste NDB onderbelicht waren gebleven (DNRI, 2006). Door de politieministers is bepaald dat het Nationaal dreigingsbeeld vierjaarlijks moet worden vervaardigd. Reden waarom in 2008 het tweede NDB is vervaardigd.

Vanwege het toekomstgerichte karakter van het NDB wordt niet alleen de huidige stand van zaken van criminele verschijnselen onderzocht, maar gaat de aandacht ook uit naar maatschappelijke factoren die van invloed zijn (of kunnen zijn) op de criminele verschijnselen. Deze worden aangeduid als criminaliteitsrelevante factoren. De invloed op aard en omvang van de criminaliteit kan zowel bevorderend als remmend zijn. Bij remmende factoren kan mede worden gedacht aan inspanningen op het vlak van de criminaliteitsbeheersing, zoals de intensivering van controles bij de export van goederen naar het buitenland. Ook wordt aandacht besteed aan maatschappelijke gevolgen. Hiermee worden de schadelijke gevolgen bedoeld van de criminele verschijnselen in hun totaliteit voor de Nederlandse samenleving. De (veronderstelde) causale samenhangen tussen criminaliteitsrelevante factoren, criminele verschijnselen en maatschappelijke gevolgen kunnen als volgt schematisch worden weergegeven:



Het NDB wordt in opdracht van het College van procureurs–generaal samengesteld door de Dienst IPOL van het Korps landelijke politiediensten. Het wordt gebruikt om beleidsprioriteiten vast te stellen in de aanpak door politie en justitie van criminaliteit met een georganiseerd karakter op nationaal en regionaal besturingsniveau. Tevens beoogt het aanknopingspunten te bieden voor een bestuurlijke aanpak.

Het domein van criminaliteit met een georganiseerd karakter is breed. Het bevat de criminaliteit die haar beslag krijgt in de structurele samenwerking tussen personen, die wordt gepleegd met het oog op het gezamenlijk behalen van financieel of materieel gewin, en die ernstige gevolgen heeft voor de samenleving. 'Criminaliteit met een georganiseerd karakter' omvat zowel misdrijven die gerelateerd zijn aan illegale markten ('handelsmisdaad') als roofmisdrijven die worden gepleegd door meerdere plegers gezamenlijk ('banditisme'). Het kenmerk 'structurele samenwerking tussen personen' betekent niet alleen dat sprake is van (de intentie tot) herhaald plegen, maar ook van enige consistentie in de samenstelling van het samenwerkingsverband. Vanwege de gerichtheid op financieel of materieel gewin behoort ideologisch gemotiveerde criminaliteit niet tot het onderzoeksdomein.

Begin 2007 zijn in een voorstudie mogelijke onderwerpen voor nadere studie belicht. In overleg met de begeleidingscommissie van het NDB zijn binnen de Dienst IPOL zes deelprojecten gestart en inmiddels uitgevoerd. De onderwerpen die in deze deelprojecten centraal stonden, zijn:

- productie, handel en smokkel van cannabis;
- criminaliteit bij bodemsanering en grensoverschrijdende afvalstromen;
- fraudeconstructies;
- georganiseerde vermogenscriminaliteit;
- witwassen van wederrechtelijk verkregen vermogen;
- actualisering van dreigingen uit het eerste NDB.

De algemene vragen waarop in deze deelprojecten een antwoord moest worden geformuleerd, luidden telkens als volgt:

1 Hoe heeft de aard van het criminele verschijnsel zich ontwikkeld voor wat betreft de wijze waarop die criminaliteit wordt gepleegd?
2 Hoe heeft de omvang van het criminele verschijnsel zich ontwikkeld in termen van hoeveelheid van activiteit (frequentie, incidentie, prevalentie, schaalgrootte)?
3 Hoe heeft de aard van het criminele verschijnsel zich ontwikkeld voor wat betreft de kenmerken van personen en criminele samenwerkingsverbanden die van (betrokkenheid bij) het plegen daarvan worden verdacht?

4 Wat zijn de gevolgen van het criminele verschijnsel voor de Nederlandse samenleving?
5 Welke criminaliteitsrelevante factoren zijn in welke mate en op wat voor wijze van invloed op het criminele verschijnsel?
6 Wat zijn de verwachtingen over omvang, werkwijze, betrokken criminele samenwerkingsverbanden en maatschappelijke gevolgen van het criminele verschijnsel voor de komende jaren?

Bovenstaande vragen zijn niet alleen uitgangspunt geweest voor de deelrapporten van de Dienst IPOL, maar zijn ook richtinggevend geweest voor landelijke criminaliteitsbeeldanalyses op de aandachtsgebieden van de dienst Nationale Recherche als ook voor analyserapporten van regionale politiekorpsen over criminaliteit met een georganiseerd karakter. De bevindingen uit deze rapporten vormen het basismateriaal voor het eindrapport NDB 2008.

1.2 Deelproject Actualisering van dreigingen uit het NDB 2004

Voor het NDB 2008 worden een aantal deelrapporten gemaakt waarin een thema wordt uitgediept. Het onderhavige rapport wijkt af van de overige deelrapporten, omdat in dit rapport een aantal verschillende thema's onder de loep wordt genomen. Deze opzet vloeit voort uit de voorstudie die er op gericht was om keuzes te maken voor het NDB 2008. Van een aantal onderwerpen is toen besloten om daar geen aparte deelstudie aan te wijden, maar te volstaan met een actualisering. Deze criminele verschijnselen zijn al aan de orde geweest in het NDB 2004 en sommige zijn ook nog behandeld in de Vervolgstudie (DNRI, 2006a).

De in het NDB 2004 genoemde dreigingen en 'voorwaardelijke dreigingen' zijn als volgt geclusterd.

1 Corruptie
   a Ambtelijke corruptie;
   b Corruptie bij grensoverschrijding;
   c Corruptie van vrijberoepsbeoefenaars.

2 Geweld
   a Geweld binnen criminele samenwerkingsverbanden;
   b Geweld tussen criminele samenwerkingsverbanden;
   c Intimidatie en bedreiging van politie en justitie;
   d Intimidatie en bedreiging van verdachten en getuigen;
   e Geweld bij autodiefstal.

3 Misbruik van ICT
   a ICT–piraterij;
   b Phishing.

4 Werkwijzen van csv's
   a Misbruik van ondernemingen;
   b Desinformatie als contrastrategie;
   c Documentvervalsing.

1.3 Doel en globale vraagstelling

Het doel van dit deelproject is om de kennis over de criminele verschijnselen die in het NDB 2004 als (potentiële) dreiging worden gekwalificeerd, te actualiseren. Het NDB 2004 wordt dan ook als uitgangspunt genomen bij de domeinafbakening van de verschillende onderwerpen binnen dit project. Onder actualiseren verstaan we dat aangegeven wordt in welke mate zich nieuwe ontwikkelingen hebben voorgedaan sinds de laatste rapportage (2004 en in sommige gevallen 2006), en of die leiden tot een aanpassing van de verwachtingen die zich in de nabije toekomst op het betreffende terrein zouden kunnen gaan voordoen. De vraag in hoeverre deze actualisering tevens aanleiding zou kunnen geven tot een aanpassing van de kwalificatie als 'dreiging' en de strategische planning bij de bestrijding van de georganiseerde criminaliteit valt buiten het bestek van deze deelstudie. De resultaten van de deelstudies, waaronder de onderhavige, worden in een latere fase van het project NDB 2008 voor dat doel benut. De zes hoofdvragen van het NDB 2008 zullen in dit rapport per dreiging of thema van een antwoord worden voorzien.

1.4 Onderzoeksmethode

In het kader van de voorbereiding van het NDB 2008 is ten aanzien van de onderwerpen die in dit project aan de orde komen, besloten dat ze met een beperkte onderzoeksopzet en een 'relatief geringe inspanning' kunnen worden geactualiseerd. De vraagstelling is steeds: zijn er sinds de laatste rapportage nieuwe ontwikkelingen die een actualisering/update voor het betreffende onderwerp noodzakelijk maken? Op grond van literatuurstudie en gesprekken met experts is bezien welke nieuwe ontwikkelingen van belang kunnen zijn om bepaalde activiteiten van de georganiseerde criminaliteit in termen van 'dreiging' te kwalificeren. Hierbij moet worden aangetekend dat over sommige onderwerpen zeer weinig recent onderzoek te vinden is en dat

de rapportage in die gevallen alleen gebaseerd is op de 'zachte' informatie uit interviews met experts. De respondenten zijn vooral medewerkers van justitie, politie en andere opsporingsdiensten, zoals de douane en de Marechaussee.

2
Corruptie

Wij kennen in onze samenleving verschillende categorieën van functionarissen die beschikken over bijzondere bevoegdheden of die een bijzondere informatiepositie hebben die ze geacht worden aan te wenden in het algemeen belang. Zij kunnen er soms toe gebracht worden om hun invloed aan te wenden om beslissingen te nemen die niet in het algemeen belang zijn. Zo kan iemand met wie de functionaris een bijzondere relatie heeft, hem daartoe aanzetten. Ook kan het gebeuren dat iemand de functionaris in geld of in natura betaalt als tegenprestatie voor het genoten voordeel. Al sinds de oudheid komt het voor dat personen die bijzondere bevoegdheden hebben of over bijzondere informatie beschikken, daar misbruik van maken om bepaalde mensen te bevoordelen en daar een of andere tegenprestatie voor terugkrijgen. Van Hulten (2002) noemt voorbeelden uit verschillende historische perioden en uit de Bijbel waar ook al sprake is van omkoping van functionarissen. Dit zou al gauw tot de conclusie kunnen leiden dat corruptie iets 'van alle tijden' is, dat nu eenmaal bij de mens hoort. Corruptie vindt echter niet altijd en overal in dezelfde mate en op dezelfde manier plaats. Volgens de Corruption Perceptions Index[1] behoort Nederland tot de top 10 van 'minst corrupte' landen (Transparancy International, 2007). Niettemin komt corruptie ook in Nederland wel degelijk voor. In dit hoofdstuk gaan we in op corruptie waarbij de georganiseerde criminaliteit is betrokken. Het gaat hierbij met name om ambtelijke corruptie, (paragraaf 2.1), corruptie bij grensoverschrijding (paragraaf 2.2) en verwijtbare betrokkenheid van vrijberoepsbeoefenaars en andere financiële dienstverleners bij de georganiseerde criminaliteit (paragraaf 2.3).

2.1 Ambtelijke corruptie

2.1.1 Inleiding

Onder ambtelijke corruptie wordt verstaan dat misbruik wordt gemaakt van ambtelijke bevoegdheden om iets te doen of juist na te laten ten gunste van een derde partij, waardoor persoonlijk voordeel wordt behaald in de vorm van financiële of andersoortige gunsten. In het kader van deze studie wordt bij 'een derde partij' vooral gedacht aan vertegenwoordigers van criminele

[1] Deze index werd overigens recentelijk bekritiseerd, onder meer door Van Hulten (zie artikel van J. Dohmen in NRC, 26 sept. 2007).

samenwerkingsverbanden (csv's). In dit hoofdstuk zullen niet alle vormen van corruptie worden behandeld, maar met name corruptie bij politie en justitie.

Corruptie is een ernstige vorm van schending van de ambtelijke integriteit. Tot in de jaren 80 leefde het idee dat ambtelijke corruptie iets was van verre, exotische landen dat in Nederland niet voorkwam. Ambtelijke corruptie is in 1992 op de agenda gezet door de toenmalige minister Ien Dales in een toespraak voor de Vereniging Nederlandse Gemeenten. Deze toespraak is vooral bekend geworden door het volgende citaat: 'De overheid is wel of niet integer. Een beetje integer kan niet. En met de integriteit van de overheid valt of staat het bestuur.' De toespraak leidde aanvankelijk tot ophef en ook tot ontkenning bij verschillende betrokken instanties. Bij de politie heeft de discussie geleid tot het opzetten van een integriteitsbeleid waarmee wordt beoogd corrupt en ander niet–integer gedrag tegen te gaan. Er is een integriteitsstatuut opgesteld en er zijn bureaus interne onderzoeken (BIO's) en vergelijkbare instellingen opgericht bij de politieregio's en andere opsporingsdiensten. Wie bij deze diensten wil gaan werken, moet een uitgebreid veiligheidsonderzoek ondergaan (Adviescommissie Politie en Integriteit, 2000). De interne bureaus vormen een belangrijke bron voor het onderzoek dat voor dit rapport is verricht.

De belangrijkste recente studie op het gebied van corruptie is die van Huberts en Nelen (2005) die gericht is op het openbaar bestuur in brede zin. Volgens deze studie worden jaarlijks 130 interne en 50 strafrechtelijke onderzoeken naar corruptie in de overheidssector uitgevoerd. Hoewel dit al snel tot relativering van de omvang van corruptie in ons land zou kunnen leiden, waarschuwen de auteurs tegen al te veel zelfgenoegzaamheid. Zo blijkt dat in sommige sectoren in het geheel geen corruptieonderzoeken worden uitgevoerd, terwijl uit internationaal onderzoek blijkt dat er wel degelijk sprake is van kwetsbaarheid voor corruptie. Dit gold bijvoorbeeld voor de sectoren landbouw, natuurbeheer en milieu. Volgens de auteurs is het niet aannemelijk dat zich niets voordoet in die sectoren en lijkt het er meer op dat er onvoldoende serieus werk wordt gemaakt van onderzoek naar en bestrijding van corruptie. Zij stellen dat er vele vermoedens zijn van verbanden tussen corruptie en de georganiseerde misdaad. Naar aanleiding van de IRT–affaire werd bijvoorbeeld gewezen op het gevaar dat het bestuur zou worden gecorrumpeerd door de georganiseerde misdaad.
In Amsterdam leidde dit tot het opzetten van specifiek beleid, hoewel er van concrete bewijzen voor het bestaan van aan de georganiseerde misdaad gelieerde corruptie geen sprake was op dat moment. In Amsterdam zijn meer corruptiezaken aan het licht gekomen dan in andere gemeenten, maar betekent dat ook dat Amsterdam corrupter is?

De corruptieparadox

Huberts en Lasthuizen (2005) bevestigen de bevinding dat de corruptie in Nederland laag is in vergelijking met derdewereldlanden en ook met bijvoorbeeld Italië, maar dat neemt niet weg dat er een probleem is. Naarmate er meer aandacht is voor integriteit en corruptie, worden meer onderzoeken opgezet naar zaken die daar mee te maken hebben. Zo zijn er sinds het opzetten van het Bureau Integriteit bij de gemeente Amsterdam aanmerkelijk meer zaken aan het licht gekomen dan in andere gemeenten. Er wordt wel gesproken van een 'corruptieparadox'. Het aantal corruptiezaken dat aan het licht komt, zou niet zozeer een reflectie zijn van het niet–integer handelen, maar van de hoeveelheid energie die wordt vrijgemaakt om dit handelen boven water te krijgen. Dit is ook aangevoerd als argument om aan te tonen dat corruptie in Nederland nog wel meevalt, zoals min of meer is gesuggereerd door premier Balkenende in een brief aan de Tweede Kamer: bij ons zijn er een aantal corruptiezaken, maar dat komt juist omdat we de integriteit zo goed op orde hebben en er hard achteraan zitten (Kamerstukken II 2003–2004). Huberts en Lasthuizen wijzen er op dat een aanzienlijk deel van de overheidsinstanties geen enkel geval van corruptie heeft gerapporteerd, hetgeen volgens hen duidt op naïviteit en zelfs luiheid om het probleem aan de orde te stellen. Kortom, er zijn waarschijnlijk veel meer gevallen dan uit de cijfers blijkt. In welke mate corruptiegevallen verband houden met de georganiseerde criminaliteit is overigens een vraag die Huberts en Lasthuizen niet hebben gesteld en dus niet beantwoord.

Dark number

Naast het gegeven dat de aandacht voor corruptie en ander niet–integer handelen wisselend is, bestaat nog het probleem van het *dark number*: een groot deel van de corruptie blijft waarschijnlijk verborgen omdat alle betrokken partijen hierbij belang hebben. Als er al vermoedens ontstaan dan blijkt het een probleem om ambtelijke corruptie te bewijzen. Van Duyne (geciteerd door Van Hulten, 2006) heeft er in 1994 al op gewezen dat het (te) vaak gebeurt dat officieren van justitie een zaak tegen een ambtenaar aanhangig maken die uiteindelijk geseponeerd wordt of tot vrijspraak leidt, omdat het bewijs niet geleverd kan worden. Het bederf van de samenleving, de regering en de politiek grijpt intussen om zich heen, aldus Van Duyne. In dit verband wordt er op gewezen dat al sinds de zeventiger jaren politici door delen van de bevolking worden gezien als 'zakkenvullers' (Van Hulten, 2006). Elk corruptiegeval dat aan het licht komt zal dit gevoel versterken, waardoor het gezag van de overheid en het vertrouwen in de rechtsstaat wordt ondermijnd.

Criminele samenwerkingverbanden en corruptie

Volgens Van Duyne (1997) is het idee dat de georganiseerde misdaad zal proberen de overheid en opsporingsdiensten te corrumperen, overgenomen uit andere landen, zoals de VS en Italië. Misdaadondernemers die in Nederland actief zijn hebben er juist belang bij om zo weinig mogelijk contacten te hebben in de bovenwereld. Deze brengen immers aanzienlijke risico's voor ontdekking met zich mee, die veelal nauwelijks opwegen tegen het mogelijke voordeel dat er mee te behalen is (zie ook Kleemans, 2007). Een voorbeeld van corruptie waar de georganiseerde criminaliteit wel belang bij heeft, is het leggen van contacten met politiemensen om informatie over opsporingsonderzoeken te krijgen. Deze vorm van corruptie zal dan ook centraal staan in deze paragraaf.

Corruptie op de agenda

De houding van de overheid is (in elk geval ten dele) veranderd van zelfgenoegzaamheid ('corruptie komt bij ons vrijwel niet voor') naar actief optreden. Sinds kort is er veel aandacht voor integriteit het voorkómen van corruptie. Er zijn diverse instanties opgericht, zoals het Bureau Integriteitsbevordering Openbare Sector, de BIO's bij de politieregio's en de Bureaus Integriteit en Veiligheid bij de verschillende opsporingsdiensten. Dit heeft geleid tot een toename van het bewustzijn dat personen binnen de overheid risico lopen en ook tot een toename van het aantal zaken waarin integriteitsschending aan de orde is.

Afbakening

Volgens Nelen en Nieuwendijk (2003) zijn er vier verschijningsvormen van ambtelijke corruptie:

1 het lekken van politie–informatie naar criminelen;
2 het binnenbrengen van contrabande (drugs/alcohol) in penitentiaire inrichtingen;
3 het ten onrechte verlenen van een verblijfsvergunning;
4 de invoer van verdovende middelen op Schiphol.

In de deelstudie *Criminele afscherming en verweving* (DNRI, 2004b), die uitgevoerd werd in het kader van het NDB 2004, wordt gesteld dat corruptie van overheidsfunctionarissen in relatie tot georganiseerde criminaliteit zich vooral voordoet onder ambtenaren van politie, douane en marechaussee. Het gaat hierbij met name om het lekken van informatie naar criminelen waardoor onderzoeken worden gefrustreerd. Corruptie bij de politie wordt in deze paragraaf besproken, waarbij het lekken van politie–informatie naar criminelen centraal staat. Niet–integer handelen in de penitentiaire inrichtingen komt eveneens kort aan de orde. Aangezien in dit rapport de nadruk ligt op de

georganiseerde criminaliteit wordt het ten onrechte verlenen van een verblijfsvergunning hier niet behandeld. Betrokkenheid van ambtenaren bij grensoverschrijding, waaronder de invoer van verdovende middelen, komt in paragraaf 2.2 aan de orde.

Onderzoek voor deze actualisering

Voor het thema ambtelijke corruptie is de meest recente literatuur bestudeerd. Als indicatie voor de omvang van het probleem zijn de cijfers uit het Herkenningsdienstsysteem (HKS) over verdachten van omkoping opgevraagd. Ook is gekeken naar de jaarlijkse landelijke inventarisatie van criminele samenwerkingsverbanden die in samenwerking met Europol wordt gemaakt voor het Europese Dreigingsbeeld (OCTA). Bij de Rijksrecherche zijn dossiers ingezien van een aantal opsporingsonderzoeken naar corruptie waarbij de georganiseerde criminaliteit een rol speelt. Dit vooral ter illustratie, de opzet van het dossieronderzoek was te beperkt om op enige volledigheid te kunnen bogen. Maar vooral zijn interviews gehouden met mensen die uit hoofde van hun functie inzicht hebben in integriteit en veiligheid bij politie, douane, marechaussee en het gevangeniswezen. Een volledig overzicht van functies van de geïnterviewden is weergegeven in bijlage 1.

2.1.2 Aard

Hoe kan het gebeuren dat een politiemedewerker informatie over onderzoeken aan criminelen doorspeelt? En omgekeerd, hoe leggen criminelen contact met politiemensen die ze mogelijk zo ver kunnen krijgen om hand– en spandiensten te verlenen? Deze vragen zijn in de interviews aan de orde gesteld.

Uit krantenberichten doemt wel het beeld op dat criminelen met een grote zak geld op zoek gaan naar potentieel te corrumperen politiemensen. Deze worden vervolgens omgekocht om informatie te leveren of een opsporingsonderzoek op een dwaalspoor te zetten. Dit beeld wordt door de geïnterviewde experts naar het rijk der fabelen verwezen. Wel zijn criminelen altijd geïnteresseerd in contacten om aan relevante informatie te komen en ze zullen hiervan gebruikmaken als de gelegenheid zich aandient. Het is immers altijd goed om te weten waar de tegenstander mee bezig is. Dat neemt niet weg dat er wel degelijk expliciete pogingen vanuit de georganiseerde criminaliteit worden ondernomen om politiemensen als informatiebron te werven. Het is niet duidelijk hoe vaak een dergelijke poging bij leidinggevenden wordt gemeld. Uiteraard is al helemaal niet duidelijk hoe vaak het niet wordt gemeld en de betrokkene op het aanbod in gaat. De geïnterviewde experts zijn het er echter over eens dat de bedragen die

omgaan veelal betrekkelijk klein en soms ronduit gering zijn. Niet zelden gaat het om bedragen van enkele duizenden euro's waarvoor men zijn carrière op het spel zet. De verklaring hiervoor is dat er andere belangen in het spel zijn, zoals het investeren in familie, vriendschap of soms de liefde.

Allereerst werd opgemerkt dat het bewust lekken van informatie niet vaak voorkomt. Volgens respondenten gebeurt dat in de meeste gevallen door toeval, naïviteit of onvoorzichtigheid. Een recent voorbeeld is dat van een rechercheur die thuis vertelt dat een zaak gaat 'klappen', ofwel dat er huiszoekingen en arrestaties gepland zijn, waarbij hij de plaatsnaam noemt waar dit gaat gebeuren. Zijn partner bespreekt dit met een vriendin in een openbare locatie, in dit geval de sauna, en daar is bij toeval ook de vriendin van een van de verdachten aanwezig. Die belt met haar mobiele telefoon met als resultaat dat er geen verdachten worden aangetroffen. Ook het bewijsmateriaal is weg en de zaak is stuk. Verschillende geïnterviewden klaagden ook dat van veel zaken een te groot aantal mensen op de hoogte is zonder dat zij zelf een rol van betekenis hebben. Dit vergroot de kans op het onbewust of bewust naar buiten brengen van informatie aanmerkelijk, terwijl het achterhalen van het lek juist wordt bemoeilijkt.

Dat neemt niet weg dat er ook gevallen zijn waarbij wel degelijk sprake is van bewuste schending van het ambtsgeheim. Zoals hiervoor al uiteengezet is, is pas sprake van corruptie als er ook een tegenprestatie komt van de kant van degene die informatie ontvangt. Volgens respondenten bij interne onderzoeksafdelingen is er veelal een bestaande relatie (soms indirect) met criminelen. Het patroon dat in een groot deel van de gevallen wordt aangetroffen, is dat iemand wordt verleid om een klein stukje informatie te leveren, bijvoorbeeld op wiens naam een bepaald kenteken staat. Vervolgens komen ze langzaam maar zeker in de greep van het criminele contact. Het is ook voorgekomen dat mensen steeds verder afglijden tot en met het daadwerkelijk deelnemen aan criminele activiteiten.

Een contact kan ontstaan door een bepaalde vorm van nabijheid, zoals in het geval van een Amsterdamse rechercheur die opgroeide met verschillende bekende figuren uit de 'Hollandse netwerken'. De loyaliteit naar de oude buurtgenoten kan de loyaliteit naar de politieorganisatie gaan overstijgen. Een dergelijk risico bestaat ook bij allochtone politiemedewerkers. Bij overmatige loyaliteit naar familie en naar de etnische groep neem de kans op corruptie toe.

Er zijn politiemensen die in hun vrije tijd op plaatsen komen waar ook criminelen komen, zoals een café of een sportschool. Het komt ook voor dat collega's zich aangetrokken voelen tot (grote) criminelen en plaatsen waar deze komen.

Als vervolgens bekend wordt dat zich in de kring van de sportschool of het café politiemedewerkers bevinden, dan vormt dit een mogelijke ingang voor criminelen voor het corrumperen van deze medewerkers. Loslippigheid of zelfs grootspraak over het werk bij de politie kan het risico op corrumperende contacten verder vergroten.

Er bestaan ook ten opzichte van het geschetste patroon atypische gevallen. Onlangs werd een vrouwelijke politiemedewerker in eerste aanleg veroordeeld wegens het lekken van opsporingsinformatie, waarbij het sterke vermoeden bestaat dat ze de informatie op eigen initiatief te koop aanbood aan criminelen. De vrouw opereerde samen met een vriendin, die al eerder legale handelswaar te koop aanbood op een plaats waar ook vraag bleek te bestaan naar opsporingsinformatie.

Infiltratie?

Naast het al dan niet tegen betaling verkrijgen van informatie van politiemensen is het in theorie mogelijk dat criminelen iemand uit hun netwerk in de opsporingsdiensten laten infiltreren met de bedoeling om een informatiepositie te verkrijgen dan wel om anderszins zand in de machine te strooien. Hoewel het door geen van de respondenten geheel wordt uitgesloten, wordt het onwaarschijnlijk geacht dat dit zich op enige schaal voordoet. De reden hiervoor is dat infiltratie erg omslachtig is en veel tijd kost, terwijl criminele samenwerkingsverbanden veel efficiëntere manieren tot hun beschikking hebben om aan informatie te komen.

Corruptie versus schending van het ambtsgeheim

Het is niet altijd zeker dat tegenover het leveren van informatie een tegenprestatie staat. En als daar al sprake van is, hoeft dat nog geen directe tegenprestatie te zijn. Het kan ook gaan om een investering in de relatie zodat er op enig moment in de toekomst een wederdienst te verwachten is.
Het bestaan van een tegenprestatie is bijzonder moeilijk te bewijzen zo lang de betrokkenen er het zwijgen toe doen en er geen administratieve sporen van de transactie zijn nagelaten. Hierbij speelt ook een rol dat pas ‘getapt’ mag worden bij een redelijk vermoeden van schuld aan het aannemen van een tegenprestatie. Van de onderzoeken die van start gaan onder de noemer ‘corruptie’ (art 363 Sr) eindigt dan ook uiteindelijk een groot deel als ‘schending van het ambtsgeheim’ (art 272 Sr).

Respondenten stellen ook dat corruptie weinig aan het licht komt, omdat de informatiesystemen van de Nederlandse opsporingsdiensten onvoldoende op elkaar afgestemd zijn. Indicaties dat er iets aan de hand is, zouden te vaak

ergens 'blijven hangen' zonder dat er daadwerkelijk iets mee wordt gedaan. Het zou ook voorkomen dat tijdens een onderzoek een (mogelijk) lek wordt geconstateerd, maar dat hierop niet wordt gerechercheerd, bijvoorbeeld wegens een gebrek aan capaciteit. Uit de database met verdachten in verband met criminele samenwerkingsverbanden blijkt in 25 gevallen sprake te zijn van (soms vage) vermoedens van lekken van opsporingsinformatie, waarbij soms expliciet wordt vermeld dat met dit vermoeden niets is gedaan.

De informatiemakelaar

In twee recente zaken die aanzienlijke publiciteit hebben opgeleverd is sprake van 'informatiemakelaars'. Ex–politiemensen zijn contact blijven houden met vroegere collega's en zouden er in geslaagd zijn om informatie te krijgen en die tegen betaling door te geven aan criminelen. De informatiemakelaar speelt dus de rol van intermediair tussen criminelen en politiemensen. De laatstgenoemden hoeven zelf geen direct contact met elkaar te hebben. Beide zaken zijn nog in behandeling.

Corruptie in justitiële inrichtingen

Het Gedetineerden Recherche Informatie Punt (GRIP) van de Dienst IPOL heeft informatie gegeven over integriteitsschendingen in justitiële inrichtingen. Het GRIP werkt samen met het bureau Integriteit en Veiligheid van de Dienst Justitiële Inrichtingen (DJI). Het verzorgt veiligheidsonderzoeken voor DJI–personeel en is het centrale punt voor informatie over gedetineerden. Het GRIP controleert vooral of nieuw aan te nemen personeel voorkomt in HKS.

Bij integriteitsschendingen in inrichtingen gaat het veelal om betrokkenheid bij het binnensmokkelen van contrabande, zoals drugs en mobiele telefoons. Een andere belangrijke categorie is het verstrekken van informatie aan gedetineerden of hun contacten, waardoor zaken soms gefrustreerd kunnen worden. Ook komen intieme contacten voor, waarbij bijvoorbeeld pakketten worden doorgelaten in ruil voor seks. Medewerkers spelen soms de rol van liaison tussen een gedetineerde en diens partner of familie die informatie doorspeelt. Een medewerkster is ontslagen nadat een verdachte van een liquidatie verklaard had dat zij een rol gespeeld had bij het leggen van contacten tussen hem en zijn opdrachtgever.

Volgens een medewerker van het GRIP gaan de grotere criminelen vrijwel altijd in de gevangenis door met hun criminele activiteiten. Hiervoor hebben zij een zekere bewegingsvrijheid nodig die zij krijgen via gunsten van het personeel. Deze categorie gedetineerden heeft er dus veel belang bij om DJI–medewerkers te corrumperen.

De ‘topcriminelen’ kunnen een machtspositie opbouwen door de middelen waarover zij beschikken. Het komt voor dat gedetineerden hele afdelingen fêteren. Zo heeft iemand voor de hele afdeling schoenen laten aanrukken. Personeel kan in de verleiding komen hierin mee te delen. Een indicatie dat een medewerker afglijdt, kan bijvoorbeeld zijn dat hij opvallend weinig opmerkingen in de verslagen noteert. Het komt voor dat directeuren dergelijke signalen lang ‘onder de pet houden’ en pas in een heel laat stadium een onderzoek laten instellen. Er wordt een nieuw integriteitshandboek ontwikkeld met concrete richtlijnen voor deze problematiek.

Medewerkers van justitiële instellingen zijn kwetsbaar omdat ze vaak laag opgeleid zijn en weinig verdienen. Ze kunnen beïnvloed worden door de soms sociaal zeer vaardige gedetineerden, die bovendien als welgesteld te boek staan. Wanneer een gedetineerde vermoedt dat een medewerker financiële problemen heeft, kan hij hem onder druk zetten. Ook als een medewerker in dezelfde buurt woont als (de familie van) de gedetineerde loopt hij meer risico om onder criminele invloed te komen. Vooral de ‘grotere’ of ‘topcriminelen’ hebben talent om mensen een bepaalde richting op te sturen. Zo runnen ze ook hun eigen organisaties. Een ander risicofactor is dat veel medewerkers van justitiële inrichtingen bijbanen hebben, zoals portier in horecagelegenheden, waar ze in contact kunnen komen met criminelen. Hierbij kunnen ze soms zeer vriendelijk behandeld worden door criminelen, die daar wel weer iets voor terugwillen als de gelegenheid zich voordoet. De controle op bijbanen ontbreekt en volgens de respondent wordt er niet veel gedaan met bekende gevallen van medewerkers die bijbanen hebben in een omgeving waar ook criminelen komen.

2.1.3 Omvang

Het bleek in eerdere rapportages moeilijk een goed beeld te krijgen van de materie, omdat er slecht wordt geregistreerd. Gevallen van corruptie waarbij de georganiseerde criminaliteit betrokken is als corrumperende partij, zijn moeilijk te identificeren. Enerzijds lijkt het hierdoor mee te vallen, anderzijds zou er sprake kunnen zijn van een aanzienlijk *dark number*.

Sinds het eerste NDB is er enige vooruitgang geboekt op het gebied van registratie. Sinds 2004 (na een *pilot* in 2003) wordt een database bijgehouden van integriteitsschendingen binnen de politie, de RIO (Registratie Interne Onderzoeken). Het verslag voor 2006 meldt een totaal van 1393 onderzoeken, waarbij 1495 personen betrokken waren en 1514 delicten. Sinds 1999 is dit aantal steeds gestegen, al is de stijging in 2006 (8%) minder groot dan in 2005 (20%). In 180 gevallen werd een strafbaar feit geconstateerd en in 507 gevallen

plichtsverzuim. 113 personen werden ontslagen, 64 personen werden voorwaardelijk ontslagen en 42 mensen namen zelf ontslag. De RIO houdt helaas geen aparte registratie bij van zaken die samenhangen met georganiseerde criminaliteit, maar er zijn wel een aantal categorieën die hierop kunnen duiden. Dit betreft met name 'misbruik van de positie'. Dit betreft 258 van de 1514 delicten voor 2006, ofwel zo'n 17 procent. In 53 gevallen ging het om lekken van informatie naar criminelen en in tien gevallen om omkoping. Zoals eerder aan de orde kwam, is omkoping moeilijk te bewijzen. Binnen de 481 gevallen van 'rechtspositionele' integriteitsschendingen ging het in 61 gevallen om 'ongewenste contacten'. Om vast te stellen in welke mate er georganiseerde criminaliteit in het spel is, moet nader onderzoek gedaan worden.

De verdeling van alle integriteitsschendingen naar sekse en executief/niet–executief komt overeen met de verdeling in de korpsen als geheel. Een relatie tussen werkervaring en integriteitsincidenten is wel geconstateerd: mensen die tussen vijf en tien jaar in dienst zijn, blijken het meest kwetsbaar. Een vergelijking met de totale populatie is op dit punt moeilijk te realiseren, omdat het rapport *Kerngegevens Nederlandse Politie* geen informatie over het aantal dienstjaren van de medewerkers bevat (ministerie van BZK, 2007).

Onder medewerkers van de DJI worden per jaar ongeveer 250 interne onderzoeken verricht, waarbij ongeveer in de helft van de gevallen het GRIP wordt ingeschakeld. Het GRIP maakt per jaar zo'n 1800 dreigingsinschattingen op basis van risicoprofielen van gedetineerden. Zo'n 200 à 300 staan er steeds op een lijst van zware criminelen met een hoog risicoprofiel.

Bij de Rijksrecherche werden in 2006 in totaal 345 zaken aangemeld, waarvan er 120 'Rijksrecherchewaardig' werden bevonden en in behandeling zijn genomen. In 46 gevallen betrof het corruptiezaken, tegen 14 in 2005. De contactpersonen bij de Rijksrecherche verklaren dit verschil door een andere wijze van registratie, capaciteitsvergroting en een andere definiëring. Zij benadrukken ook dat de omvang van corruptie in Nederland een *dark number* is. Het komt waarschijnlijk vaker voor dan er bekend is. Vaak worden zaken die begonnen als corruptie uiteindelijk weggeschreven als schending van het ambtsgeheim, omdat de voor corruptie vereiste tegenprestatie moeilijk te bewijzen is. In de voor dit onderzoek ingeziene dossiers bleek inderdaad dat de betrokkenen in verschillende gevallen uiteindelijk op grond van een ander delict (zoals druggebruik) uit de politierangen werden verwijderd. Verschillende respondenten stellen ook dat dit op een bewust gekozen tactiek berust: de prioriteit ligt bij het verwijderen van de betrokkene, de 'rotte appel in de mand'. Het daadwerkelijk aantonen en bestraffen van corruptie komt op de tweede plaats.

Onlangs zijn enkele grotere zaken aan de orde gekomen, die nog onder de rechter zijn. Voor dit onderzoek zijn alleen afgesloten dossiers ingezien, maar tijdens de meeste interviews is wel over deze lopende onderzoeken gesproken. De informatie die daarin aan de orde kwam, komt grosso modo overeen met wat bekend is uit openbare bronnen. Criminelen beschikken slechts in een enkel geval over bronnen waar werkelijk belangrijke informatie te halen valt. Bij detentie gaan die over naar degene die de opengevallen plaats in het criminele milieu overneemt. Volgens sommige respondenten is dit soort onderlinge samenwerking typisch voor de 'Hollandse netwerken'. Hieruit blijkt dat criminelen zuinig zijn op hun bronnen, wat er op zou kunnen duiden dat dergelijke goede bronnen bij de politie slechts sporadisch voorhanden zijn. Anders gezegd: corruptie van ernstig kaliber komt niet vaak voor. Corrupte politiemensen worden door toevalligheden ontdekt, wat erop zou kunnen duiden dat ook op dit gebied een *dark number* bestaat. Zo kwam een verdachte 'informatiemakelaar' en ex–politiemedewerker in beeld, omdat hij in een auto reed die gerelateerd was aan een onderzoek naar verduistering van dure leaseauto's.

De meeste geïnterviewden zijn ervan overtuigd dat er meer corruptie aan het licht zou komen als er meer geïnvesteerd zou worden in de opsporing ervan. Soms zijn er vage vermoedens van 'lekken' wanneer invallen en pogingen tot arrestatie mislukken. De verdachten zouden dan tevoren op de hoogte gebracht zijn. Deze vermoedens, die veelal niet nader worden onderzocht, zouden afgedaan kunnen worden als rationalisaties van politiemensen die hun tegenslagen proberen te verklaren. Volgens sommige respondenten doen zich in opsporingsonderzoeken soms daadwerkelijk zaken voor die alleen maar verklaard kunnen worden door lekken, bijvoorbeeld als bij criminelen stukken uit een opsporingsonderzoek worden aangetroffen, terwijl er nog geen proces begonnen is. Dergelijke stukken kunnen dan niet afkomstig zijn van de advocaat en moeten dus wel van de politie komen, zo wordt geredeneerd. Ook dan wordt er niet altijd een onderzoek naar het lekken verricht. Reden is dat het vaak moeilijk te achterhalen is wie precies heeft gelekt. Verschillende respondenten wijzen erop dat vaak een grote kring van collega's op de hoogte is van de *ins* en *outs* van een lopend onderzoek. Mensen praten nu eenmaal graag over wat gezien wordt als de meer spannende aspecten van het werk. Ook binnen het *old boys network* waarin vaak ex–collega's voorkomen, is men soms in detail op de hoogte van bepaalde onderzoeken. Er wordt dan ook voor gepleit om in rechercheteams een vorm van controle te organiseren om te voorkomen dat te veel mensen op de hoogte zijn. Immers hoe minder mensen weet van het onderzoek, hoe kleiner de kans op lekken. Tot slot besteden we kort aandacht aan de gegevens van het herkenningsdienstsysteem (HKS), waarin alle aangiften

en verdachten worden geregistreerd. (Voor een nadere toelichting zie bijlage 5 van de LCK 2005: DNRI, 2006b).

HKS biedt geen aanknopingspunten om georganiseerde criminele groeperingen af te zonderen van de overige criminaliteit. Het bevat basale gegevens en geen inhoudelijke informatie over de zaken. Niettemin loont het de moeite om tabel 2.1 kort te bespreken. Hoewel het niet echt een trend genoemd kan worden, blijken er stijgingen in de HKS–gegevens wat betreft 'omkoping ambtenaar', 'aannemen steekpenningen' en 'schending van het ambtsgeheim'. Wellicht speelt de eerder besproken 'corruptieparadox' hier een rol. De laatste jaren is er meer aandacht voor corruptie, wat zou kunnen leiden tot een groter aantal zaken bij politiemensen en andere ambtenaren. Hieruit zou volgen dat dit niet zozeer duidt op een toename in de feitelijke delicten. Het beeld dat naar voren komt over de omvang van corruptie is niet anders dan bij vorige rondes van het Nationaal dreigingsbeeld: corruptie bestaat en zo nu en dan komen er ook gevallen aan het licht. Hoe groot het *dark number* is, blijft een open vraag. Naarmate er meer moeite wordt gedaan om corruptie en integriteitsschendingen in het algemeen op te sporen, wordt er meer gevonden. Echt ernstige gevallen lijken maar zelden voor te komen, maar ze kunnen wel aanzienlijke schade aanrichten voor lopende opsporingsonderzoeken.

Tabel 2.1

Aantal verdachten van enkele delicten naar jaar												
Soort	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	Totaal
Omkopen van ambtenaar	8	11	9	12	14	14	13	27	16	31	16	171
Omkopen van rechter	0	1	1	0	1	0	0	0	0	0	0	3
Aannemen steekpenningen	2	19	4	7	8	0	10	16	6	27	8	107
Schending ambtsgeheim	5	12	8	7	7	5	5	18	12	16	15	110
Omkoping anderen	3	1	3	8	7	1	0	1	2	5	10	41
Schending briefgeheim	4	1	4	11	0	2	3	5	2	12	6	50
Totaal	**22**	**45**	**29**	**45**	**37**	**22**	**31**	**67**	**38**	**91**	**55**	**482**

Bron: HKS

2.1.4 Betrokken personen en groeperingen

Veel kleine en grote criminelen zullen belang stellen in informatie over de tegenstander. De geïnterviewden nemen aan dat alleen criminelen met een zekere structuur en continuïteit in hun activiteiten corrupte contacten met een meer dan incidenteel karakter ontwikkelen. Ook dan geldt dat het aangaan van contacten met de 'tegenpartij' een risico inhoudt waar belangrijke voordelen tegenover moeten staan. Voor groeperingen die zich vooral bezighouden met *transit crime*, zoals drugshandel, lijkt het vooral zaak om zo weinig mogelijk in het oog te lopen. Naarmate meer mensen betrokken zijn, wordt de kans op ongewenste belangstelling van de kant van politie en justitie immers groter.

Gecorrumpeerde opsporingsambtenaren komen vaker voor in de lagere rangen dan in de hogere. Hiervoor worden verschillende speculatieve verklaringen geopperd. Zo zou de financiële prikkel om wat bij te verdienen, bijvoorbeeld door het tegen betaling lekken van opsporingsinformatie, groter zijn bij mensen met een laag inkomen. Wat dit betreft is ook opgemerkt dat mensen in de opsporing relatief weinig verdienen en daardoor onder financiële druk kunnen komen te staan. Ook kan meespelen dat het risico van een verwoeste carrière bij lagere rangen een kleinere rol speelt. De recent bekend geworden zaken waarbij

ervaren rechercheurs betrokken zijn, worden vanuit dit oogpunt als uitzonderlijk gezien. De meest basale verklaring is dat mensen in lagere rangen vaker in integriteitszaken voorkomen omdat er nu eenmaal meer van zijn. Ook is wel opgemerkt dat bij mensen in de hogere rangen de kans op ontdekking kleiner is, omdat ze zich waarschijnlijk effectiever kunnen afschermen en bovendien soms zeggenschap hebben over het instellen van een onderzoek. Mogelijk zou een nadere analyse van concrete zaken meer uitsluitsel kunnen geven.

Medewerkers van de Rijksrecherche wijzen het vanuit de politiek geopperde idee om de aandacht vooral op de hogergeplaatsten te richten van de hand. Volgens hen zijn leidinggevenden juist minder interessant, omdat ze niet in detail op de hoogte zijn van de lopende onderzoeken. Een infodeskmedewerker die toegang heeft tot alle systemen, is aanmerkelijk interessanter. Mensen op zeer gevoelige functies, zoals medewerkers van observatieteams, zijn weliswaar het meest interessant vanuit het gezichtspunt van de criminelen, maar in dergelijke functies is ook sprake van een grote mate van sociale controle.

Voor sommige gevallen van corruptie en integriteitsschending speelt een rol dat de loyaliteit naar de organisatie niet opweegt tegen die naar de buurt of de etnische groep. Dit is gezegd over politiemensen die opgroeiden met buurtgenoten die later crimineel werden. Ook voor etnische minderheden is deze verklaring geopperd en er is in de interviews een parallel getrokken met de buurt. In een aantal gevallen speelde een liefdesrelatie een rol. Het ging hierbij vrijwel altijd om vrouwelijke medewerkers.

2.1.5 Gevolgen voor de Nederlandse samenleving

Ongeacht de omvang van corruptie, kan een enkel geval zeer grote schade aanrichten. Concrete opsporingsonderzoeken worden geschaad, maar ook het vertrouwen in politie en justitie kan worden aangetast. Dit is immers juist gebaseerd op het idee dat de medewerkers van het OM en politie integer zijn, alleen verantwoording afleggen aan het bevoegd gezag en het algemeen belang dienen. Aantasting van het vertrouwen gebeurt niet alleen door het lekken van vertrouwelijke informatie, maar vooral ook door de ophef die hierover ontstaat in de media.

2.1.6 Criminaliteitsrelevante factoren

Factoren die corruptie kunnen bevorderen, hebben vooral met het politiewerk zelf te maken. Volgens verschillende respondenten wordt er in het algemeen slecht omgegaan met informatiebeveiliging. Enerzijds door de (soms) gebrekkige

systemen, anderzijds heeft het te maken met de houding van medewerkers die met de vertrouwelijke, beveiligde informatie om moeten gaan. Zij zijn soms naïef en zich onvoldoende bewust van de gevaren. Door loslippigheid richting (oud) collega's doet een verhaal verrassend snel de ronde. Respondenten zijn van mening dat het moeilijk is om informatie in een beperkte kring te houden. Het *old boys network* vormt in meerdere zaken de basis voor het lekken van vertrouwelijke informatie.

Naarmate opsporingsambtenaren dichter bij de criminaliteit komen te staan, kunnen deze factoren een grotere rol gaan spelen en zullen de risico's toenemen. Zo staan wijkagenten dichtbij het publiek en beschikken over een uitgebreid netwerk waarin ook personen kunnen voorkomen die contacten hebben met criminelen. Daardoor zijn dit soort medewerkers meer ontvankelijk voor corruptie dan een collega die administratieve werkzaamheden op een bureau verricht. Sommige politiemensen lopen door de aard van hun werk meer gevaar dan anderen om af te glijden naar corruptie. Een voorbeeld hiervan is het verhoor van bepaalde grote criminelen. In de verhoorkamer waar rechercheurs en criminelen vaak en langdurig in elkaars gezelschap verkeren, ontstaat soms een band. Politiemensen gaan soms opkijken tegen deze verdachten en ook speelt een rol dat het indruk maakt als zij contact hebben met dergelijke figuren. Er gaat een bepaalde fascinatie van uit. Momenteel worden verhoormethoden ontwikkeld om politiemensen te wapenen tegen dergelijke druk door het bewaren van de professionele distantie.

Ook politiemensen die betrokken zijn bij Pseudokoop–Infiltratie–Teams (PIT–teams) lopen extra risico, omdat ze 'erg dicht tegen de criminaliteit aan zitten'. Toch komt het niet vaak voor dat zich in dit soort teams corruptiezaken voordoen, omdat juist daar sprake is van een saamhorigheidsgevoel en een sociale controle die nog sterker is dan elders binnen de politie.

Onder bepaalde omstandigheden is het risico aanwezig dat cynisme ontstaat in de richting van de organisatie, waardoor de loyaliteit wordt ondermijnd en de kans op integriteitsschendingen toeneemt. Dit risico is groter bij politiemensen die al langer in dienst zijn en bij hen die te eentonig en soms ook slecht betaald werk doen, zoals bijvoorbeeld bepaalde bewakingstaken. Dit kan uiteindelijk de arbeidssatisfactie negatief beïnvloeden, waardoor de loyaliteit kan afnemen. Als iemand slecht verdient en wordt gepasseerd voor een promotie, dan zou dit bij kunnen dragen aan de afbreukrisico's.

Een risicofactor waar door respondenten op werd gewezen is het (nieuwe) beleid waar de Nederlandse politie mee te maken heeft: hoog opgeleide

zij–instromers moeten ingewerkt worden door oudere collega's. Met het binnenhalen van mensen met een hoog opleidingsniveau wordt beoogd om het recherchevak vooruit te brengen. Het zittende oudere personeel kan dit echter ook aanvoelen als een teken dat bij de politieleiding het idee leeft dat zij in het verleden onder de maat gepresteerd hebben. Frustraties en ook disloyaal gedrag zijn dan niet uit te sluiten. De 'generatiekloof' binnen de politie zou in de komende jaren wel eens de grootste bottleneck voor de politie kunnen zijn.

Zoals al eerder vermeld, komen corrupte contacten veelal via via tot stand. Bestaande relaties die niet voor dat doel waren aangegaan, leiden uiteindelijk tot contacten met criminelen. Door nieuwe communicatiemogelijkheden kunnen ook nieuwe manieren voor het aangaan van corrupte contacten ontstaan. Een voorbeeld is Hyves, een internetservice waar mensen contact met elkaar kunnen leggen. Door persoonlijke informatie prijs te geven maak je je kwetsbaar voor corrumperende contacten. Zo is het voorgekomen dat iemand zich bekend maakte als politiemedewerker en op een andere plaats op zijn pagina iets onoorbaars deed, zoals aangeven wel een politie–uniform te kunnen regelen.

Als tegenhanger van de genoemde risicofactoren wordt de toegenomen nadruk op het integriteitsbeleid genoemd. Er is de laatste jaren meer aandacht voor het verschijnsel corruptie, hetgeen onder andere tot uiting komt in meer wet– en regelgeving en in het ontwikkelen van integriteitsbeleid bij overheid en bedrijven.

Volgens respondenten bij de Rijksrecherche valt veel winst te behalen door medewerkers goed te begeleiden. Integriteitsrisico's nemen af als voldaan wordt aan het '3S–model': selectie, salariëring en scholing. Bij de selectie moet al goed worden gelet op mogelijke kwetsbaarheid voor corruptie, zoals het hebben van risicovolle contacten. In veiligheidsonderzoeken zoals bij de politie wordt hier aandacht aan besteed. Een risicofactor is ook lage salariëring en hier zou volgens de respondenten ook aandacht aan besteed moeten worden om corruptie terug te dringen. Door scholing kan worden bereikt dat medewerkers helder voor ogen hebben welke gevaren er dreigen en hoe ze zich daar tegen kunnen wapenen.

In het deelrapport *Criminele afscherming en verweving* (DNRI, 2004b) staan enkele maatschappelijke factoren die mogelijk een relatie hebben met corruptie. Van de EU–uitbreiding (en internationalisering in het algemeen) wordt een mogelijk 'besmettend' effect verwacht. Ten tijde van het eerste NDB was de uitbreiding van de EU en het te verwachten effect daarvan op de criminaliteit een onderwerp van discussie. Anders dan destijds verwacht werd, lijkt het er in 2007 niet op dat Oost–Europeanen oververtegenwoordigd zijn bij de criminelen die overheidsdienaren corrumperen. Criminele groepen uit Oost–Europa houden

zich vooral bezig met vermogenscriminaliteit, waarbij activiteiten zich snel verplaatsen. Het corrumperen van opsporingsambtenaren is hiervoor weinig relevant. Bovendien verloopt het lekken van opsporingsinformatie veelal via bestaande relaties en mensen uit Oost–Europese landen beschikken vaak (nog) niet over dergelijke contacten.

2.1.7 Verwachtingen voor de toekomst

In de deelstudie voor het NDB 2004 (DNRI, 2004b) wordt geen voorspelling gedaan over toename of afname van corruptie. Het aantal bekende zaken was klein en er was geen sprake van een trend in enige richting. Cijfers zijn echter ook niet helemaal compleet en daardoor kan het beeld dat ze oproepen onbetrouwbaar zijn.

Volgens sommige respondenten hebben bepaalde groepen criminelen zoveel belang bij het verkrijgen van *inside information* over de opsporing, dat ze ver zouden kunnen gaan om mensen binnen de opsporingsdiensten te corrumperen. Tot op heden zijn er echter weinig signalen van het tegen betaling lekken van belangrijke gegevens. De belangen die criminelen hebben bij deze informatie zal de komen jaren niet afnemen, zodat verwacht mag worden dat af en toe pogingen aan het licht komen om politiemensen te corrumperen.

Voor de toekomst is de aard en omvang eigenlijk niet te voorspellen. Ieder zichzelf respecterend crimineel samenwerkingsverband moet ervan uitgaan dat het de aandacht heeft (of krijgt) van recherchediensten. Contrastrategieën vanuit criminele samenwerkingsverbanden zullen dan ook actueel blijven. Ze kunnen verschillende vormen aannemen, waaronder corruptie.

2.2 Corruptie bij grensoverschrijding

In deze paragraaf worden de bevindingen gepresenteerd ten aanzien van corruptie van toezichthouders en personeel in de logistiek bij grensoverschrijding. Omdat toezichthouders veelal ambtenaar zijn, overlapt deze paragraaf ten dele de vorige. De wijze van benadering door leden van criminele samenwerkingsverbanden is daar beschreven.

2.2.1 Inleiding

Toezicht bij het overschrijden van de landsgrenzen wordt uitgeoefend door de douane, de marechaussee en de politie. Het komt voor dat deze toezichthouders tegen vergoeding hand– en spandiensten verlenen aan criminele

samenwerkingsverbanden. Ondanks de geringe cijfers worden de gevolgen voor de Nederlandse samenleving als aanzienlijk gezien. Om die reden is corruptie van toezichthouders bij grensoverschrijding in het NDB 2004 aangemerkt als een potentiële dreiging (DNRI, 2004a).

Ook medewerkers van private bedrijven in de logistieke keten kunnen gecorrumpeerd worden om medewerking te verlenen aan illegale grensoverschrijding of drugssmokkel. Bij de informatieverzameling heeft de nadruk gelegen op de toezichthouders, voornamelijk de douane en de marechaussee. De respondenten hebben ook informatie verschaft over activiteiten van medewerkers van bedrijven in de logistieke keten.

Voor het NDB 2004 werd een (vertrouwelijke) studie verricht naar infrastructuren van grensoverschrijding (DNRI, 2004c). De studie is ingericht naar de vier vervoersmodaliteiten luchtvaart, scheepvaart, wegtransport en railtransport. Het thema corruptie komt het meest uitgebreid aan de orde onder de kop 'luchtvaart'. Volgens het rapport zijn er medewerkers van Schiphol betrokken bij criminaliteit, met name bij drugs– en mensensmokkel. Ook werd geregeld diefstal geconstateerd. Medewerkers in de bagagekelder en schoonmakers behoren tot de risicogroepen. Het betreft laag gekwalificeerd en weinig aantrekkelijk werk dat in wisseldiensten wordt verricht. Personeel wordt vaak via uitzendbureaus geworven. Volgens sommige experts neemt de criminele druk op medewerkers van Schiphol om mee te werken aan delicten toe door voortschrijdende technische beveiliging. Naast corruptie zou daarbij ook chantage en geweld niet worden geschuwd. Wat betreft de havens wordt in het rapport Infrastructuren van grensoverschrijding slechts vermeld dat corruptie een rol speelt bij diefstal van containers met kostbare lading. Dergelijke diefstallen zijn vrijwel onmogelijk zonder hulp van binnenuit. Ook technologische mogelijkheden om te controleren of containers open geweest zijn sinds de verzegeling, kunnen altijd worden gesaboteerd door corrupte medewerkers. Dit vormt ook een dreiging voor de toekomst: technologische vormen van controle zullen leiden tot een verdere toename van de druk op medewerkers vanuit criminele hoek.

Door Nelen en Nieuwendijk (zie ook 2.1.1) werd een studie verricht naar ambtelijke corruptie, onder meer bij grensoverschrijding. Zij komen tot de bevinding dat het in Nederland voor criminelen meestal onnodig is om ambtenaren op een strategisch niveau te corrumperen. Door het transitkarakter van de criminaliteit in Nederland is het vaak afdoende om op uitvoerend niveau medewerking van ambtenaren en toezichthouders te verkrijgen. Het is niet nodig om werkelijk machtsposities op te bouwen (Nelen en Nieuwendijk, 2003).

Onderzoek voor deze actualisering

Voor deze actualisering is beperkt literatuuronderzoek verricht. Er bleek weinig literatuur beschikbaar die specifiek op het onderhavige thema gericht is. Verder zijn interviews gehouden met mensen van de marechaussee, onder meer van de afdeling Intern Onderzoek en van het Expertisecentrum Luchthavens. Bij de douane is gesproken met medewerkers van het Douane Informatiecentrum (DIC) en het expertisecentrum Zeehavens. Bij de politie spraken we met een vertegenwoordiger van het programma *Transport Security*. De volledige lijst van functies van geïnterviewden is te vinden in bijlage 1.

2.2.2 Aard

In het NDB 2004 werd al gerapporteerd dat er op Schiphol veel mogelijkheden voor criminaliteit zijn waarbij vaak medewerkers zijn betrokken en soms ook medewerkers van de douane of de marechaussee. Onderscheid moet gemaakt worden tussen het verlenen van hand– en spandiensten, bijvoorbeeld door iets door te laten of bepaalde informatie te geven, en het zelf bezig zijn met een bepaalde handel, dus meer directe betrokkenheid. Beide vormen komen voor.
De belangrijkste vormen van criminaliteit op Schiphol zijn drugssmokkel, mensensmokkel en mensenhandel. Diefstallen en overvallen komen ook voor. Het komt ook voor dat drugskoeriers worden gericht door mensen die zich voordoen als contactpersonen van de opdrachtgever. In sommige gevallen is hierbij sprake van hulp van binnenuit, dus van personeel op Schiphol. In het geval van diefstal van vracht wordt ervan uitgegaan dat er veelal sprake is van betrokkenheid van binnenuit, omdat het anders bijzonder moeilijk is een bepaalde kostbare vracht te traceren. Het meest aansprekende voorbeeld is de diamantroof, die later nog aan de orde komt (paragraaf 2.6.2). Dit incident was de aanleiding om de toegang tot de luchthaven grondig onder de loep te nemen.

Douaniers opgepakt bij oprollen drugsbende Schiphol
Uitgegeven: 30 mei 2007 13:20

SCHIPHOL – Rechercheurs van de marechaussee hebben negen verdachten, onder wie twee douaniers, aangehouden tijdens het oprollen van een drugsorganisatie die actief was op luchthaven Schiphol. De douaniers werden onder meer bij drugscontroles ingezet, laat de marechaussee op Schiphol woensdag weten.
Volgens woordvoerder Rob Stenacker van de marechaussee maakt dit onderzoek deel uit van een groot offensief tegen allerlei medewerkers op Schiphol die bij de drugshandel zijn betrokken. Ook een derde gearresteerde verdachte in deze zaak, werkt op de luchthaven.

Cocaïne

Tijdens het opsporingsonderzoek heeft de marechaussee in totaal 78 kilo cocaïne weten te onderscheppen. Op zes plaatsen werd huiszoeking gedaan. Daarbij vond de marechaussee nog eens een vuurwapen, drie imitatiewapens en nog een kleine hoeveelheid cocaïne.

"Deze aanhoudingen behoren tot een reeks arrestaties waarbij de marechaussee de invoer van drugs met behulp van personeel op Schiphol een grote slag wil toedienen", benadrukt Stenacker. "We willen het misbruik van de bevoegdheden van medewerkers op Schiphol tegengaan, omdat zij een belangrijke schakel kunnen vormen in een drugsorganisatie."

Misbruik

Het offensief heeft de afgelopen maanden al tot verschillende resultaten geleid. Zo wisten de opsporingsdiensten op het vliegveld in maart, april en mei al verschillende drugsorganisaties op te rollen die misbruik maakten van medewerkers op Schiphol.

De laatste drie maanden arresteerden de marechaussee, de douane en de FIOD/ECD in totaal zestien personen die op Schiphol werken en die verdacht worden van betrokkenheid bij drugssmokkel. Bij deze acties werd in totaal 378 kilo cocaïne onderschept.

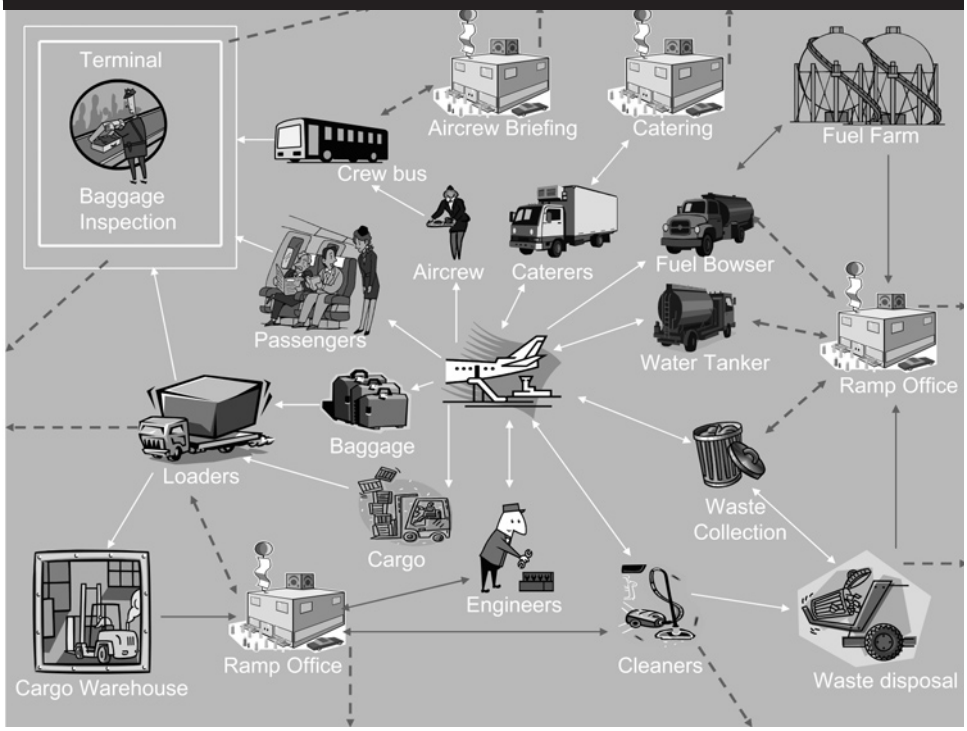
(c) ANP

Betrokkenheid bij (drugs–)smokkel

Een aanzienlijk deel van de criminaliteit op Schiphol heeft een relatie met drugshandel. De bagagekelder wordt al jaren gezien als een plek waar medewerkers zich inlaten met drugshandel. Volgens een respondent heeft er de laatste 25 jaar altijd wel een onderzoek naar verdovende middelen gelopen op de bagageafhandeling. Steeds weer worden medewerkers van de bagageafhandeling gearresteerd. Het aanbod van nieuw personeel is echter zeer groot en het lukt kennelijk niet om criminele elementen buiten de deur te houden. Behalve de bagageafhandeling zijn er ook andere mogelijkheden voor smokkel. Figuur 2.1 geeft alle logistieke stromen op een luchthaven weer. In principe kan iedere stap in het logistieke proces aangegrepen worden voor criminaliteit en dit blijkt volgens respondenten ook te gebeuren.

Figuur 2.1

Mogelijkheden voor criminaliteit op een luchthaven



Een respondent bij de douane onderscheidt enkele laakbare methoden die gebruikt worden door mensen binnen de luchthaven. *Ongemanifesteerde lading* is lading die niet of foutief is aangemeld en nergens in de systemen voorkomt. De moeilijkheid voor een crimineel samenwerkingsverband is dat zowel bij vertrek als ontvangst een corrupte medewerker aanwezig moet zijn. Daarnaast wordt de *diefstal uit het logistieke proces* onderscheiden. Hierbij wordt smokkelwaar meegestuurd met reguliere zendingen. Het is dan uiteraard zaak dit weer tijdig uit deze zendingen te halen. Dit vereist voorkennis van de lading. Vaak wordt een combinatie van deze twee methoden aangetroffen. Een derde methode betreft de *airbags* waarbij bagage zonder passagier reist, veelal met valse labels. In een grote koffer zitten tassen of rugzakjes die gemakkelijk meegenomen kunnen worden door corrupte handlangers in de bagagekelders. Deze methode is zeer moeilijk te bestrijden, omdat het onmogelijk is om iedere activiteit in de bagageafhandeling te controleren. Ten vierde wordt via *secundaire stromen* veel gesmokkeld. Bij deze vorm van smokkel is catering–, platform– of emballagepersoneel betrokken.

Corruptie bij transportexpediteurs

Een respondent bij de douane wijst erop dat criminele samenwerkingsverbanden in toenemende mate expertise binnenhalen die van pas kan komen bij hun activiteiten. Voor succesvolle smokkel, is het van belang om goed ingevoerd te zijn in de wereld van het transport. Daarom proberen criminele samenwerkingsverbanden binnen te komen bij bedrijven waar deze expertise voorkomt. Dit is bijvoorbeeld het geval bij transportexpediteurs, gespecialiseerde bedrijven die formaliteiten bij de grensoverschrijding van goederen afhandelen. Daarbinnen zijn enige honderden 'douane expediteurs', bedrijven die werken op basis van een speciale vergunning van de douane.

Bij een integere dienstverlening kunnen deze bedrijven vaak als een verlengstuk van de opsporing worden beschouwd. Vanwege hun expertise zijn ze in staat om onregelmatigheden in het transport te ontdekken, zoals een product dat te licht of juist te zwaar blijkt te zijn. Hun kennis kan echter ook misbruikt worden door criminelen. Om zich tegen de inmenging van criminelen te weren, hanteren de grote bedrijven veelal een streng intake–beleid. Als gevolg hiervan zijn vooral de kleinere bedrijven kwetsbaar voor criminele bemoeienis. Zij zijn in grotere mate afhankelijk van een enkele klant, waardoor ze vaker bereid zijn risico's te nemen.

Mensensmokkel en mensenhandel op Schiphol

In het verleden is veel misbruik gemaakt van de passen van werknemers van bedrijven op Schiphol naar het beveiligde deel van de luchthaven. Deze pasjes werden gebruikt om mensen mee te laten lopen. Ook werden ze uitgeleend om ongeautoriseerde personen toegang tot de luchthaven te verschaffen. Om het misbruik van de passen uit te bannen is eind 2005 een nieuwe pas ingevoerd waarbij gebruik gemaakt wordt van de irisscan (zie paragraaf 2.2.6 over de commissie Oord) waardoor de Schipholpas niet meer overdraagbaar is. Dit blijkt een goed middel te zijn om mensensmokkel tegen te gaan[2]. Hoewel de respondent de verwachting uitsprak dat mensensmokkelaars wel weer nieuwe methoden zullen vinden, is vooralsnog de daling van de aantallen een feit (zie ook het nog te verschijnen Dreigingsbeeld Luchthavens.) Wel is het zo dat transitomigratie, waarbij gesmokkelden niet buiten het beveiligde gebied komen, niet kan worden voorkomen door deze nieuwe pas. Hiermee kunnen mensen echter niet Nederland binnen komen.

---

[2] Na het sluiten van de gegevensverzameling voor dit rapport bleek echter dat journalisten wel degelijk Schiphol binnen konden komen. Zie: NRC Handelsblad, 7 februari 2008.

Havens

Bij beschrijvingen van corruptie in de logistiek ligt de nadruk sterk op de luchtvaart, met name op de luchthaven Schiphol. Ook in opsporings-onderzoeken van de Rijksrecherche ligt de nadruk vooral daar, als het gaat om grensoverschrijding. Nelen en Nieuwendijk (2003) vonden in hun analyse van dossiers bij de Rijksrecherche maar één zaak die in de Rotterdamse haven speelde. De auteurs verwijzen ook naar de WODC–monitor (Kleemans, Brienen & Van de Bunt, 2002) waarin eveneens gerapporteerd werd dat corruptie van politie en douane in de havens niet aan de orde lijkt te zijn. In deze rapporten werd vooral gekeken naar ambtelijke corruptie.

De ondervraagde experts stellen dat de kans op corruptie onder toezichthouders in de Rotterdamse haven kleiner moet zijn dan op Schiphol. Smokkel via zeehavens vraagt andere werkwijzen dan die via de lucht, wat te maken heeft met het verschil in typen goederenstromen tussen beide vervoersmodaliteiten. Bovendien is er in de zeehavens geen sprake van een grote stroom personen-vervoer zoals op luchthavens. Luchtvracht is, in vergelijking met zeevracht, voor criminelen relatief eenvoudig bereikbaar om er illegale zaken tussen te voegen dan wel uit te halen.

Anders dan bij luchtvracht wordt bij smokkel via de zee smokkelwaar vaak verborgen in bulkgoed, zoals bijvoorbeeld koffie. Volgens een respondent bij de douane komt deze methode het meest voor bij smokkel via de zee. Corruptie is dan niet nodig. In het vrachtvervoer wordt om dezelfde reden minder corruptie verwacht. Het vervoer van vracht gaat gepaard met een papieren proces waarbij diverse actoren betrokken zijn. Vergeleken met smokkel via de passagiersstroom is smokkel in vrachtvervoer moeilijker te organiseren, maar is tegelijkertijd minder afhankelijk van ambtelijke corruptie.

Dat neemt niet weg dat er groot belang is bij medewerking van binnenuit voor het volbrengen van criminele activiteiten. Naast smokkel vindt in en om de haven ook veel diefstal van waardevolle ladingen plaats. Dit blijkt ook uit de opsporingsonderzoeken van de zeehavenpolitie en de douane. In 2006 liep bij een van de grote containerterminals een omvangrijk onderzoek tegen een groep havenarbeiders (waaronder een kraanmeester) die hand– en spandiensten verleenden aan een criminele groep. Voor criminelen is het belangrijk om mensen op informatieposities te hebben, zodat ze op de hoogte zijn van de locatie van bepaalde containers of zelfs in staat zijn om hierin te sturen. Volgens de respondent bij het expertisecentrum Zeehavens is niet alleen directe betrokkenheid of corruptie van medewerkers in het spel. Ook via cafés in de buurt kunnen criminelen veel te weten komen, bijvoorbeeld waar de (financieel)

zwakke bedrijven zitten. In ruil voor wat geld krijgen zij informatie of kunnen zij zelfs iemand 'er tussen schuiven'. Chauffeurs kunnen bij het ophalen van hun werkpapieren in het bakje van een collega kijken en er zo achter komen wie een mooie lading heeft. Er worden weliswaar preventieve maatregelen getroffen (bakjes op slot), maar daar wordt in de praktijk vaak de hand mee gelicht. Wat ook voorkwam is dat een beveiligingsmedewerker van een bedrijf zelf corrupt was. Tegen forse betaling wilde hij de slagboom zonder vragen omhoog doen om een container door te laten.

Wat betreft de aard van de diefstallen is sprake van een grote variatie en soms is er sprake van betrokkenheid van werknemers of van handelaren. Bij ladingdiefstal kan het gaan om goederen die per stuk een grote waarde vertegenwoordigen, zoals computers en plasmaschermen. Deze kunnen relatief eenvoudig worden afgezet. Maar het gaat bij ladingdiefstal ook geregeld om ruwe materialen, zoals bijvoorbeeld metalen, olie en benzine. Diefstal van dergelijke materialen duidt op verwevenheid van onder– en bovenwereld. Grote hoeveelheden nikkel of stookolie kunnen immers niet via de kroeg worden afgezet. Voor dergelijke handel moet gespecialiseerde klandizie worden gevonden. Er zijn onderzoeken geweest tegen handelaren die zich in hebben gelaten met ladingdiefstal. In sommige gevallen is in de boekhouding te achterhalen dat zich onregelmatigheden moeten hebben voorgedaan bij de inkoop van producten.

Koeriersbedrijven: blinde vlek bij grensoverschrijding

De mate waarin medewerkers van internationale koeriersbedrijven betrokken zijn bij smokkel is niet bekend. Volgens een respondent wordt deze stroom niet serieus gecontroleerd. Wel zou *pre departure controle* opkomen. Pakketten worden dan voor verzending gecontroleerd.

Een medewerker van de betrokken douaneafdeling vertelde dat er wel verdenkingen zijn dat zich zaken voordoen in de koeriersbranche, maar dat er recentelijk niets is geconstateerd. Ook waren er geen gevallen bekend van douaniers die zich lieten corrumperen. Eerder werd wel gerapporteerd dat medewerkers van koeriersbedrijven soms betrokken zijn bij smokkel (DNRI, 2004c).

2.2.3 Omvang

In de literatuur over corruptie is de verzuchting te lezen dat alle betrokken partijen er belang bij hebben dat corruptie verborgen blijft, zo ook in het NDB 2004. Daarom wordt alom aangenomen dat er sprake is van een aanzienlijk *dark number*, en dat de geconstateerde gevallen slechts het topje van de ijsberg vormen.

Voor ambtelijke corruptie op de luchthaven Schiphol zijn volgens respondenten veel potentiële mogelijkheden en er staan grote belangen op het spel. Het gaat daarbij vooral om zaken rond drugs en mensensmokkel. De indruk bestaat dat het vooral gaat om 'kleine' contacten, bijvoorbeeld iets doorlaten of informatie over een bepaalde vlucht geven. Een respondent bij de marechaussee spreekt zijn twijfels uit over de vraag of corruptie op grote schaal voorkomt. Volgens een respondent bij de douane gaat het bij die dienst om slechts enkele gevallen per jaar. Niettemin zijn er ook grotere zaken geweest waarbij toezichthouders waren betrokken. (Zie bijvoorbeeld het kader in paragraaf 2.2.2).

De cijfers gaan als altijd over de zaken die wel geconstateerd zijn. Op Schiphol zijn in 2006 in totaal 44 zaken geweest, waarvan er 10 zijn overgedragen aan de politie (zowel regio's, bovenregionale rechercheteams als de Nationale Recherche). Er waren 9 zaken niet opgestart wegens te weinig opsporings-indicatie. 17 zaken zijn op Schiphol zelf gedraaid en 8 zijn nog in behandeling. Van deze 44 zaken zijn er 13 gerelateerd aan migratie, één aan vuurwapens en de rest (30) gaat om drugssmokkel.

Volgens een respondent bij de marechaussee is het zeer moeilijk om precieze aantallen corruptiezaken (en een stijging of daling) aan te geven. Voor een deel komt dit door gebrek aan capaciteit, waardoor niet iedere zaak tot een opsporingsonderzoek leidt. Ook kan het voorkomen dat een oude zaak, die in eerste instantie geen prioriteit heeft gekregen, op een later tijdstip opnieuw wordt aangeboden en dan wel wordt aangepakt.

Ook een respondent van het expertisecentrum Havens vindt het moeilijk om uitspraken te doen over de omvang van corruptie. Veel bedrijven waarvan spullen zijn gestolen, veelal met betrokkenheid van binnenuit, doen geen aangifte. Hiervoor worden verschillende redenen genoemd. Bedrijven zijn beducht voor imagoschade. Als bekend is dat er bij hen veel gestolen wordt, lopen zij de kans minder opdrachten te krijgen. Bovendien wordt schade ook ingecalculeerd, het is een bedrijfsrisico. Een andere reden om geen aangifte te doen is dat bedrijven de kans lopen alsnog BTW te moeten betalen over de gestolen lading. Als geen aangifte wordt gedaan, kan het bedrijf niet verantwoordelijk worden gehouden voor de invoer in Nederland.

Cijfers over aangiften waarbij corruptie in het spel is, kon het expertisecentrum Havens niet geven. Hierbij speelt ook een rol dat de corruptie zich kan afspelen in de haven, terwijl het feitelijke delict ergens anders gepleegd wordt. Dit is bijvoorbeeld het geval als een medewerker van een bedrijf in de haven informatie over een transport doorgeeft aan criminelen, waardoor de lading

buiten het haventerrein gestolen wordt. Dit kan op de snelweg zijn, ergens in Nederland of in het buitenland. Het expertisecentrum krijgt daardoor lang niet alle gevallen door waar mogelijk een relatie is met corruptie in de haven.

2.2.4 Betrokken personen en groeperingen

In het NDB 2004 werd gerapporteerd over de risicogroepen voor corruptie in de logistieke keten. Hiertoe behoren medewerkers van bagageafhandeling en schoonmaak op Schiphol, van containerbedrijven in de havens en mensen die betrokken zijn bij het vrachtvervoer per spoor of over de weg. Deze groepen komen in deze actualisering ook weer naar voren.

Het beeld dat uit de interviews naar voren komt, is dat corruptie vooral speelt op de werkvloer. Dit is niet verbazingwekkend. Zoals al eerder aan de orde kwam, hebben criminelen, waarvan de meesten zich in Nederland voornamelijk bezighouden met *transit crime*, er weinig belang bij om zich in te laten met hogere functionarissen en deze te corrumperen. Een respondent opperde wel dat het mogelijk is dat de focus van de opsporingsonderzoeken tot enige vertekening leidt: deze zijn vooral gericht op de lagere rangen. Overigens bevestigen deze onderzoeken het beeld dat criminelen vooral daar belang hebben: er moet iemand gevonden worden om iets door te laten of hand– en spandiensten te verlenen bij smokkelpraktijken. Het beïnvloeden van meer strategische beslissingen is voor criminelen niet zo relevant.

Op Schiphol worden de medewerkers van de bagagekelder en de platforms gezien als de zwakke schakel in het personeelsbestand. Het betreft veelal laag opgeleide werknemers in de onderste salarisschalen. Volgens een respondent bij de marechaussee valt op dat voor dit weinig aangename werk altijd mensen in de rij staan om vacatures op te vullen. Er blijven steeds nieuwe mensen binnenkomen die mee kunnen gaan doen met de criminele praktijken. Het lijkt er op dat de opsporingsonderzoeken bij de bagageafhandeling weinig afschrikkende werking hebben op de criminaliteit.

Evenals in vorige rapportages van het NDB wordt door sommige respondenten gewezen op de mogelijkheid dat mensen uit andere culturen een risico vormen. In sommige landen komt corruptie vaker voor dan in Nederland en zijn de onderlinge contacten, zoals familiebanden, anders dan hier. Of er ook werkelijk sprake is van een oververtegenwoordiging van mensen met een niet–Nederlandse etnische achtergrond is niet duidelijk. Er wordt geen registratie van corruptiegevallen naar etniciteit bijgehouden. In eerder NDB–onderzoek werd nagegaan in hoeverre er een verhoogd risico was voor corruptie onder

allochtone (financiële) dienstverleners (DNRI, 2006c). Daar werden geen aanwijzingen voor gevonden, wat nog niet betekent dat dit resultaat ook geldig is voor de logistieke sector.

Een respondent bij de douane geeft aan dat er beleid is ten aanzien van bepaalde risicogroepen. Hij wees erop dat het team van de douane dat zich richt op drugskoeriers bijzonder interessant is voor criminelen. Als ze daar iemand 'plat' kunnen krijgen, dan kunnen ze veel eenvoudiger de grens passeren. De douane-medewerkers zijn door hun expertise kwetsbaar voor corruptie. Om die reden worden mensen in dergelijke functies na drie jaar vervangen door anderen.

2.2.5 Gevolgen voor de Nederlandse samenleving

Zoals al in het NDB 2004 werd vermeld, kan corruptie onder personeel in de logistieke keten criminele activiteiten vergemakkelijken en kan het imago van het Nederlandse bedrijfsleven worden ondermijnd. Een respondent bij het expertisecentrum Havens meldde dat in de Engelse pers bericht is dat er in de Rotterdamse haven veel gestolen wordt. Het gevolg hiervan kan zijn dat reders uitwijken naar andere havens, wat leidt tot economische schade.

2.2.6 Criminaliteitsrelevante factoren

Zoals ook al in paragraaf 2.1 werd gesteld, zijn criminele samenwerkingsverbanden altijd geïnteresseerd in informatie over de activiteit van de 'tegenstander'. Bij voorkomende gelegenheden zullen ze de kans grijpen om iemand te betalen om deze informatie in handen te krijgen. Soms zullen ze proberen om iemand op een strategische positie in het logistieke proces te brengen ('er tussen te schuiven', in het jargon van respondenten) om de criminele plannen, zoals drugs– en mensensmokkel en ladingdiefstal te kunnen volbrengen. Zoals door Kleemans e.a. (2002) werd gesteld, houden de in Nederland actieve criminelen zich vooral bezig met *transit crime*, waarbij zij vooral belang hebben bij 'kleine corruptie': betrokkenheid van personen op de werkvloer en van mensen die bepaalde concrete informatie kunnen verschaffen. In zekere zin is dit belang 'van alle tijden', zoals veel respondenten het uitdrukten. Niettemin worden er ook wel ontwikkelingen gesignaleerd op het vlak van corruptie in de logistiek.

Verbetering van de beveiliging

In het algemeen wordt gesteld dat een toename van de beveiliging op bepaalde locaties tot gevolg zal hebben dat enerzijds een verplaatsing optreedt en dat anderzijds het belang om mensen te corrumperen (nog) groter wordt. Als

containers in de terminals in de Rotterdamse haven zodanig beveiligd worden met hekken, camera's en passen dat men er niet meer mee de poort uit komt, ook niet als iemand die welbewust opent, dan wordt het zaak om andere manieren te vinden om de waardevolle lading te ontvreemden. Dit kan bijvoorbeeld door aan informatie te komen over waar en wanneer een bepaalde lading op een andere, minder beveiligde locatie, kan worden gestolen. Zo leidt een verbetering van de beveiliging bij de containerterminals mogelijk tot een toename van ladingdiefstal op de parkeerplaatsen langs de grote snelwegen in Nederland en daarbuiten.

Commissie Oord: beveiliging Schiphol verbeterd

De afgelopen jaren zijn op Schiphol diverse maatregelen genomen om de veiligheid te vergroten. De bestrijding van terrorisme, prioriteit sinds september 2001, heeft hierbij een rol gespeeld. Meer nog is de beveiliging verbeterd naar aanleiding van de diamantroof in februari 2005. Hoewel tot op heden niet opgehelderd is hoe deze roof precies heeft kunnen plaatsvinden, wordt het uiterst onwaarschijnlijk geacht dat de daders dit zonder hulp van binnenuit hebben gedaan. Ze hebben de diamanten geroofd en zijn van het Schiphol-terrein weggekomen in een busje waarin de diamanten naar een vliegtuig vervoerd zouden worden. De roep om verbetering van de beveiliging van de luchthaven zwol dan ook aan. In juni van dat jaar verscheen het rapport van de commissie Oord waarin een aantal aanbevelingen werden gedaan, met name gericht op het toegangsbeheer en het passensysteem (Commissie Toegangsbeheer Schiphol, 2005). Van belang voor dit onderzoek is dat naar aanleiding van het rapport van de commissie Oord enkele maatregelen, die al in voorbereiding waren, versneld werden ingevoerd. Dit betreft met name het invoeren van een passensysteem waarbij gebruik gemaakt wordt van biometrische kenmerken van de houder (irisscan), het drastisch inperken van het aantal poortjes tussen de *landside* en de *airside* van de luchthaven en het geheel uitbannen van onbewaakte poortjes tussen beide gebieden. Deze maatregelen maken het uitlenen van passen en het laten meelopen van anderen bij het betreden van de beveiligde delen van Schiphol volgens geïnterviewden nagenoeg onmogelijk[3].

Een respondent stelt dat door de toename van de beveiliging op Schiphol, met name de invoering van de irisscan, er minder gebruikgemaakt wordt van corrupte toezichthouders. Men probeert methoden te gebruiken waarbij geen hulp van binnenuit nodig is, zoals drugssmokkel op of in het lichaam. De irisscan heeft tot gevolg gehad dat de mensensmokkel is verminderd. Respondenten

[3] Hoewel het systeem in februari 2008 nog niet waterdicht bleek, zie NRC, 7 februari 2008.

nemen overigens wel aan dat mensensmokkelaars op zoek gaan naar andere manieren om mensen de grens over te krijgen, al zijn dergelijke nieuwe werkwijzen nog niet gesignaleerd.

Wat betreft de luchtvaart ligt de nadruk steeds op Schiphol, waar de beveiliging onder invloed van de commissie Oord is verbeterd. Maar er zijn nog meer vliegvelden in Nederland en zij vormen de zwakke schakel. De vijf grootste van deze kleinere vliegvelden staan onder controle van de marechaussee wat betreft de algemene politietaak. Deze taak ligt bij de kleinere vliegvelden bij de politiekorpsen. Voor de grenscontrole op de kleine luchthavens door douane en marechaussee is er in Nederland sinds 2006 een plan van aanpak, nadat eerder geconstateerd was dat op deze vliegvelden kans op smokkelpraktijken was ontstaan. Volgens een respondent bij de douane is het wel een probleem dat de grenscontrole op afroep plaatsvindt, waardoor het niet altijd mogelijk is om op de juiste tijd op de juiste plaats te zijn.

2.2.7 Verwachtingen voor de toekomst

'Het is er altijd geweest, en zal altijd wel blijven' is een citaat uit veel verschillende interviews.

Niettemin verwachten diverse respondenten dat de betrokkenheid bij criminaliteit van toezichthouders, maar vooral personeel van bedrijven in de logistieke sector zal toenemen. De reden daarvoor is dat de criminele belangen bij grensoverschrijding bijzonder groot zijn en alleen maar toenemen.

Op Schiphol is men weinig optimistisch ten aanzien van de toekomst van de luchthavencriminaliteit. Het is moeilijk om laakbaar gedrag van medewerkers in de uitoefening van de reguliere functie te ontdekken, laat staan aan te tonen. Bij de bagageafhandeling is bijvoorbeeld geen verschil te zien tussen criminele handelingen en het gewone dagelijkse werk. De mogelijkheden om te variëren in criminele werkwijzen zijn legio. Niettemin heeft de irisscan geleid tot een daling van mensensmokkelhandel. In de toekomst wil men gaan werken met *integrity testing*, waarbij bijvoorbeeld gebruik gemaakt wordt van lokkoffers om te kijken wie bereid is om deze weg te nemen. Volgens een respondent bij de douane is het vooral belangrijk om medewerkers bewust te maken van integriteit en hen te wijzen op de risico's van corruptie.

Een respondent in de Rotterdamse haven vermoedt dat de onderwereld steeds meer vervlecht raakt in de bovenwereld. Er zijn grote bedragen gemoeid met smokkel en diefstal. Voor criminelen is het redelijk eenvoudig om in de haven

binnen te komen. Antecedentenonderzoeken zijn in het bedrijfsleven ongebruikelijk en uitzendkrachten worden al helemaal niet gecontroleerd. Respondenten schatten in dat het probleem alleen maar groter zal worden. De ontwikkeling van de tweede Maasvlakte zal leiden tot een enorme uitbreiding. Als het controlerend personeel niet eveneens wordt uitgebreid, zal op dat vlak een achterstand ontstaan.

2.3 Corruptie van vrijberoepsbeoefenaars

'En die accountants die de fraude afdekten in plaats van justitie te bellen, dat waren ónze accountants. "Ach, die Nederlanders." Het wordt tijd voor bijstelling van het zelfbeeld' (Verlaan en Dohmen, 2003).

2.3.1 Inleiding

Onder corruptie onder vrijberoepsbeoefenaars wordt, evenals bij andere beroepen, verstaan dat bevoegdheden die uit hoofde van het beroep aan iemand zijn toegekend worden gebruikt ten gunste van derden in ruil voor een financiële of andere beloning. De derde partij bestaat in dit geval uit vertegenwoordigers van criminele samenwerkingsverbanden. Alle andere vormen van corruptie waarbij geen contacten met de georganiseerde criminaliteit voorkomen vallen dus buiten het domein van het onderzoek. In de praktijk wordt vaak gesproken van 'verwijtbare betrokkenheid bij georganiseerde criminaliteit' (DNRI, 2006c). In het NDB 2004 is corruptie onder vrijberoepsbeoefenaars als een dreiging aangeduid. Ook wordt gememoreerd dat de groep Fijnaut in 1996 heeft gewezen op het vóórkomen van betrokkenheid van advocaten en notarissen bij witwassen en afschermings-praktijken van de georganiseerde criminaliteit (Fijnaut, Bovenkerk, Bruinsma & Van de Bunt, 1996).

Naast de vrijberoepsbeoefenaars advocaten, notarissen en accountants worden ook andere financiële dienstverleners wel genoemd als een beroepsgroep die diensten kan verlenen aan criminelen. Het gaat hier om een grote groep adviseurs en tussenpersonen van diverse pluimage, zoals assurantie-tussenpersonen, medewerkers van trustkantoren, makelaars, gevolmachtigde agenten en belastingadviseurs. Over hun betrokkenheid bij criminaliteit is tot op heden weinig bekend, behalve dat er incidenteel gevallen worden aangetroffen in opsporingsonderzoeken. Evenals in de Vervolgstudie NDB (DNRI, 2006a) is in de onderhavige studie besloten om deze groep beroepsbeoefenaren buiten beschouwing te laten.

Bij de voorbereiding van deze studie is de gegevensverzameling ingeperkt, vanwege de overlap met de NDB–deelprojecten 'Witwassen' en 'Fraude'. Registratiesystemen van de politie en de EU–inventarisatie van criminele samenwerkingsverbanden zijn geraadpleegd. Daarnaast zijn interviews gehouden met vertegenwoordigers van de beroeporganisaties van advocaten (de Nederlandse Orde van Advocaten) en notarissen (de Koninklijke Notariële Beroepsorganisatie) en met mensen uit de opsporing (FIOD–ECD, Financial Intelligence Unit). Een voorgenomen interview met de Vereniging van Registeraccountants is helaas niet doorgegaan. Een overzicht van de functies van geïnterviewden is te vinden in bijlage 1.

2.3.2 Aard

Advocaten, notarissen en accountants hebben specifieke kennis op juridisch, fiscaal en financieel terrein die noodzakelijk is bij sommige aspecten van de georganiseerde criminaliteit. Het gaat hierbij met name om het management van de criminele geldstromen: het witwassen van de criminele winsten en de handelingen die hierbij komen kijken, zoals het oprichten van rechtspersonen en het aan– en verkopen van onroerend goed. Betrokkenheid kan onder meer de vorm aannemen van advisering bij financiële constructies, het passeren van een notariële akte of het bemiddelen bij onroerendgoedtransacties. Doordat criminelen de diensten inhuren van vrijberoepsbeoefenaars, worden deze bewust dan wel onbewust betrokken bij criminaliteit. Maar ook kunnen zij, maar dan meestal bewust, fungeren als katvanger, stroman of zetbaas.

Naast bepaalde kennis en bevoegdheden zijn er nog andere aspecten waardoor vrijberoepsbeoefenaars voor criminelen aantrekkelijk zijn om mee samen te werken. Vrijberoepsbeoefenaars hebben een geheimhoudingsplicht en in het geval van advocaten en notarissen een verschoningsrecht, waardoor zij niet verplicht kunnen worden om informatie over hun cliënten te verstrekken.

Faciliterende diensten die door vrijberoepsbeoefenaars worden geleverd aan criminele cliënten kunnen daardoor moeilijk achterhaald worden. Voor advocaten geldt dat ze hun geheimhoudingsplicht en verschoningsrecht kunnen gebruiken om communicatie van hun cliënt af te schermen, bijvoorbeeld door de telefoon op kantoor te laten gebruiken. Ook kunnen zij berichten meenemen voor cliënten die in beperking gedetineerd zijn en dus geen contacten met de buitenwereld mogen onderhouden. Deze mogelijkheden zijn voor criminelen aantrekkelijk en maken vrijberoepsbeoefenaars kwetsbaar om verwijtbaar betrokken te raken bij criminaliteit (Fijnaut e.a., 1996, Lankhorst & Nelen, 2004). Voor bepaalde aspecten van het logistieke proces van de georganiseerde

criminaliteit zijn vrijberoepsbeoefenaars zelfs onmisbaar. In de eerder gesignaleerde verwevenheid van de onderwereld met de bovenwereld speelt deze categorie *facilitators* een belangrijke rol (Fijnaut e.a., 1996).

Er kan een tweedeling gemaakt worden in verwijtbare betrokkenheid (corruptie) van vrijberoepsbeoefenaars. Onder verwijtbare betrokkenheid *in enge zin* wordt verstaan het willens en wetens medeplegen of medeplichtig zijn aan strafbare gedragingen. Van verwijtbare betrokkenheid *in brede zin* is sprake als er onvoldoende zorgvuldigheid is betracht, soms ook is sprake van betrokkenheid uit naïviteit (Lankhorst & Nelen, 2004).

In beide gevallen kunnen diverse gedragingen worden onderscheiden (Lankhorst & Nelen, 2004). Een advocaat kan (bewust) *lekken naar de pers*. Door stukken uit een strafdossier naar de pers te lekken, kan hij het proces beïnvloeden. Dit is sinds de aanscherping van de gedragsregels voor advocaten vanaf januari 2006 verboden. Diverse respondenten geven echter aan dat dit geen garantie is dat het sindsdien niet meer gebeurt.

Ook kan een advocaat met behulp van de pers (door te lekken of een mededeling te doen) een getuige onder druk zetten. Toen de Amsterdamse cafébaas Van der Bijl in het voorjaar van 2006 vermoord werd, vertelde een strafpleiter de volgende dag in de media dat het slachtoffer een politie–informant was. Op dat moment was dat niet bekend, dus gaf de strafpleiter volgens respondenten een signaal af aan potentiële getuigen over de mogelijke gevolgen van praten met de politie. Hoewel het moeilijk hard te maken is dat dit de bedoeling was, kan deze handelswijze een eventuele nieuwe getuige afschrikken. Overigens distantieert de Nederlandse Orde van Advocaten (NOvA) zich van deze gang van zaken en de Orde heeft het voorbeeld van Van der Bijl aangegrepen om de discussie aan te gaan op het congres 'Omgang met de Media' in 2006.

Een advocaat kan *optreden als boodschapper* voor een cliënt die in beperking gedetineerd zit. Via zijn advocaat kan hij zijn zaken blijven doen, zoals bewijsmiddelen laten verdwijnen of getuigen onder druk zetten, ondanks het feit dat hij afgesloten van de wereld behoort te zijn. Diverse respondenten hekelen deze gang van zaken en geven aan dat het op deze wijze misbruik maken van de privileges van de advocaat hen een doorn in het oog is.

Een advocaat, notaris of accountant kan zich schuldig maken aan *belangenverstrengeling* of tegenstrijdige belangen behartigen. Zo was de advocaat van Holleeder ook advocaat van een slachtoffer in hetzelfde proces en moest hij daardoor de verdediging neerleggen.

Een vierde verwijtbare handeling waaraan een vrijberoepsbeoefenaar zich schuldig kan maken is het *adviseren of uitvoeren van dubieuze transacties*. Als tijdens een ABC–constructie een pand verschillende keren in één sessie wordt doorverkocht en daarbij sterk in waarde stijgt, dan zou dit de aandacht moeten trekken van de notaris. Het probleem is volgens respondenten, dat een dergelijke dienstverlener beperkt is in het onderzoek wat hij hiernaar zou kunnen doen. In de meeste gevallen kan hij weinig anders dan zijn cliënt geloven. Ook is het volgens respondenten mogelijk dat er sprake is van 'handige zakenlieden' die het onroerend goed op korte termijn op legale wijze aanzienlijk in waarde kunnen laten stijgen. Volgens respondenten, zoals de Koninklijke Notariële Beroepsorganisatie, is een dienstverlener ook niet in staat om dit diepgaand uit te zoeken, maar daarnaast "..is het vooral zijn taak niet". Volgens diverse gesprekspartners zou je dit over moeten laten aan de opsporingsdiensten, en daarvoor zijn dan ook de Wet identificatie bij dienstverlening (WID) en de Melding Ongebruikelijke Transacties (MOT) in het leven geroepen (zie paragraaf 2.3.6).

Advocaten en andere financiële dienstverleners worden ook ingehuurd voor het adviseren over 'creatieve' financiële constructies, veelal gericht op het witwassen van crimineel geld. Een respondent bij de FIU merkt op dat dergelijke betrokkenheid bij criminaliteit veelal niet strafbaar is. De gedraging van de dienstverlener wordt pas strafbaar als hij weet, of had moeten weten, dat de herkomst van de investering van crimineel geld afkomstig is. Dit laatste is uiteraard mede afhankelijk van de mate waarin de adviseur vragen stelt en een onderzoek instelt.

Een andere vorm waar deze groep zich schuldig aan kan maken is *het misbruik van de faciliteiten*. Het verschoningsrecht (zie paragraaf 2.3.6) geldt ook voor zaken als de telefoon op kantoor en de derdenrekening. Dit biedt voor een crimineel bij uitstek een platform om zijn handelingen af te schermen voor de controle– en opsporingsinstanties, tenminste als zijn advocaat hieraan mee wil werken. Diverse respondenten zijn ervan overtuigd dat dit ook gebeurt, al doen zij geen uitspraken over de omvang.

2.3.3 Omvang

Hiervoor werd uiteengezet dat vrijberoepsbeoefenaars onder druk kunnen komen van de georganiseerde criminaliteit, omdat zij beschikken over kennis, bevoegdheden en privileges waar criminelen hun voordeel mee kunnen doen en waar ze in sommige gevallen niet buiten kunnen. Dit betekent uiteraard nog niet dat de verwijtbare betrokkenheid bij criminaliteit door vrijberoepsbeoefenaars

ook op grote schaal voorkomt. Voor een schatting van de mate waarin corruptie van vrijberoepsbeoefenaars voorkomt, kunnen verschillende bronnen gebruikt worden die alle hun beperkingen kennen. Allereerst kan gekeken worden naar de mate waarin het delict voorkomt in politieregisters. In tabel 2.1 werd de informatie uit HKS over corruptie al weergegeven, over vrijberoepsbeoefenaars is daar niets in te vinden. De jaarlijkse EU–inventarisatie van criminele samenwerkingsverbanden bevat wel enige informatie. Zie tabel 2.2.

Tabel 2.2

Aantal politieonderzoeken waarbij betrokkenheid van vrijberoepsbeoefenaars is geconstateerd

	1998	1999	2000	2001	2005	2006
Alle onderzoeken	153	118	149	146	176	182
Waarvan met vermoedens van corrumptieve contacten	56	49	45	40	45	56
Betrokkenheid bij criminele samenwerkingsverbanden						
Advocatuur	21	10	10	9	15	15
Notariaat	4	2	5	2	12	10
Accountancy en belastingexperts	7	2	3	1	15	18

Bron: EU–inventarisatie DNRI. De selectie is aangepast aan de selectie van de eerdere rapportage (DNRI, 2004b, p. 62).

Uit tabel 2.2 kan niet worden geconcludeerd dat het aantal dienstverleners dat zich laakbaar heeft gedragen de laatste jaren is gestegen.

Ook uit de interviews ontstaat de indruk dat het jaarlijks om een beperkt aantal gevallen gaat. Diverse respondenten geven aan dat uit deze beroepsgroepen slechts enkelen per jaar in beeld komen vanwege verwijtbare betrokkenheid. Niettemin kan ook een beperkt aantal vrijberoepsbeoefenaars dat zich inlaat met criminelen voor een omvangrijk probleem zorgen. Eerder is gebleken dat dienstverleners die zich laten verleiden om hand– en spandiensten te verlenen aan criminelen, al snel kan rekenen op belangstelling van meerdere criminele samenwerkingsverbanden. Iemand die zich eenmaal heeft ingelaten met criminaliteit, kan vervolgens onder druk gezet worden om nog dieper betrokken te *raken*. Deze dienstverlener is immers chantabel geworden, waardoor criminelen hem of haar 'in de tang' kunnen nemen, zoals respondenten het uitdrukken. Eén corrupte notaris, advocaat of accountant kan aldus grote schade aanrichten.

Een mogelijke bron voor een schatting van de omvang van betrokkenheid bij criminaliteit van vrijberoepsbeoefenaars wordt gevormd door de tuchtafdelingen van de beroepsorganisaties van advocaten, notarissen en accountants. Gesprekken met vertegenwoordigers van de beroepsorganisaties leveren echter weinig concrete gegevens op. Enerzijds komt dit door de manier waarop zaken worden geregistreerd en gerapporteerd. De jaarverslagen bevatten weliswaar cijfers over het aantal tuchtzaken dat wordt gevoerd, maar zaken die gerelateerd zijn aan georganiseerde criminaliteit kunnen daarin niet worden onderscheiden van bijvoorbeeld zaken naar aanleiding van klachten over dienstverleners[4]. Anderzijds zijn de beroepsgroepen er sterk op gericht om het imago van het beroep zuiver te houden. Elk krantenartikel over een vermeende corrupte advocaat, notaris of accountant schaadt dit imago. Vandaar dat bij de organisaties beleid bestaat om strafrechtelijke onderzoeken tegen leden zo veel mogelijk te voorkomen. Het primaat wordt daarom gelegd bij het tuchtrecht, waarmee de beroepsgroep laakbaar gedrag dient op te lossen. Hierbij wordt sterk gelet op het imago van de beroepsgroep als geheel. Dit beleid wordt overigens gesteund door het Openbaar Ministerie.

Het Openbaar Ministerie (OM) heeft de mogelijkheid om een dienstverlener strafrechtelijk te vervolgen. Volgens respondenten stuurt het OM echter evenals de beroepsgroepen aan op afdoening in eigen kring. Dit sluit aan bij de verplichting van het OM om bij een verdenking de beroepsgroep te benaderen. Zo moet de deken aanwezig zijn bij een doorzoeking van een advocatenkantoor in het kader van een opsporingsonderzoek. Daarnaast zijn er juridische bezwaren om een onderzoek rond te krijgen. Een verschoningsgerechtigde is moeilijk te vervolgen, want hij kan zich eenvoudig achter zijn geheimhoudingsplicht verschuilen. Respondenten wijzen erop dat kwaadwillende vrijberoepsbeoefenaars ook goed op de hoogte zijn van manieren om verborgen te blijven voor politie en justitie. Bovendien kan van een verdachte verschoningsgerechtigde niet eenvoudig de telefoon worden getapt, waardoor het OM een belangrijk opsporingsmiddel moet missen.

Volgens respondenten in de opsporing is er bij het OM in het algemeen sprake van een grote terughoudendheid om zaken tegen vrijberoepsbeoefenaars aan te pakken. Volgens hen komt het voor dat in een opsporingsonderzoek aanvankelijk *facilitators* in beeld zijn die later buiten beschouwing worden gelaten. Het gaat dan bijvoorbeeld om accountants of fiscalisten van wie door taps of financieel onderzoek vermoed wordt dat ze actief betrokken zijn bij delicten.

---

[4] In de periode van het schrijven van dit rapport haalden wel zaken de media, zoals een zaak van een advocaat uit Drenthe die verdacht werd van witwassen, btw–fraude en handel in nep–Viagrapillen eind 2007.

Het is al met al niet gemakkelijk om de omvang van verwijtbare betrokkenheid van vrijberoepsbeoefenaars bij de georganiseerde criminaliteit in beeld te brengen. Een factor die hierin ook een rol speelt, is dat de beroepsorganisaties hun best doen om er voor te zorgen dat leden die in beeld zijn gekomen in verband met het faciliteren van criminaliteit, de eer aan zichzelf houden en opstappen voordat het tot een tuchtzaak komt. Enkele bekende zaken rond advocaten kunnen hier als voorbeeld dienen. Zo hebben de advocaten Hingst en Zeegers zich beiden vrijwillig van het tableau laten schrappen toen duidelijk werd dat de beroepsgroep er anders niet aan zou ontkomen om hen te royeren. Het feit dat beiden later onder verdachte omstandigheden omgekomen zijn, kan erop duiden dat het hier om uitzonderlijke gevallen gaat[5]. Respondenten wijzen er ook op dat de (media–) aandacht voor witwassen, verwevenheid van boven– en onderwereld en het Holleeder–proces er voor gezorgd heeft dat de aandacht voor mogelijk corrupte dienstverleners is toegenomen. Hierdoor lijkt het of het aantal verwijtbaar betrokken dienstverleners is toegenomen, maar respondenten hebben niet die indruk.

2.3.4 Betrokken personen en groeperingen

Afgaande op uitspraken van respondenten, spelen bij het betrokken raken van dienstverleners als *facilitators* van criminele samenwerkingsverbanden dezelfde factoren een rol als bij het proces dat leidt tot corruptie van politiemensen en toezichthouders bij grensoverschrijding. Sommigen hebben een zekere fascinatie met 'topcriminelen' en worden aangetrokken door hun glamour. Er zijn mensen die een kleine dienst verlenen onder het motto 'dat is toch niet zo erg' en vervolgens steeds verder in het web van de criminaliteit verstrikt *raken*. Ze zijn chantabel geworden en kunnen niet meer terug. Bij de dienstverleners speelt de mogelijkheid om snel en met weinig inspanning relatief veel geld te verdienen ook een rol (Lankhorst & Nelen, 2004).

Een ander opvallend punt waar de respondenten eensgezind op duiden, is de betrekkelijk kleine sociale kring waar de onder– en bovenwereld elkaar treft. Als voorbeeld kan de Amsterdamse vastgoedwereld dienen: criminelen en dienstverleners ontmoeten elkaar in dezelfde horecagelegenheden en gaan naar dezelfde sportschool. Ook de nabijheid die eerder als criminaliteitsrelevante factor werd genoemd, speelt bij vrijberoepsbeoefenaars een rol. Zo is er het geval van een advocaat, die in zijn jeugd optrok met een latere 'topcrimineel'[6].

---

5 Hingst is in het najaar van 2005 geliquideerd en Zeegers kwam in de zomer van 2007 een aantal dagen na zijn getuigenis in het Holleeder–proces onder verdachte omstandigheden om het leven.

6 Dit vertoont gelijkenis met de eerder genoemde politieman die op school zat met de latere crimineel die hij van informatie ging voorzien.

In de vervolgstudie werd aandacht besteed aan corruptie onder allochtone dienstverleners (DNRI, 2006a). Het in het NDB 2004 ontstane idee dat deze groep een groter risico zou lopen werd niet bevestigd. Ook anderszins is er in dit onderzoek geen informatie naar voren gekomen dat mensen in bepaalde categorieën beroepsgroepen een verhoogd risico lopen.

2.3.5 Gevolgen voor de Nederlandse samenleving

Uit strafrechtelijke onderzoeken komt het beeld naar voren dat er sprake is van grote hoeveelheden crimineel geld die moeten worden witgewassen en geïnvesteerd, bijvoorbeeld in onroerend goed. Notarissen, advocaten en accountants die hierbij als dienstverleners optreden voor criminelen spelen een belangrijke rol in de verweving van boven– en onderwereld (DNRI, 2004a: p. 64). De onderzoeksgroep Fijnaut concludeerde destijds:

> "de plegers van criminele 'grondfeiten' krijgen dankzij deze dienstverleners en het misbruik van constructies de mogelijkheid om zich een weg te banen in de financieel–economische wereld. Niet de door hen gepleegde feiten leiden tot de innesteling, maar de illegaal verkregen vermogens" (Fijnaut e.a. 1996, p. 131).

De verweving van onder– en bovenwereld brengt met zich mee dat grote hoeveelheden crimineel geld binnenstromen in bepaalde markten. Bonafide partijen worden hierdoor benadeeld, omdat ze moeilijk kunnen concurreren tegen 'collega's' met illegaal verkregen vermogens. De illegale geldstromen brengen ook met zich mee dat de fiscus aanzienlijke bedragen aan belastingen derft.

Het mogelijk geringe aantal betrokkenen zegt niet veel over de totale (mogelijke) schade die wordt aangericht. Een enkele corrupte dienstverlener kan meerdere criminelen bedienen en volgens respondenten gebeurt dat ook in de praktijk. Als er van een notaris (of dienstverlener) eenmaal bekend is dat hij 'geen vervelende vragen stelt' weten collega–criminelen deze notaris eenvoudig te vinden. Tevens is het denkbaar dat hij makkelijk slachtoffer van afpersing kan worden. Een enkeling kan dus grote schade aanrichten, zowel aan de rechtsstaat als aan het imago van de eigen beroepsgroep.

2.3.6 Criminaliteitsrelevante factoren

Zoals hierboven al aan de orde kwam, hebben criminelen advies van financiële deskundigen nodig om hun illegaal verkregen vermogens wit te wassen en te investeren. De geheimhoudingsplicht en het verschoningsrecht van vrijberoepsbeoefenaars in de financiële wereld maken deze groep adviseurs des

te interessanter voor criminele samenwerkingsverbanden. Zo kunnen transacties die het daglicht minder goed kunnen verdragen, worden afgeschermd. Bijkomende gevaren zijn dat criminelen deze privileges kunnen misbruiken voor hun dagelijkse bezigheden. Zo kunnen 'derdenrekeningen' worden misbruikt om geld uit het zicht van de opsporingsdiensten te houden. De telefoon op het kantoor van de dienstverlener kan worden gebruikt voor afgeschermde communicatie, deze lijnen mogen immers niet worden afgeluisterd door justitie. Kwaadwillende leden van de vrij beroepsgroepen zijn experts op hun vakgebied en van hen kan ook verwacht worden dat ze hun eigen criminele activiteiten goed weten af te schermen.

Risico voor eenpitters en nieuwe kantoren?

Diverse respondenten (NOvA, KNB) wijzen erop dat dienstverleners van kleinere kantoren (zoals eenpitters) een verhoogd risico lopen te worden gecorrumpeerd. Kleinere kantoren zijn soms afhankelijk van een enkele cliënt, waardoor ze kwetsbaarder worden. Ook zouden jonge advocaten en accountants een grotere geldingsdrang bezitten en daarmee een verhoogd risico lopen, 'omdat ze willen scoren'. Niet alleen de notarissen en advocaten kunnen malafide zijn. Ook hun kantoorpersoneel wil opdrachten binnenhalen en kan daarbij verwijtbaar handelen. Hoe beter en meer ervaren het personeel is, des te kleiner de prikkel om deze medewerkers kritisch en minutieus te controleren. Hoewel dergelijke overwegingen plausibel lijken, gaat het om speculaties van respondenten en vergt het duiden van deze kwetsbare groepen meer onderzoek.

WID/MOT

In 2003 is de Wet identificatie bij dienstverlening (WID) en de wet Melding Ongebruikelijke Transacties (MOT) in werking getreden. Daarna is afgesproken dat de NOvA toezicht gaat houden op de naleving van de WID en de wet MOT. De dienstverleners moeten nu tijdens de intake de identiteit van hun cliënten controleren en transacties van meer dan 15.000 euro doorgeven aan de FIU. Er zitten een aantal haken en ogen aan deze betrekkelijk nieuwe wet– en regelgeving. Advocaten worden gevrijwaard van de MOT–melding als het een betaling betreft die direct gerelateerd is aan de verdediging (Lankhorst & Nelen, 2004). Van advocaten ontvangt de FIU slechts enige tientallen MOT–meldingen per jaar (DNRI, 2007a). De respondenten spreken van een aanloopperiode van zo'n anderhalf jaar, waarin de sector aan het nieuwe systeem moest wennen en waarin inhoudelijk niet veel gebeurd is. Ook is het nog onduidelijk wat er gebeurt als een dienstverlener een MOT–plichtige transactie niet meldt. Er is dan sprake van een strafbaar feit, maar hoe en door wie dit wordt aangepakt, tuchtrechtelijk danwel strafrechtelijk of een combinatie van beide, is nog niet duidelijk. Het wordt waarschijnlijk geacht dat er meer ongebruikelijke transacties

zijn dan er gemeld worden. Sinds enige tijd wordt gelobbyd om ook taxaties onder de wet MOT te laten vallen. Volgens een respondent bij de FIU zou dat een zeer welkome aanvulling zijn op het opsporingsarsenaal.

Vervolging

Volgens Lankhorst en Nelen (2004) blijft het aantal vervolgingen van verwijtbaar betrokken dienstverleners sterk achter bij het aantal verdenkingen. Bij het OM lijkt aarzeling te bestaan om verdachten strafrechtelijk aan te pakken. In de interviews werd gespeculeerd over de achtergrond van deze terughoudendheid. Zo wordt gedacht dat het politiek gevoelig ligt om verdachte advocaten aan te pakken. Het zou gezien kunnen worden als een poging tot 'uitschakeling van de tegenstander'. Het relatief hoge afbreukrisico zou er toe leiden dat het OM kopschuw wordt: mislukte zaken leiden onvermijdelijk tot negatieve publiciteit. In veel onderzoeken worden de facilitators in het begin meegenomen, maar later niet meer. Soms worden ze zelfs uit het dossier geschreven. Naast het probleem dat advocaten en notarissen zich kunnen beroepen op hun verschoningsrecht en de geheimhoudingsplicht, blijkt financieel onderzoek niet bepaald eenvoudig te zijn. Deze forensisch financiële onderzoeken zijn in vele gevallen uitermate ingewikkeld. Er zijn diverse lijnen van en naar het buitenland waar de medewerking van politie en justitie niet altijd vanzelfsprekend is. Door diverse respondenten werd aangegeven dat de Nederlandse opsporingsdiensten in het algemeen de financiële expertise missen. Nog los van het gebrek aan kennis, merkten respondenten op dat de gemiddelde rechercheur in Nederland niet snel warm loopt voor een financieel onderzoek. Een andere reden dat er niet zo snel strafrechtelijk wordt vervolgd is dat het OM de voorkeur geeft aan het 'zelfreinigende vermogen' van de beroepsgroepen. Ze kiezen primair voor het tuchtrecht. Zoals al aan de orde kwam, leidt het gebruik van het tuchtrecht tot een vertekend beeld van de omvang van het probleem. Beroepsgroepen sturen er in de meeste gevallen op aan dat de verdachte collega de eer aan zichzelf houdt.

Tarieven

Ten slotte heeft de vrije marktwerking in het notariaat (in 2006 zijn de vaste tarieven losgelaten) er volgens de KNB voor gezorgd dat "…tarieven ernstig onder druk zijn komen te staan, wat ertoe heeft geleid dat de, vooral, kleinere kantoren en eenpitters 'rollebollend' over straat gaan". Dit zou ertoe kunnen leiden dat ze minder kritisch zijn bij de intake van een nieuwe klant. Hierboven is reeds aangehaald dat juist de kleinere kantoren een verhoogd risico lopen. Overigens wordt deze stelling niet door iedere respondent gedeeld. Respondenten bij de advocatuur stellen dat er eigenlijk altijd al sprake was van vrije tarieven (op een enkele uitzondering na), maar geloven niet dat hierdoor een verandering in de gevoeligheid voor corruptie teweeg gebracht zou kunnen worden.

2.3.7 Verwachtingen voor de toekomst

Eigenlijk zeggen alle respondenten hetzelfde: het is qua corruptie in Nederland minder ernstig gesteld dan in veel andere landen, maar we moeten zeker waakzaam blijven. Vooral om de reden dat een enkele corrupte dienstverlener enorme schade kan toebrengen.

Duidelijke regelgeving en een duidelijke afbakening tussen het tuchtrecht en het strafrecht zullen een verbetering kunnen brengen. Meer en beter toezicht helpt, maar het gevaar bestaat dat de echte kwaadwillenden nieuwe wegen zullen vinden en meer 'ondergronds' gaan werken. De opsporing zal er niet eenvoudiger op worden en dit zou dan weer een extra beroep doen op de kunde en capaciteit van de financiële recherche.

3

Geweld, intimidatie enbedreiging door criminele samenwerkingsverbanden

In dit hoofdstuk staan de bevindingen ten aanzien van verschillende aspecten van geweld in relatie tot criminele samenwerkingsverbanden. In de deelstudie *Criminele samenwerking* bij het NDB 2004 (DNRI 2004d) wordt gememoreerd dat geweld weliswaar niet meer wordt gezien als inherent aan georganiseerde criminaliteit, maar dat het onder bepaalde omstandigheden wel degelijk een rol kan spelen (p. 77). In het NDB 2004 (DNRI, 2004a) is het gebruik van geweld door criminele samenwerkingsverbanden als een dreiging aangeduid.

Omdat criminele samenwerkingsverbanden spelers zijn op illegale markten, kunnen ze zich niet beroepen op de rechter en de overheid om het nakomen van gemaakte afspraken af te dwingen. Er zullen dus andere manieren gevonden moeten worden om conflicten te beslechten. Een mogelijkheid is om iemand met aanzien in het criminele milieu te vragen om te bemiddelen. Als dat niet werkt, dan is er de mogelijkheid om geweld te gebruiken of hiermee te dreigen. In alle criminele bedrijfstakken is het bezit van wapens dan ook vrij algemeen. Het daadwerkelijk gebruik wordt zo veel mogelijk vermeden, er wordt verwacht dat de dreiging met geweld afdoende is om zijn gelijk te halen. De dreiging met geweld hoeft niet altijd gepaard te gaan met concrete bedreigingen. Het hebben en houden van een gewelddadige reputatie heeft hetzelfde effect. Nadeel van het daadwerkelijk gebruik van geweld is dat er slachtoffers vallen, waardoor gemakkelijk de aandacht getrokken kan worden van politie en justitie. Het is voor criminelen dus zaak om zo rationeel mogelijk met dreiging met en gebruik van geweld om te gaan. Dat lukt niet altijd, want vele criminelen hebben een 'kort lontje' en kunnen gemakkelijk agressief en dus gewelddadig worden. Veel leden van criminele samenwerkingsverbanden (csv's) hebben antecedenten die te maken hebben met geweld, variërend van openlijke geweldpleging tot liquidaties.

In sommige csv's is sprake van een duidelijke taakverdeling, waarbij de toepassing van geweld is toebedeeld aan bepaalde specialisten. In de Criminaliteitsbeeldanalyse (CBA) Heroïne is sprake van een veelheid aan rollen binnen csv's, waarbij sommige personen binnen één csv meerdere rollen op zich kunnen nemen. In totaal konden negen rollen worden onderscheiden, waarvan geweldpleging er één is. Andere rollen die genoemd worden, zijn die

van leider, opdrachtgever, coördinator transporten, handelaar, koerier (chauffeur), leverancier, uitvoerder van ondersteunende criminele activiteiten en stroman (DNR, 2008).

Er kunnen ruwweg drie situaties worden onderscheiden waarbij geweld wordt gebruikt in het kader van de bedrijfsvoering van criminele samenwerkingsverbanden. Ten eerste wordt geweld binnen csv's gebruikt voor de handhaving van de binding aan de groep en om te voorkomen dat (afvallige) leden informatie geven aan de politie. Ten tweede kan geweld tussen csv's worden ingezet om conflicten te beslechten, concurrentieposities op criminele markten te bevechten of om elkaar te beroven. Tot slot kan geweld tegen derden worden gebruikt ter afscherming van het samenwerkingsverband tegenover politie en justitie. Hierbij kan een onderscheid gemaakt worden tussen bedreiging van medeverdachten en getuigen enerzijds en medewerkers van politie en justitie anderzijds. Deze aspecten van het gebruik van geweld zullen in dit hoofdstuk aan de orde komen. Verder zal in dit hoofdstuk aandacht worden besteed aan geweld door Oost–Europese criminele samenwerkingsverbanden en aan geweld bij autodiefstal. Beide thema's werden in het NDB 2004 als dreiging aangeduid. Geweld dat inherent is aan delicten anders dan autodiefstal (zoals in het geval van overvallen) vallen dus buiten het kader van dit hoofdstuk.

In de volgende paragrafen zal worden behandeld: intern geweld van csv's (3.1), geweld tussen csv's (3.2), intimidatie en bedreiging van politie en justitie (3.3) en van getuigen en medeverdachten (3.4). De informatie in deze paragrafen is geheel ontleend aan de landelijke CBA's die gemaakt worden door de Dienst Nationale Recherche en de regionale CBA's die gemaakt worden door de meeste politieregio's. Daarna volgen een paragraaf over geweld door Oost–Europese criminele samenwerkingsverbanden (3.5) en tot slot een over geweld bij autodiefstal (3.6).

3.1 Geweld binnen criminele samenwerkingsverbanden

3.1.1 Inleiding

Binnen csv's kan geweld gebruikt worden om loyaliteit af te dwingen. Al eerder werd geconstateerd dat het gebruik van geweld aanmerkelijk varieert per csv. Sommige zijn meer geneigd om mensen te binden met positieve prikkels, zoals beloningen. Intern geweld wordt gerelateerd aan handel in harddrugs en aan organisaties met een verticale structuur. Naast fysiek geweld werden ook geldboeten en het terugsturen naar het land van herkomst als sanctie gehanteerd (DNRI, 2004d).

3.1.2 Aard

Geweld binnen csv's wordt ook wel aangeduid als 'verticaal geweld', ter onderscheiding van 'horizontaal geweld', waarmee geweld tussen csv's wordt aangeduid. Uit de CBA's komen verschillende vormen van geweldsgebruik binnen csv's naar voren. In de volgende paragrafen worden deze besproken.

Binden van hulpkrachten

Hierbij is sprake van het onder dwang opeisen van medewerking aan criminele bedrijfsprocessen, bijvoorbeeld als koerier of als verhuurder van ruimte voor wietkwekerijen. Hoewel dergelijke medewerking meestal uit financieel oogmerk wordt gegeven, is soms ook sprake van dwang. Zo werd iemand gedwongen om heroïne te smokkelen, omdat er anders iets met zijn familie zou gebeuren. In hoeverre verdachten dergelijke verhalen vertellen om hun eigen rol ogenschijnlijk kleiner te maken is niet duidelijk. Zo vertelde de eigenaar van een schuur dat hij bedenktijd had gevraagd over een verzoek om de locatie te verhuren voor de opslag van meubilair. Al voordat hij uitsluitsel had gegeven werden er vaten naar binnen gedragen. Hij zou zijn bedreigd toen hij daar wat van zei. Anders dan uit recent onderzoek naar voren komt, wordt in de CBA's melding gemaakt van geweld en intimidatie bij het verkrijgen van de medewerking van de verhuurders van 'wiethokken'. Overigens is dat lang niet altijd het geval.

"Eén kweker komt met een bandopname van een telefoongesprek aanzetten dat zijn organisator met hem voerde. Hij werd daarin verantwoordelijk gesteld voor het verlies van de plantage. Anderen vertellen over bedreigingen: 'Ze kwamen met een mes en een vuurwapen en zeiden dat ik en m'n gezin in problemen zouden komen. Ik wist dat ze iemand anders door zijn knie hadden geschoten en iemand een pink afsneden, dus die lui zijn tot alles in staat'.
Een ander werd aangezegd: 'Je weet wel wat er gaat gebeuren als…'. Iemand werd een kogel ter hand gesteld met de mededeling: 'cadeautje van X.'
Een andere kweker wiens plantage is leeggehaald krijgt mensen op bezoek die hem in het gezicht slaan en die kostbaarheden uit zijn huis halen met de mededeling 'dit is voor de geleden schade van de kwekerij'. Weer een ander vertelt: 'Ze zeiden dat als ik naar de politie zou gaan, ze een zak over mijn hoofd zouden trekken en me in de Maas dumpen'. Zover de politie bekend is, zijn dergelijke bedreigingen nooit tot uitvoering gebracht.
De indruk die uit het materiaal dat voorhanden is, oprijst is dat zich wel degelijk een criminele wereld op de achtergrond van de hennepteelt ontwikkelt.
Het niveau van dwang en intimidatie is echter niet zeer hoog" (Regiopolitie Limburg–Zuid, 2007).

Een ander voorbeeld van geweld binnen csv's is het laten rippen van eigen koeriers en hen te dwingen de geleden schade te vergoeden. Hierdoor ontstaat een schuld die alleen afgelost kan worden door nieuwe opdrachten aan te nemen. Het incasseren van de schuld gaat gepaard met bedreigingen[7].

In de CBA's wordt melding gemaakt van het bedreigen van personen binnen het csv op het moment dat zij hun werkzaamheden niet naar behoren hadden uitgevoerd. Mishandeling als negatieve sanctie is voorgekomen bij csv's (DNR, 2008b). Dit blijkt niet altijd een verstandige zet van de misdaadondernemers. Het is voorgekomen dat iemand zich zodanig bedreigd voelde dat hij naar de politie stapte en, voor lief nam dat hij zelf ook gestraft zou kunnen worden. Gewelddadige incidenten hebben meerdere malen tot ontdekking van csv's geleid (DNR, 2008b, p. 127–128).

Schade verhalen op medewerkers

In de hennepteelt komt het voor dat personen die ruimte verhuren voor de exploitatie van kwekerijen, verantwoordelijk worden gesteld voor de schade als de oogst door wat voor omstandigheden dan ook verloren gaat. Bij in gebreke blijven wordt gedreigd met geweld.

Binden van leden

Binnen enkele criminele samenwerkingverbanden worden dealers van 'boven in de organisatie' met geweld onder druk gezet als ze plannen hebben om het csv te verlaten. Mensen die zich vanwege financiële problemen laten ronselen als koerier, bijvoorbeeld voor de smokkel van XTC, worden onder druk gezet om niet te gaan 'praten'.

Wraak, verduistering en diefstal

Leden van csv's die beschuldigd worden van het verduisteren van geld of van diefstal van een deel van een drugstransport, worden soms met geweld tot de orde geroepen.

3.1.3 Omvang

Volgens het rapport *Criminele samenwerking* (DNRI, 2004d) wordt in 25 procent van de zaken van de EU–inventarisatie intern geweld aangetroffen. Volgens de Vervolgstudie deed intern geweld zich voor in 30 procent van de csv's (DNRI, 2006a). Hierbij moet wel aangetekend worden dat de inventarisatie niet

[7] Een ander voorbeeld van binding is het tegen woekerrente verstrekken van leningen die alleen terugbetaald kunnen worden door werkzaamheden voor het csv te verrichten.

compleet is en dat het niet duidelijk is of intern geweld een rol heeft gespeeld in de selectie van zaken die ingevoerd zijn.

3.1.4 Betrokken personen en groeperingen

De verhouding tussen beloning en straf bij het binden van medewerkers en het handhaven van de orde varieert per csv. Er is geen duidelijk verschil tussen de diverse criminele bedrijfstakken. Intern geweld is vooral gerelateerd aan drugsgroeperingen en aan csv's met een meer verticale organisatiestructuur (DNRI, 2004d). Ook in recente CBA's wordt dit bevestigd. Vooral in de hennepsector komt geweld voor, omdat daar veel mensen aan de periferie van csv's bij worden betrokken. Het gebruik van geweld tegenover ondergeschikten en hulpkrachten kan duiden op een hiërarchische organisatievorm.

3.1.5 Gevolgen voor de Nederlandse samenleving

Het grootste deel van het interne geweld van csv's onttrekt zich aan de waarneming van de bevolking en levert voor het merendeel daarvan geen directe bedreiging op. Iets anders wordt het als er openlijk geweld wordt gepleegd, zeker als daarbij wordt geschoten of als er doden vallen. Los van het feit dat dit zeer bedreigend is voor mensen die dicht in de buurt zijn, wordt de rechtsorde aangetast.

In een van de regionale CBA's wordt de hennepteelt genoemd als een specifiek probleem omdat er zoveel (gewone) mensen door in de richting van de criminaliteit worden getrokken:

> "Zij worden daar voor hun inkomen afhankelijk van of ze worden gedwongen daarover naar buiten geen mededeling te doen. Dit heeft voor andere terreinen van aandacht van de politie allerlei nog weinig doordachte consequenties. Welke invloed heeft de opkomst van zo'n illegale economie op de opgroeiende jeugd? Wat betekent dit voor het geweldsniveau in de regio? Wat betekent de welvaart door illegale middelen verkregen, voor de solidariteit en de moraliteit van de buurt?" (Regiopolitie Zuid–Holland–Zuid, 2007).

3.1.6 Criminaliteitsrelevante factoren

Intern geweld komt vooral voor bij csv's die zich bezighouden met drugshandel of die een verticale organisatiestructuur kennen. Ook de beschikbaarheid van wapens is van invloed op het gebruik van geweld, maar deze factor is voor het hele geweldsspectrum van belang.

3.1.7 Verwachtingen voor de toekomst

In de CBA's worden weinig uitspraken over de toekomst gedaan. Het is niet te verwachten dat het intern geweld van csv's af zal nemen. Dit lijkt vooral afhankelijk van de ontwikkelingen in de drugshandel en de hennepteelt. De belangen zijn groot en vooralsnog is enige regulering niet te verwachten.

3.2 Geweld tussen criminele samenwerkingsverbanden

3.2.1 Inleiding

Het gaat hierbij om geweld dat een rol speelt in de concurrentie en machtsverhoudingen tussen csv's. In het NDB 2004 was al sprake van ripdeals, liquidaties (afrekeningen) en het opeisen van protectiegeld of 'pacht' van minder machtige groeperingen. Met name van liquidaties, die meestal in de openbare ruimte plaatsvinden, gaat een grote dreiging uit. Hun aantal is de laatste jaren wel afgenomen. Alle aspecten van geweld waarvan eerder sprake was, komen nog steeds voor in de regionale CBA's en die van de DNR. Op veel plaatsen wordt gerefereerd aan gebruik van geweld door csv's, maar lang niet altijd wordt ingegaan op de specifieke achtergronden of oorzaken. De volgende paragrafen zijn dan ook vooral gebaseerd op passages waarin enige context wordt gegeven aan geweldstoepassing door criminelen.

3.2.2 Aard

Liquidaties

Van liquidatie is sprake als er dodelijk geweld wordt gebruikt waarvan het motief samenhangt met een of meer andere delicten (DNRI 2004d, p. 28–29). Of sprake is geweest van een liquidatie kan daarom strikt genomen pas worden vastgesteld als het misdrijf is opgelost. Het is mogelijk dat liquidaties niet altijd als zodanig worden herkend. Niettemin lijken liquidaties eerder in aantal af dan toe te nemen, de grote media–aandacht ten spijt. In het NDB 2004 werd op basis van gegevens van opsporingsteams gesignaleerd dat het aantal liquidaties aan het afnemen was. Ook in de recentere CBA's is slechts sporadisch sprake van liquidaties.

In relatie tot synthetische drugs zijn zeven personen geliquideerd. Onder hen waren vijf Chinezen, die vermoedelijk te maken hadden met precursorenhandel (DNR, 2008b, p. 131). Ook zijn er twee liquidatiepogingen geweest. Daarnaast was er nog een gijzeling en waren er vermoedelijk meerdere mishandelingen. De meeste van deze geweldsincidenten hebben zich in Noord–Brabant en Limburg voorgedaan.

Volgens een recent rapport hebben politiemensen de indruk dat een aanzienlijk deel van de gevallen van moord en doodslag in het zuiden van het land te maken heeft met hennepteelt (Spapens, Van de Bunt & Rastovac, 2007). Een analyse wees uit dat 10 procent van de onderzoeken waarbij een Team Grootschalig Onderzoek werd ingezet inderdaad te maken had met hennepteelt. De auteurs tekenen hierbij aan dat een aanzienlijk deel van de ernstige geweldsdelicten zich voordoet in de relationele sfeer. Anders gezegd: hennep speelt een belangrijke rol bij geweld tussen csv's.

Liquidaties trekken uiteraard de aandacht van politie en justitie. De liquidatiegolf van enkele jaren geleden in Amsterdam leidde tot een grootschalige aanpak van de groep rond topcrimineel Holleeder. Criminelen gaven met deze liquidaties een visitekaartje af en maakten duidelijk dat er met hen niet te spotten valt. Dit had waarschijnlijk een intimiderend effect op andere criminelen die van plan waren om met de politie te gaan praten. De liquidaties hebben er ook toe geleid dat er een roep vanuit het publiek en de politiek kwam om grootschalige middelen vrij te maken om de Amsterdamse topcriminelen aan te pakken.

Weliswaar is er niet veel sprake van liquidaties, maar niettemin zijn er criminelen actief die antecedenten hebben op dit terrein. In de CBA heroïne is hierover geschreven. Van een van de csv's die in beeld kwamen bleken enkele personen deel uit te maken die in Italië veroordeeld waren wegens liquidaties (DNR, 2008a, p 104).

Conflicten over toegang tot criminele markten

Bij de strijd om de macht worden uiteraard ook lichtere vormen van geweld ingezet. De CBA Brabant–Noord maakt melding van een 'territoriumstrijd' die gewoed heeft tussen een groep kampers en een hennepteeltorganisatie. Na een ripactie waren de betrokkenen ertoe overgegaan wapens te dragen en de kweeklocaties te beveiligen. Het rapport concludeert: 'momenteel lijken de territoriumgrenzen afgebakend te zijn' (Regiopolitie Brabant Noord, 2007). Of het hier nou gaat om werkelijke territoriumstrijd of vooral om onderlinge diefstal is niet helemaal duidelijk .

Over het algemeen lijken criminelen eerder geneigd om samen te werken dan om elkaar onderling te bestrijden. Dit leidt immers de aandacht af van de c*ore business*, groot geld verdienen met illegale activiteiten, en trekt bovendien de aandacht van de politie. 'De handel staat centraal, daar waar wenselijk wordt samengewerkt', zo staat in de CBA van de regio Gelderland–Midden. Een toename van onderling geweld is te verwachten als de trend van het rippen van elkaars wietoogsten verder doorzet. In deze regio was hiervan (nog) geen sprake (Regiopolitie Gelderland–Midden, 2007).

Afhandeling van conflicten over geld

Zoals gezegd is het in de criminaliteit niet mogelijk om een incassobureau in te schakelen wanneer een zakenpartner in gebreke blijft bij het betalen van geleverde waren of diensten. In zo'n geval wordt soms een gemeenschappelijke kennis ingezet om te bemiddelen. Als dat geen soelaas biedt, dan kan men nog proberen de achterstallige betaling te innen door te dreigen met geweld. Dit komt dan ook geregeld voor. Sommige csv's deinzen er niet voor terug om personen die een relatie hebben met andere csv's (of familieleden of vrienden) te gijzeen tot de betaling (of de levering) geregeld is. De CBA Haaglanden maakt melding van een zaak waarbij incasso overgaat in afpersing. Toen bleek dat bij de schuldenaar niets te halen viel, werd de eigenaar van een bedrijf dat nog geld schuldig was aan de debiteur gesommeerd met geld over de brug te komen, al was dit bedrijf geen partij in de betreffende deal (Regiopolitie Haaglanden, 2007).

In de CBA's is melding gemaakt van criminelen die zich laten inhuren voor incassoklussen. Een gewelddadige reputatie is uiteraard een pre op deze markt. Een specifieke vorm van afpersing wordt gevormd door criminelen die bepaalde afnemers dwingen om alleen met hen in zee te gaan, onder dreiging met geweld. Hiervan is sprake in de CBA Heroïne.

De volgende passage uit de CBA Heroïne geeft een idee van de gewelddadigheid van csv's in deze branche:

> "Csv's hebben zich schuldig gemaakt aan ontvoering, intimidatie c.q. bedreiging, mishandeling, moord. Een voorbeeld van ontvoering is terug te vinden in het onderzoek Nummer. In dit onderzoek werd een vriend of partner van de leverancier van zijn of haar vrijheid beroofd als borgstelling voor de betaling van de verdovende middelen. De bedreigingen waren onder meer te relateren aan de zogenaamde incassopraktijken van sommige csv's. Maar ook werden personen binnen het csv bedreigd op het moment dat zij hun werkzaamheden niet naar behoren hadden uitgevoerd. In sommige gevallen werden zij mishandeld, zoals blijkt uit het onderzoek Zappen. Een voorbeeld van de moord is terug te vinden in het onderzoek Citroen. Uit dit onderzoek komt naar voren dat de leider – een Merseyside crimineel – van het csv tijdens zijn detentie in Nederland een Turk heeft doodgeslagen. Volgens zijn zeggen zou hij dit gedaan hebben uit zelfverdediging." (DNR, 2008a, p. 154)

Afpersing, pacht, protectie

Hoewel afpersing als een dreiging is genoemd in het NDB 2004, wordt er niet vaak melding van gemaakt in de CBA's. In de CBA Zeeland wordt melding

gemaakt van de arrestatie van Albanese criminelen die op de kade in Vlissingen een soort 'tol' vragen van mensensmokkelaars. Zij maken hierbij gebruik van messen. De smokkelaars moeten per gesmokkelde een bedrag (gesproken wordt van 100 euro) aan de Albanezen betalen, anders wordt hen de toegang tot de haven ontzegd. Ook criminelen uit voormalig Joegoslavië zouden zich met deze vorm van afpersing bezighouden. De onderzoekers zien dit als een nevenverschijnsel dat voortkomt uit mensenhandel (Regiopolitie Zeeland, 2007).

Een ander geval van afpersing betrof een groepering die de eigenaar van een henneplocatie sommeerde om 'een zeer fors bedrag' te betalen in verband met het huurcontract en een rekening voor illegaal afgetapte stroom' (Regiopolitie Haaglanden, 2007).

Rippen

De meest voorkomende vorm van geweld tussen csv's bestaat uit ripdeals. In de CBA's wordt op vele plaatsen gesproken over ripdeals, maar lang niet altijd wordt informatie over de context gegeven. Wellicht een teken dat men van doen heeft met een bekend verondersteld fenomeen.

Een bekende variant van ripdeals is dat afnemers van een partij drugs niet betalen, maar er met gebruikmaking van geweld met de drugs vandoor gaan. Er zijn csv's die dit als een nevenactiviteit naast hun eigen drugshandel hebben, maar ook zijn er csv's die zich hier meer op toegelegd hebben. Bij ripdeals wordt soms extreem geweld toegepast. In de CBA Heroïne wordt melding gemaakt van een geval waarbij uit het huis van een csv–lid 20 kg heroïne werd gestolen, waarbij een van de leden werd doodgeschoten (DNR, 2008a).

Een andere variant is het leeghalen van hennepplantages net voordat de eigenaren tot de oogst kunnen overgaan. Hierbij komt alleen geweld te pas als de daders worden 'overlopen'. Het gevaar van het rippen van oogsten leidt er toe dat eigenaren overgaan tot bewaking van de wietplantages, veelal met vuurwapens. De beveiliging van de plantages is eerder gericht tegen concurrerende criminelen dan tegen de opsporingsdiensten. Een factor die bij de hennepteelt het risico op rippen vergroot, is dat vaak vrij veel mensen, ook van buiten de csv's, noodgedwongen op de hoogte zijn van de activiteiten. Eigenaren van locaties die worden gehuurd om hennep te telen worden soms verdacht als er gerипt wordt en krijgen zodoende te maken met verticaal geweld. Het rippen gaat ook in de hennepbranche lang niet altijd stiekem. In de CBA's wordt melding gemaakt van overvallen op leden van andere csv's om hen de oogst of de opbrengst daarvan afhandig te maken. Hierbij wordt gebruik gemaakt van (soms zware) vuurwapens.

De CBA van de regio Zuid–Holland–Zuid maakt melding van schietpartijen binnen de Antillianengemeenschap in Dordrecht in 2005. Deze schietpartijen waren vermoedelijk terug te voeren op een ripdeal in een cocaïnezaak (Politieregio Zuid–Holland–Zuid, 2007).

Casus

In de woning van een facilitator zou een transactie plaatsvinden van veertig kilogram marihuana (waarde 120.000 euro) met vier Franse afnemers; met dezelfde afnemers had eerder eveneens een transactie plaatsgevonden van veertig kilogram marihuana (deze was waarschijnlijk bewerkt, want de Franse afnemers hadden geklaagd over de kwaliteit). De partij softdrugs was verpakt in twee tassen welke in een garagebox overgeplaatst zouden worden in één van de auto's van de afnemers (of dit de uiteindelijke kopers of koeriers waren, is overigens niet bekend). Alvorens de overdracht, is de tussenpersoon met één van de afnemers naar de woning en garagebox gereden om de partij te laten zien en wederzijds vertrouwen te bewerkstelligen. Echter, tijdens de transactie zijn de leden van het criminele verband bedreigd en beschoten met een vuurwapen door de afnemers waarbij de coördinator dodelijk verwond is.

(Regiopolitie Midden en West–Brabant, 2007)

Een specifieke manier van rippen wordt gemeld in de CBA Limburg–Zuid: criminelen gaan bij collega's op bezoek en doen zich voor als rechercheurs. Vervolgens nemen ze alles mee wat van hun gading is (Regiopolitie Limburg–Zuid, 2007).

3.2.3 Omvang

Over de omvang van geweld tussen csv's zijn geen cijfers voorhanden. De teneur in de rapportages is wel dat er sprake is van een aanzienlijk probleem.

3.2.4 Betrokken personen en groeperingen

In de CBA's is geregeld sprake van etnische groepen die actief zijn in een bepaalde criminele branche en daarbij ook geweld gebruiken. Volgens de CBA Heroïne zijn er twee groepen die de Nederlandse heroïnemarkt domineren, namelijk Turkse leveranciers en hun Britse afnemers. Beide groepen deinzen er niet voor terug om extreme vormen van geweld toe te (laten) passen, zoals gijzelingen, steek– en schietpartijen, bedreigingen, intimidatie en liquidaties (DNR, 2008a, p. 182).

In de precursorenhandel zijn leden van de Chinese criminele gemeenschap actief en de toepassing van geweld is daarbij nooit ver weg. In de onderzoeksperiode werden bij vier incidenten vijf Chinezen vermoord, waarbij volgens de CBA Synthetische drugs een verband is met conflicten in de precursorenhandel (DNR, 2008b).

Bij het rippen van wietkwekerijen komt geregeld geweld voor. Hierbij worden kampers genoemd en in de regio's Zuid–Holland–Zuid en Zeeland is sprake van Antillianen die zich hier mee bezig houden. Zoals eerder al aan de orde kwam, worden in de zuidelijke provincies liquidaties gepleegd in verband met de wiethandel. Over de kenmerken van de daders werd echter niets gerapporteerd.

Een bekende zaak in verband met de hennepkweek is nog die in Venray waarbij twee Marokkanen geprobeerd hebben een kwekerij te rippen. Waarschijnlijk zijn ze daarbij betrapt en vervolgens om het leven gebracht (Regiopolitie Limburg–Noord, 2007).

De regio Limburg–Zuid maakt melding van Antillianen die zich schuldig maken aan overvallen op adressen waarvan bekend is dat er betrokkenheid is met de wiethandel. Het gaat dan vooral om coffeeshophouders. Ook werd diverse malen een wiettaxi overvallen, nadat eerst een bestelling werd gedaan. (Regiopolitie Limburg–Zuid, 2007).

Eén groepering in Utrecht houdt zich naast de handel in hennep ook bezig met het rippen van hennepkwekerijen. Ze maken gebruik van warmtemeters om de locaties van de hennepkwekerijen vast te stellen. Het belangrijkste kernlid van deze groepering is van Surinaamse afkomst. Albanezen en criminelen uit het voormalige Joegoslavië worden genoemd in verband met afpersing van mensenhandelaren.

Al met al kan geen bepaald profiel, al dan niet op basis van etniciteit, worden geschetst van geweldplegers. Hoewel niet alle csv's even gewelddadig zijn, is in alle branches en groeperingen sprake van het gebruik van geweld.

3.2.5 Gevolgen voor de Nederlandse samenleving

Zolang het gebruik van geweld een intern aspect van het criminele milieu blijft, zijn de gevolgen voor de samenleving niet al te groot. Vooral van dreiging met geweld en afpersingen zal men niet gauw iets merken. Als er echter gewelddadigheden in de openbare ruimte worden gepleegd en als er geregeld berichten in (lokale) media verschijnen over moorden of liquidaties zal dit anders komen te liggen. Dan zullen onveiligheidsgevoelens toenemen.

Grootschalig geweld, zoals de liquidatiegolf in Amsterdam enkele jaren geleden wordt gezien als een ernstige ondermijning van de rechtsstaat. Zoals al eerder vermeld, lijkt er echter sprake van een afname van dergelijk geweld. Anderzijds worden recente moorden in Zuid–Nederland aan de hennepteelt gerelateerd.

3.2.6 Criminaliteitsrelevante factoren

In het algemeen wordt gesteld dat de kans op geweld tussen csv's toeneemt als er sprake is van grote belangen en nieuwe partijen een aandeel op de markt willen opbouwen. Bij de hennepteelt speelt een rol dat een aanzienlijk aantal personen op een of andere manier op de hoogte is en het is dan natuurlijk zaak er voor te zorgen dat iedereen zijn mond houdt.

De betrokkenheid van dienstverleners als notarissen en advocaten bij het crimineel milieu is genoemd als een risicofactor. Facilitering kan omslaan in een risico: als de dienstverlener niet meer van nut is voor de groepering dan kan hij een risico vormen omdat hij veel weet. In hoeverre hier sprake is van speculatie of dat er daadwerkelijk bedreigingen zijn geuit of geweld is gebruikt tegen vrijberoepsbeoefenaars wordt echter niet duidelijk.

Een respondent bij het OM merkt op dat de verhoogde inzet van capaciteit naar aanleiding van de liquidaties in het Amsterdamse milieu een nieuwe risicofactor kan genereren. Het OM zal zich telkens moeten afvragen of het bezig is om oude zaken op te lossen, dan wel nieuwe te creëren. Een verhoging van de opsporingsdruk kan er immers toe leiden dat sommige criminelen met de politie gaan praten, wat weer kan leiden tot gewelddadigheden.

De CBA Drenthe maakt melding van de stijgende wapenproductie als een criminaliserende factor. Door toenemende wapenproductie in Oost–Europa en steeds betere importmogelijkheden komen er in de regio meer wapens in de omloop.

3.2.7 Verwachtingen voor de toekomst

Gezien de grote variatie in onderling geweldsgebruik en in de daaraan gerelateerde factoren is het niet eenvoudig om uitspraken te doen over de ontwikkelingen in de komende jaren. Gebruik van geweld is voor criminelen een manier om conflicten op te lossen wanneer andere mogelijkheden niet het gewenste resultaat opleveren. Over de mate waarin csv's samen willen werken en onderling in een goede verstandhouding handel drijven is moeilijk een uitspraak te doen.

Geweld wordt lang niet altijd op basis van een rationele berekening toegepast. Het temperament van betrokkenen, die niet zelden een 'kort lontje' blijken te hebben, speelt een grote rol. Dit maakt de voorspelbaarheid van gewelddadigheden niet eenvoudiger.

Volgens de CBA Heroïne zijn de financiële belangen in de heroïnemarkt dusdanig groot dat een toename van geweld in de nabije toekomst niet uit te sluiten valt. Voor de andere branches geldt hetzelfde. Met name in de hennepteelt gaan de laatste jaren enorme bedragen om. In de CBA van de regio Brabant–Zuid–Oost wordt voorspeld dat '…steeds meer mensen mee willen liften op het snelle geld dat hier gemaakt wordt. Voor sommigen betekent dit dat men zich gaat mengen in meestal toch al langer bestaande en gevestigde orde van de georganiseerde criminaliteit. De geweldsspiraal zal ook binnen deze branche toenemen, niet in de laatste plaats omdat de 'deelnemers' vaak al gelouterde criminelen betreft uit andere criminele activiteiten'.

De multi–etnische samenstelling van het Amsterdamse criminele milieu zou kunnen leiden tot meer geweld: in sommige herkomstlanden ligt de drempel voor grof geweld lager. Bovendien zijn er veel en zware wapens beschikbaar.

3.3 Intimidatie en bedreiging van politie en justitie

3.3.1 Inleiding

Een mogelijke contrastrategie die door criminele samenwerkingsverbanden kan worden gevolgd is het frustreren van opsporingsonderzoeken door het bedreigen en intimideren van medewerkers van politie en justitie. Enkele jaren geleden zijn vooraanstaande officieren van justitie met de dood bedreigd, een van hen heeft zelfs enige tijd het onderzoek neergelegd. Dit is de afgelopen jaren niet meer gebeurd. Ook als er geen sprake is van concrete bedreigingen wordt door de politie een inschatting gemaakt van de dreiging die uitgaat naar bijvoorbeeld bepaalde officieren van justitie of onderzoeksleiders. Ze kunnen immers gevaar kunnen lopen zonder dat ze concreet worden bedreigd. Als belangrijke criminelen in het vizier komen gaat van deze situatie altijd een zekere dreiging uit. Zo werd bij het begin van het proces tegen Willem Holleeder een raket afgevuurd op het gerechtsgebouw. Hiervan gaat een dreiging uit, zonder dat duidelijk is tegen wie deze precies is gericht. Ook voelen leden van observatieteams zich soms bedreigd. Het komt voor dat criminelen hun nabijheid merken en overgaan tot intimidatie.

3.3.2 Aard

Medewerkers van justitie die beveiligd worden in verband met dreigende situaties, zijn meestal niet concreet bedreigd. De beveiliging vindt plaats op grond van risicoanalyses van het KLPD (en van de NCTB in geval van terroristische dreiging).

Concrete bedreigingen van officieren van justitie komen niet vaak voor. De afgelopen vier jaar zijn er geen concrete voorbeelden bekend bij het OM. Wel worden geregeld door afzonderlijke verdachten bedreigingen geuit. Een verdachte roept bijvoorbeeld bij zijn veroordeling uit dat hij de officier of de rechter 'nog wel weet te vinden'. De betrokkenen weten vaak niet hoe hier mee om te gaan. Het wordt als een soort beroepsrisico beschouwd en niet al te serieus genomen. Daardoor worden dergelijke uitingen niet altijd gemeld bij het speciale meldpunt dat het OM heeft ingericht.

Bij bedreigingen is het niet vanzelfsprekend dat de officier rechtstreeks benaderd wordt. Het kan ook zijn dat bij een loket of in een brief die een verdachte vanuit de gevangenis stuurt een bedreiging wordt geuit. Het is in dergelijke gevallen niet makkelijk om de betrokken bedreigde te gaan vertellen dat hij bedreigd wordt. Op dit vlak valt volgens een respondent bij het meldpunt nog winst te behalen. Overigens zijn de meeste bedreigingen niet gerelateerd aan criminele samenwerkingsverbanden, meestal gaat het om individuele gevallen.

Het vermoeden bestaat dat officieren bedreigingen tegen het thuisfront eerder zullen melden dan wanneer deze tegen henzelf gericht zijn. Dit soort bedreigingen komt zelden voor.

Tot op heden hebben bedreigingen geen succes, omdat zaken altijd zijn doorgezet. Er zou een nieuwe vorm van subtiele intimidatie in opkomst zijn, namelijk pogingen om de integriteit van justitie of van afzonderlijke medewerkers via de media in twijfel te trekken. In dit rapport wordt dit fenomeen gerekend onder de kop 'desinformatie' (zie paragraaf 5.2).

De FIOD–ECD meldt dat criminelen dreigen rechtszaken tegen individuele medewerkers aan te spannen. Op die manier willen zij schadevergoeding krijgen als reactie op onderzoeken naar financieel–economische delicten. Hoewel dit een tamelijk kansloze juridische onderneming zal zijn, gaat er een dreiging uit van het gegeven dat de betreffende crimineel kennelijk precies weet wie met zijn zaak bezig is.

3.3.3 Omvang

In het jaarbericht 2006 van het OM–meldpunt was sprake van 24 gevallen van concrete intimidatie, agressie of bedreiging en 15 gevallen van potentiële dreigingen, gericht tegen tien officieren. In totaal werden 34 officieren bedreigd. Aangezien niet alle bedreigingen worden gemeld, mag aangenomen worden dat het werkelijke aantal bedreigingen hoger ligt. Overigens zullen de ernstige gevallen wel worden gemeld.

Concrete gevallen van bedreiging uit het georganiseerde criminele milieu kwamen in 2005 en 2006 niet voor. In 2006 waren het vooral individuen die bedreigingen hebben geuit. Het ging bijvoorbeeld om veroordeelden die het niet eens waren met de strafmaat, een man die door zijn toekomstige straf niet bij de geboorte van zijn kind zou kunnen zijn en zelfs een slachtoffer die bedreigingen uitte omdat de officier een dader niet wilde vervolgen.
Csv's komen bijna alleen naar voren in de dreigingsinschattingen die gemaakt worden bij bepaalde risicovolle strafzaken.

Bedreigingen aan het adres van andere ambtenaren die bij justitie werkzaam zijn, worden vaak nog niet gemeld. Dit komt onder meer doordat de ernst van dergelijke bedreigingen moeilijk is in te schatten. Hoe serieus is de dreiging tegen een telefoniste die dertig tot veertig keer door dezelfde persoon gebeld wordt? Hoe vaak dergelijke situaties zich voordoen is niet bekend, maar het wordt wel van belang geacht om hier ook aandacht aan te schenken.

Enkele jaren geleden voorspelde de toenmalige officier van justitie Teeven dat bedreigingen zouden toenemen naarmate er grootschaliger en harder opgetreden zou worden tegen de georganiseerde criminaliteit. Deze voorspelling is niet uitgekomen. Er worden de laatste jaren belangrijke criminelen gepakt, maar het aantal bedreigingen is eerder af– dan toegenomen. Sinds twee à drie jaar is van directe intimidatie (en/of bedreiging) van officieren van justitie, rechters en politiemensen geen sprake meer.

3.3.4 Betrokken personen en groeperingen

Zoals gezegd gaat het bij de meeste concrete bedreigingen om individuele verdachten die in de woede van het moment iets roepen over een politie-medewerker, officier of rechter en is er geen crimineel samenwerkingsverband in het spel. Dat betekent niet dat van csv's geen dreiging uitgaat, alleen uit zich dat meestal niet in concrete dreigementen. Dat is wellicht ook minder noodzakelijk voor criminelen die een gewelddadig imago hebben gecultiveerd.

Het is moeilijk te zeggen wat voor personen in het algemeen achter bedreigingen zitten. De vraag is ook wie gevaarlijker is. Een veelpleger die niets te verliezen heeft kan even gevaarlijk of zelfs gevaarlijker zijn dan een criminele groep met een gewelddadige reputatie. Een nader onderzoek naar de achtergronden van verdachten die bedreigingen hebben geuit, valt buiten het kader van dit rapport.

3.3.5 Gevolgen voor de Nederlandse samenleving

Als intimidatie en bedreiging van medewerkers van Openbaar Ministerie en politie succes zou hebben, dan zou het vertrouwen in de rechtsstaat ernstig worden ondermijnd. In het verleden is wel schade aangericht, doordat een belangrijke officier van justitie zich tijdelijk terugtrok en vervanging geregeld moest worden. Hierdoor loopt een zaak al gauw vertraging op, maar de laatste jaren is dit niet meer voorgevallen.

3.3.6 Criminaliteitsrelevante factoren

Een risicofactor voor bedreigingen is de grote mediaprofilering van sommige officieren van justitie als *crime fighter*. Het beleid is tegenwoordig dat grote zaken worden gedaan door een team van officieren, zodat minder snel het risico bestaat van op de persoon gerichte animositeit tussen officieren en verdachten. Niettemin is er niet aan te ontkomen dat officieren die belangrijke zaken doen bekendheid krijgen en zij worden dan ook meestal beveiligd.

Ook het lekken van gevoelige onderzoeksinformatie door zowel onder– als bovenwereld kan een risico vormen voor individuele ambtenaren van politie en justitie. Hier wordt bijvoorbeeld gedoeld op advocaten die gemakkelijk informatie uit opsporingsdossiers naar de media kunnen laten lekken.

3.3.7 Verwachtingen voor de toekomst

Vergeleken met het NDB 2004 valt het aantal bedreigingen tegen medewerkers van politie en justitie mee. Niettemin wordt het alom terecht gevonden dat dit verschijnsel in 2004 als dreiging is gekwalificeerd. Het is niet uit te sluiten dat grote criminelen zich opnieuw verlaten op bedreiging van medewerkers, als ze dicht op de huis worden gezeten. Het feit dat recentelijk meer met teams van officieren wordt gewerkt, wordt gezien als een manier om het risico dat men bedreigd wordt, althans op individueel niveau, meer te spreiden.

3.4 Intimidatie en bedreiging van getuigen en medeverdachten

3.4.1 Inleiding

Criminelen die vervolgd worden door justitie hebben er belang bij dat mensen die weet hebben van hun activiteiten, zo veel mogelijk hun mond houden tegenover politie en justitie. Om te verhinderen dat verklaringen en getuigenissen worden afgelegd, wordt duidelijk gemaakt wat de mogelijke gevolgen zijn. De intimidatie van getuigen kan variëren van subtiele boodschappen, die juridisch nauwelijks als bedreiging zijn aan te merken, tot aan het stellen van een voorbeeld door een getuige te mishandelen of te vermoorden. Een criminele branche waar het bedreigen van getuigen tot de core business wordt gerekend, is de mensenhandel. Door middel van bedreiging (ook van familieleden of kinderen) wordt voorkomen dat slachtoffers weglopen en zich bij de politie melden. Het bedreigen van slachtoffers als getuigen komt beduidend meer voor bij mensenhandel dan bij andere criminaliteitstypen, het is inherent aan het delict. In andere criminele bedrijfstakken is bedreiging van getuigen en medeverdachten weliswaar minder evident, maar wel degelijk aanwezig. In recente onderzoeken naar grote csv's zijn mensen uit het milieu gevonden die wel wilden verklaren, maar geen verklaringen op papier wilden ondertekenen vanwege de dreiging die van de groeperingen uitging. 'Zwakke plek van potentiële getuigen is dat ze vrouw en kinderen hebben', zoals een respondent het plastisch uitdrukt.

3.4.2 Aard

Mensenhandel

"Ervan uitgaande dat slachtoffers en hun uitbuiters tegengestelde belangen hebben, vormen slachtoffers voor veel misdaadondernemers die zich bezighouden met mensenhandel vermoedelijk het grootste risico. In essentie kan de misdaadondernemer op twee manieren omgaan met het risico dat een slachtoffer hem aangeeft bij de politie: hij kan ervoor zorgen dat het slachtoffer aan zijn kant staat, samen tegen de politie, of hij kan met negatieve middelen, zoals opsluiting of geweld, zijn slachtoffers ervan 'overtuigen' niet naar de politie te gaan. Beide tactieken zijn gebruikt door de drieëntwintig bestudeerde dadercombinaties. Enkele groepen bedienden zich van een combinatie van beide. (.....) Door in ieder geval drie dadercombinaties zijn slachtoffers gewaarschuwd voor de politie of werd hen met het argument "de politie in Nederland is corrupt" ontmoedigd om naar de politie te stappen.

Door dadercombinaties 4 en 13 werd de politie tegenover de slachtoffers als tegenpartij afgeschilderd, voor wie de pooiers en de prostituees samen bepaalde zaken verborgen dienden te houden." (DNR, 2008c, p. 82).

Uit dit citaat blijkt dat slachtoffers van mensenhandel misleid of bedreigd kunnen worden, of beide tegelijk. Het komt dan ook voor dat slachtoffers van mensenhandel, die bij de politie in beeld komen, weigeren aangifte te doen. Vandaar dat in de CBA Mensenhandel wordt gesteld dat slachtoffers van mensenhandel als zodanig gezien moeten worden, ongeacht of zij zelf zeggen slachtoffer te zijn of zichzelf als zodanig beschouwen (DNR, 2008c, p. 60).

De relatie van de daders met de slachtoffers karakteriseert zich in sommige gevallen door een mengeling van intimiteit en angst. Veelal verblijven slachtoffers bij de verdachten thuis of overnachten ze op hun werkplek (CBA Mensenhandel, p. 88).

Voor de misleiding van slachtoffers wordt in sommige gevallen gebruik gemaakt van voodoo, met name bij vrouwen uit Afrika.

"Slachtoffers uit Nigeria en Malawi maken vaak gebruik van voodoopraktijken. Voodoopakketjes, bestaande uit lichaamseigen stoffen, zoals schaamhaar, stukjes van de vingernagels en bloed die van hen zijn afgenomen spelen in de macht over en de intimidatie van de meisjes een belangrijke rol (…). Bedreiging kan ook uitgaan naar de familie van de slachtoffers. Dit is onder mensenhandel een veelgebruikte machtsmethode." (Regiopolitie Drenthe, 2007, p. 52)

Drugs

Zoals al eerder aan de orde kwam, zijn er onder Zuid–Nederlandse producenten van hennep en synthetische drugs meerdere gewelddadige incidenten geweest waarbij ook doden zijn gevallen. Er zijn ook mensen gegijzeld en mishandeld. In de CBA Synthetische drugs worden dan ook zaken genoemd waarbij getuigen hun adres niet wilden geven uit angst voor represailles. In dergelijke gevallen is het niet nodig dat verdachten concrete bedreigingen uiten tegenover getuigen. Het imago, gevormd door berichten in de media, staat er borg voor dat getuigen zich bedreigd voelen (DNR, 2008b, p. 80–81).

Hoewel in andere CBA's rond drugs geen concrete voorbeelden worden genoemd, leidt het geen twijfel dat getuigen stevig in hun schoenen moeten staan om verklaringen af te leggen tegen cocaïne– of heroïnehandelaren.

Indirecte intimidatie

Van bepaalde criminelen gaat een grote dreiging uit, ook zonder dat zij iemand daadwerkelijk met concrete represailles bedreigen. Getuigen zullen er bijvoorbeeld niet op zitten te wachten dat de verdachte te weten komt wat zij precies vertellen in een getuigenverhoor bij de rechter–commissaris. Volgens respondenten bij de politie wordt het dan ook als intimiderend ervaren als advocaten hun opwachting maken bij dergelijke getuigenverhoren. Sommige medewerkers bij politie en justitie zien dit als een ernstig probleem: getuigen kunnen zo niet vrijuit spreken.

Een andere vorm van 'indirecte intimidatie' is het selectief lekken naar de pers. Direct na de moord op Thomas van der Bijl verklaarde een advocaat dat het slachtoffer met de CIE gepraat had en krantenberichten dat hij als bedreigde anonieme getuige zou gaan optreden werden niet tegengesproken. Ongeacht de bedoelingen van de advocaat zal de boodschap bij andere potentiële getuigen luid en duidelijk zijn overgekomen.

3.4.3 Omvang

Een indicatie van de omvang van het probleem van bedreiging en intimidatie van getuigen wordt gegeven door de groei van getuigenbeschermingsprogramma's in de laatste jaren. Hiervan worden geen exacte cijfers vrijgegeven, maar een betrokken respondent meldt dat er sprake is van een duidelijke stijging. Voor deze stijging noemt hij twee redenen. Enerzijds biedt de wetgeving sinds 1 april 2006 meer mogelijkheden. Anderzijds is het aantal zaken toegenomen, doordat de Dienst Nationale Recherche meer heeft geïnvesteerd in het aanpakken van grote csv's, waarbij zij zich in toenemende mate op de kernleden richt. Sinds enkele jaren is het merendeel van de 'klanten' van getuigenbeschermingsprogramma's dan ook afkomstig van de DNR, terwijl daarvoor het aandeel van (boven)regionale opsporingsonderzoeken groter was.

3.4.4 Betrokken personen en groeperingen

Uit de interviews en de CBA's ontstaat de indruk dat het aandeel van autochtone criminelen relatief groot is bij het bedreigen en intimideren van getuigen en medeverdachten. Met zekerheid is dit echter niet te zeggen omdat er geen systematisch onderzoek naar is gedaan. Het ligt voor de hand dat voor het bedreigen van personen een zekere mate van contact nodig is, een sociaal netwerk. Buitenlandse criminelen zullen hier in mindere mate over kunnen beschikken. Verder lijkt het erop dat het fenomeen in verband met allerlei delicten voorkomt, hoewel er in de ene CBA duidelijk meer over is geschreven dan in de andere.

De geïnterviewden bij het OM en de politie hekelen de rol van advocaten. Volgens hen stellen zij mensen aan gevaar bloot, bijvoorbeeld door de precieze planning van getuigenverhoren in de openbaarheid te brengen. Daardoor zou het gebeurd zijn dat een kroongetuige in een belangrijke zaak vlak voordat hij moest getuigen met de dood werd bedreigd.

3.4.5 Gevolgen voor de Nederlandse samenleving

Intimidatie en bedreiging van getuigen en medeverdachten kan ertoe leiden dat bepaalde verklaringen, die een belangrijke rol zouden kunnen spelen in de afloop van een proces niet worden afgelegd. Hierdoor zouden daders hun straf ten onrechte kunnen ontlopen, waardoor de rechtsstaat wordt geschaad.

3.4.6 Criminaliteitsrelevante factoren

Over de factoren die een rol spelen in het ontstaan van intimidatie en bedreiging valt weinig met zekerheid te zeggen. Een toename van de opsporingsdruk en de strafdreiging zou kunnen leiden tot een grotere frequentie van bedreiging van mogelijke getuigen. Bij sommige zaken staat of valt het bewijs immers met getuigenverklaringen. Het is dan zaak ervoor te zorgen dat mensen hun mond houden. In zekere zin is het bedreigen van verdachten dus te beschouwen als een belangrijke vorm van afscherming voor criminele samenwerkingsverbanden.

3.4.7 Verwachtingen voor de toekomst

In de interviews en in de CBA's zijn weinig aanknopingspunten te vinden voor het formuleren van toekomstverwachtingen omtrent bedreiging en intimidatie van getuigen en medeverdachten. De bestrijding van de georganiseerde criminaliteit zal de komende jaren onverminderd prioriteit krijgen. De verwachting is dan ook dat het fenomeen in omvang zal toenemen. Op dit moment is al sprake van een stijging van het aantal beschermde getuigen. Hierbij geldt ook dat het voor criminelen niet altijd nodig is om concrete bedreigingen te uiten. Medeverdachten die in de krant lezen over liquidaties, mishandelingen en anonieme getuigen weten waar ze aan toe zijn. Daarbij komt dat getuigenbeschermingsprogramma's waarbij betrokkenen met een nieuwe identiteit in een ver land zonder contact met familie en vrienden een nieuw bestaan moeten opbouwen, niet erg aantrekkelijk zijn.

3.5 Geweld bij autodiefstal

3.5.1 Inleiding

In het *Nationaal dreigingsbeeld 2004* (DNRI, 2004a) wordt geconcludeerd: 'het aantal autodiefstallen waarbij professionele stelersgroepen, veelal in reactie op betere beveiliging, gebruik maken van (dreiging met) geweld tegen personen neemt toe. De gevolgen hiervan kunnen als ernstig worden aangemerkt. Deze werkwijze vormt aldus een dreiging.' Vier jaar later is in het kader van het NDB 2008 bekeken of die dreiging werkelijkheid is geworden. In deze paragraaf wordt daarvan verslag gedaan. Eerst een begripsafbakening. Geweld bij autodiefstal wordt opgevat als geweld tegen personen, ten dienste van de diefstal van een auto. Met andere woorden: het gaat in deze paragraaf om carjacking en homejacking en niet om geweld tegen goederen. In een ander deelproject van het NDB – Georganiseerde vermogensmisdrijven – wordt uitgebreid aandacht besteed aan andere vormen van autodiefstal, waaronder autodiefstal door middel van woninginbraak, eventueel met geweld tegen goederen.

Carjacking is een bekende term geworden, vooral omdat het fenomeen in ons buurland België regelmatig voorkomt. Bij carjacking is sprake van 'met geweld of bedreiging met geweld tegen personen, buiten gebouwen, iemand dwingen tot afgifte van een voertuig' (De Miranda & Degen, 2004). Volgens kenners is carjacking een ideale methode om een auto te stelen. Je krijgt de sleutel direct in handen en de motor loopt al. Daar staat tegenover dat het ook een riskante methode is. De dader moet een directe confrontatie met een onbekend slachtoffer aangaan. Daarbij komt het risico dat de rechter carjacking mogelijk zwaarder zal bestraffen dan ´gewone´ autodiefstal.

Minder bekend dan carjacking, maar misschien nog wel bedreigender is het fenomeen homejacking. Hierbij gaat het om 'het met geweld of bedreiging met geweld tegen personen in een woning, kantoor of ander gebouw, iemand dwingen tot afgifte van voertuigsleutels en/of voertuig (De Miranda & Degen, 2004)'. Strafrechtelijk gezien is sprake van diefstal met geweldpleging en afpersing, strafbaar gesteld in de artikelen 312 en 317 van het Wetboek van Strafrecht. Bij artikel 312 neemt de dief de auto of de sleutels zelf weg (diefstal met geweld) en bij artikel 317 dwingt hij het slachtoffer tot afgifte (afpersing). Belangrijk verschil tussen carjacking en homejacking is dat carjacking plaatsvindt op de openbare weg en homejacking in een afgeschermde ruimte zoals een woning of een kantoor.

3.5.2 Aard

Literatuur over de fenomenen carjacking en homejacking is dungezaaid. De dienst Nationale Recherche Informatie (DNRI) heeft twee rapportages uitgebracht over autodiefstal. Het gaat om de rapportages *Stelen op bestelling; een onderzoek naar autodiefstallen door middel van woninginbraak en showroomkraak* en *Stelen op bestelling 2003; autodiefstal in georganiseerd verband*, van De Miranda en Degen (2001, 2004). Het gaat in deze rapportages niet zozeer om homejacking, maar dat komt wel ter sprake omdat woninginbraak of showroomkraak kunnen uitlopen op homejacking, bijvoorbeeld als de daders 'overlopen' worden door het slachtoffer. Uit diverse voorvallen is gebleken dat sommige daders er dan niet voor terugschrikken grof geweld te gebruiken. Bij het bedwelmen van bewoners met gas om vervolgens de autosleutels te stelen, is volgens de rechter sprake van gebruik van geweld, ook al is het volgens experts geen 'echte' homejacking.

Het lijkt erop dat 'zuivere' carjackings en homejackings, dus specifiek gericht op de auto nauwelijks voorkomen. Meestal is de auto bijvangst of wordt hij meegenomen om te vluchten. Het draait dus uit op een homejacking of carjacking, al was dat niet het misdrijf dat de dader voor ogen had. Homejacking is niets meer of minder dan een overval en carjacking is een straatroof tenzij het slachtoffer beroepsmatig onderweg is. In dat geval gaat het om een 'transportoverval'. In het Landelijk Overvallen en Ramkrakensysteem (LORS) dat wordt beheerd door de dienst IPOL, worden ook bepaalde gevallen van carjacking, homejacking en bedrijfsovervallen waarbij een auto is meegenomen vastgelegd. Bij veel van de overvallen is het de vraag of de overval gepleegd is om de autosleutels te bemachtigen of dat de auto een bijkomstigheid is. De volgende voorbeelden van homejacking komen uit het LORS.

Casus 1

"Slachtoffer 1 was samen met haar drie kinderen in de woning en deed de achterdeur open. Op dat moment stonden er drie gemaskerde mannen voor de deur die de woning binnendringen. Slachtoffer 1 wordt op een bank geduwd en er wordt naar geld en de kluis gevraagd. Slachtoffer 1 werd meegenomen naar de slaapkamer, waar zij werd geboeid met een elektriciteitssnoer. Zij kreeg een zak over haar hoofd. Daarna gingen de overvallers naar de kamer van de 18–jarige zoon (slachtoffer 2) die tv zat te kijken. Slachtoffer 2 zag dat een van de daders een klein pistool in zijn handen had. Slachtoffer 2 kreeg vervolgens een klap in zijn gezicht, werd met een elektriciteitssnoer aan handen en voeten geboeid. Hij kreeg eveneens een zak over zijn hoofd. Ook aan hem vroegen ze geld. Ook de twee

andere kinderen (slachtoffers 3 en 4) werden aan handen en voeten gekneveld met elektriciteitssnoer. Ook slachtoffer 3 zag dat een van de daders een pistool in zijn handen had. Slachtoffer 3 moest de afstandbediening van het hek laten zien. De daders hebben de woning doorzocht en namen sieraden, sleutels, enkele gsm's en een in de garage staande personenauto mee."

Casus 2

"Het slachtoffer maakte de achterdeur open en liep naar de los van de woning staande garage om daar een flesje bier te pakken. In de garage werd hij door twee gemaskerde mannen overvallen. Hij werd direct hard geslagen en overmeesterd. De vrouw des huizes lag net op bed toen haar man naar de garage liep. Zij hoorde lawaai en keek nog door het slaapkamerraam naar buiten. Op dat moment kwamen er twee gemaskerde mannen haar slaapkamer in rennen en gooiden haar voorover op bed. De vrouw werd geslagen en in gebroken Engels vroegen ze haar waar de "safe" was. Zij gaf aan dat de kluis in een kast zat naast de keuken. Toen zij naar de keuken werd geduwd zag ze dat haar man met geweld naar binnen werd geduwd. De daders eisten dat de vrouw de kluis openmaakte wat haar niet lukte. Vervolgens moest haar man de kluis open maken. Hierna moesten beide slachtoffers op de grond tegen het keukenblok aan gaan zitten. De daders haalden uit de kluis enige sieraden. Er zat geen geld in de kluis. De daders namen hiermee geen genoegen en wilden weten waar de tweede kluis was. De slachtoffers werden met bruine verpakkingstape geboeid en hen werd een mes op de keel gezet. Het mes kwam uit een messenblok dat op het aanrecht stond.
De slachtoffers probeerden duidelijk te maken dat ze geen geld in huis hadden, maar dat wilden de daders niet geloven. De slachtoffers zijn vele malen hard geslagen en geschopt. Dader 1 haalde een stroomstootapparaat uit zijn jas en bewerkte daar diverse malen de slachtoffers mee. Vervolgens werd de tape rond de benen van de vrouw des huizes los gemaakt en moest zij aanwijzen waar nog geld in huis lag. De vrouw kon ze uit een tupperware doosje nog 200 US dollar en 150 euro (3 x 50) geven. De daders namen hier nog geen genoegen mee en zeiden dat er nog een tweede kluis moest zijn, gezien het huis en interieur. Dader 1 pakte een pistool waar hij de vrouw des huizes mee bedreigde.
Na geruime tijd van bedreigen, slaan en bewerken met het stroomapparaat werd er onderling overlegd. De slachtoffers werden allebei naar de slaapkamer gebracht en daar opnieuw geboeid. Het horloge dat de heer des huizes om had werd hem afgenomen. Ze moesten een half uur blijven liggen voordat ze iemand mochten waarschuwen. Hierna hoorden de beide slachtoffers de daders wegrijden met bovengenoemde Saab. De daders kwamen echter na ongeveer vijf minuten al terug en begonnen de heer des huizes te slaan en de slaapkamer

te vernielen. Ook werd de telefoonkabel losgetrokken. Dader 1 pakte een horloge van de vrouw en zette het op 00.30 uur. Hij wees aan dat ze tot 1.00 uur moesten blijven liggen. Daarna vertrokken de daders."

Wat opvalt aan homejackings is dat ze doorgaans zeer gewelddadig verlopen. Uit meerdere onderzoeken waaronder dat van Kievit & Kaijen (2005), maar ook uit de gegevens in LORS komt naar voren dat het lijkt alsof de daders helemaal losgaan als ze eenmaal in de woning zijn. Met geweld proberen ze er achter te komen waar waardevolle spullen liggen in de woning, maar er wordt ook veel 'zinloos' geweld toegepast. Wat eveneens voorkomt is dat slachtoffers worden vernederd en seksueel geïntimideerd. De kans op letsel of op dood van het slachtoffer is groter dan bij een overval op een bedrijf.

In LORS worden behalve gegevens over homejackings ook gegevens geregistreerd over overvallen op bepaalde categorieën beroepsmatige transporten. Bij sommige van deze overvallen wordt de auto meegenomen door de overvallers waarmee het dus in feite carjackings zijn. Het valt op dat taxichauffeurs relatief vaak slachtoffer zijn. Veelal is dan sprake van een beroving door klanten die dan vervolgens ook de auto meenemen. Meestal worden de auto's later teruggevonden. In dat geval gaat het waarschijnlijk om een 'gewone' overval. De auto dient dan alleen als vluchtauto en is geen onderdeel van de buit.

3.5.3 Omvang

Carjacking is een misdrijf dat sterk tot de verbeelding spreekt. Zo was er begin 2007 veel commotie over een e–mail waarin —zogenaamd door de politie Rotterdam–Rijnmond— werd gewaarschuwd voor de 'nieuwste truc van carjackers'. Deze zouden zich voordoen als reizigers met autopech en ze zouden zich vooral ophouden naast de oprit van een snelweg. Als potentiële slachtoffers stoppen en uitstappen om te helpen, halen de carjackers een wapen te voorschijn en gaan ze er vandoor met de auto van het slachtoffer.
Het bleek echter een nepwaarschuwing (*hoax*) te zijn die al drie jaar in een e–mail op het internet circuleerde. De politie kreeg regelmatig telefoontjes van mensen die zich ongerust maakten.

Bij het verschijnen van het eerste NDB werd verwacht dat het met geweld ontvreemden van auto's in omvang zou toenemen, mede doordat nieuwe auto's steeds beter beveiligd worden. Professionele autodieven die het juist op dure nieuwe auto's gemunt hebben, zouden naar geweld grijpen als laatst overgebleven manier om auto's te kunnen stelen. Inmiddels is echter gebleken dat ook nieuwe auto's te stelen zijn zonder dat daar geweld aan te

pas komt. Volgens geïnterviewde experts doet zich een professionalisering onder autodieven voor, waardoor ze in staat zijn om de beveiliging van moderne auto's te omzeilen. Inmiddels stijgt het aantal diefstallen van nieuwe auto's zelfs enigszins. De 'noodzaak' voor het gebruik van geweld lijkt dus minder dan eerder gedacht. Wat volgens respondenten wel een probleem aan het worden is, is het aantal autodiefstallen door middel van een inbraak; de zogenaamde inbraakdiefstal. De indruk bestaat dat dit fenomeen in omvang toeneemt.

Carjacking komt voor in Nederland, maar experts die in het kader van dit onderzoek zijn geïnterviewd hebben niet de indruk dat het fenomeen in omvang sterk groeit. Er worden zoals gezegd geen specifieke cijfers bijgehouden, maar geschat wordt dat het er hooguit enkele tientallen per jaar zijn. Carjacking vindt voornamelijk plaats in de Randstad. Het gebeurt niet vaak dat een auto wordt teruggevonden. Waarschijnlijk gaan ze net als andere gestolen auto's via de Rotterdamse of Antwerpse haven naar Afrika of naar landen in Centraal– en Oost–Europa, aldus een medewerker van de stichting Aanpak Voertuigcriminaliteit (StAVC)[8].

Het Landelijk Informatiecentrum Voertuigcriminaliteit (LIV) is het expertisecentrum voor voertuigcriminaliteit en opsporingsbijstand[9]. Het is een centraal meldpunt en houdt gegevens bij over autodiefstal. Er worden echter geen aparte gegevens van carjacking en homejacking bijgehouden. Op basis van de LIV–gegevens zijn geen harde conclusies te trekken over de omvang van geweld bij autodiefstal, omdat niet alle politieregio's informatie aanleveren. Volgens het LIV komen carjacking en homejacking in Nederland nauwelijks voor. Carjacking zou iets vaker voorkomen, maar vaak gaat het dan om verslaafden die de auto kortstondig als vervoermiddel gebruiken om te scoren of om snel weg te komen. Dat het probleem van carjacking en homejacking soms groter wordt afgeschilderd dan het is, heeft te maken met definitiekwesties die al in de inleiding aan de orde kwamen (paragraaf 3.5.1).

In *Stelen op bestelling* gaan De Miranda en Degen (2004) in op het probleem om betrouwbare cijfers te krijgen. Autodiefstal door middel van woninginbraak en autodiefstal door middel van geweld worden niet als zodanig geregistreerd in

8 Deze stichting richt zich op de gezamenlijke aanpak van voertuigcriminaliteit en is een samenwerkingsverband tussen publieke en private partijen zoals onder meer de ministeries van Justitie, Binnenlandse Zaken en Verkeer en Waterstaat, de RDW, de Raad van Hoofdcommissarissen en het verbond van verzekeraars.

9 Het LIV is een publiek– en privaatsamenwerkingsverband tussen het KLPD, de RDW en de stichting VbV (Verzekerings–bureau voertuigcriminaliteit).

de systemen van de politie. Bij autodiefstal door middel van woningbraak is sprake van een zogenaamd dubbel delict: woninginbraak en autodiefstal. Van beide misdrijven worden aparte processen–verbaal opgemaakt en ze worden dus ook apart geregistreerd. Gaat het om homejacking of carjacking dan is sprake van diefstal met geweld of afpersing, afhankelijk van de vraag of de dief zelf met geweld of met bedreiging met geweld de auto of de sleutels wegneemt of het slachtoffer dwingt tot afgifte. Omdat het bij homejacking in feite gaat om een woningoverval zijn daar cijfers van te vinden in het LORS.

Bij carjacking is het lastiger om cijfers boven water te halen, behalve als het gaat om overvallen op beroepsmatige transporten waarbij een auto wordt buitgemaakt. Dat is echter maar een kleine groep. In de bedrijfsprocessensystemen van de politie kan binnen de categorie diefstal met geweld of afpersing wel gezocht worden op de term auto, maar het is niet zeker dat op die manier alle gevallen van carjacking gevonden worden. Naast het LORS kan gebruik gemaakt worden van HKS. HKS bevat alle aangiftecijfers en gegevens over bekende verdachten. Het systeem is niet geheel compleet omdat niet alle politieregio's het systeem goed vullen. HKS geeft inzicht in hoeveel auto's er zijn ontvreemd met gebruikmaking van geweld of afpersing. HKS is niet geschikt om te bepalen of het om georganiseerde of bovenregionale criminaliteit gaat. Met deze kanttekeningen worden hieronder enkele cijfers gepresenteerd om toch een indicatie van de omvang te geven.

In het LORS worden zoals gezegd gegevens bijgehouden van alle in Nederland gepleegde overvallen en ramkraken, dus ook woningovervallen. Volgens experts is LORS nagenoeg volledig, omdat het systeem centraal wordt gevoed en hiervoor bestaan goede procedures. Wel zou het probleem kunnen spelen dat niet alle misdrijven ter kennis van de politie komen, het zogenaamde *dark number*, maar dat wordt in dit geval niet hoog ingeschat. Het gaat om ernstige geweldsmisdrijven en veelal ook om materiële schadeposten waartegen veel mensen verzekerd zijn. Om die reden wordt het aannemelijk geacht dat meestal wel aangifte wordt gedaan. In tabel 3.1 is een overzicht te zien van het aantal woningovervallen waarbij twee of meerdere daders een voertuig hebben ontvreemd.

Tabel 3.1

Aantal auto's buitgemaakt bij woningovervallen					
Jaar	2002	2003	2004	2005	2006
Aantal	13	15	18	25	16

Bron: LORS

Over de geografische spreiding van de overvallen is op te merken dat dit fenomeen in Noord– en Midden–Nederland nauwelijks voorkomt. In Zuid–Nederland en de Randstad wel en dan in het bijzonder Rotterdam en Amsterdam. Zoals in de tabel te zien is, is er een piek in 2005 en dat komt doordat er dat jaar in de regio Amsterdam–Amstelland zeven homejackings zijn gepleegd. Limburg–Zuid sprong er eveneens uit met vijf overvallen. Als gekeken wordt naar de merken van de auto's, valt op dat ze sterk variëren. BMW is het enige merk dat er echt uitspringt. Het zijn over het algemeen niet de heel dure merken. Hier en daar een Porsche, maar ook een Peugeot 305, een Ford Ka en een Opel Vectra. Ongeveer de helft van de auto's wordt teruggevonden.

De informatie in HKS is beperkter dan in LORS. In LORS wordt een beschrijving van het misdrijf opgenomen, zodat na te gaan is of het ook inderdaad een carjacking of een homejacking is. Definities kunnen immers verschillen. HKS heeft geen vrij tekstgedeelte. Degene die het misdrijf invoert, bepaalt onder welk misdrijf het wordt geregistreerd. Om die reden is mogelijk sprake van overrapportage. Zoals al aan de orde kwam, komt het voor dat woninginbraken gericht op autosleutels worden gekwalificeerd als homejackings. Net als bij veel andere politiesystemen, is het natuurlijk wel de vraag hoe compleet het systeem is. Ook hier speelt, naast het probleem dat niet alle regio's HKS even goed vullen, dat er een *dark number* is.

Tabel 3.2

Totaal aantal car– en homejackings volgens HKS					
Jaar	2002	2003	2004	2005	2006
Poging	17	19	22	10	8
Meer daders	35	39	41	29	17
Erf–tuin	2	4	4	1	1
Openbare weg	69	80	92	71	43
Woning	3	5	5	3	3

3.5.4 Betrokken personen en groeperingen

Zoals uit het voorgaande blijkt, komt carjacking en homejacking in Nederland niet vaak voor. De volgende vraag is: wie is die enkele carjacker of homejacker in Nederland? Hoort hij tot een groep, een netwerk? In hoeverre bereidt hij zijn misdrijven voor? Is hij in meerdere regio's tegelijk actief? Volgens experts gaat het om twee categorieën daders:

1 Degene die uit is op de duurdere auto's, zoals BMW en Audi voor export naar bijvoorbeeld Afrika.
2 Degene die de auto's voor andere doeleinden gebruikt, zoals het plegen van een misdrijf of als goedkoop vervoermiddel.

Als er al sprake zou zijn van georganiseerde groepen die zich bezighouden met carjacking of homejacking voor het verkrijgen van dure auto's, dan ligt het voor de hand ze te zoeken in kringen die zich bezighouden met georganiseerde autodiefstal. Bij georganiseerde autodiefstal is sprake van een keten, waarin de verwerving van de auto's door middel van diefstal de eerste schakel is (Ferwerda, Arts, de Bie & van Leiden, 2005). Gebruik van geweld is te zien als een manier om auto's te verwerven, een modus operandi. Uit de opsporingsonderzoeken die de onderzoekers hebben geanalyseerd kwam naar voren dat de autosleutels in de meeste gevallen zijn verkregen via woninginbraak. Daders verschaffen zich toegang tot de woning hetzij door 'gaatjes boren', hetzij door de 'Bulgaarse methode', het breken van de cilinder. Het komt vaak voor dat de inbraak 's nachts wordt gepleegd terwijl de bewoners thuis zijn. Tot een confrontatie met de bewoners komt het meestal niet en van homejacking is dus geen sprake. In de studie van Ferwerda e.a. (2005) is sprake van één geval waarbij het leek of de bewoners zijn bedwelmd. Dit is het enige geval van geweld tegen personen dat wordt genoemd.

Kuppens e.a. (2006) deden onderzoek naar georganiseerde diefstal in de wegtransportsector. In dit onderzoek werd door experts opgemerkt dat veel dadergroepen er geen belang bij hebben om geweld te gebruiken. De gedachtegang hierachter is dat de politie mogelijk meer prioriteit geeft aan misdrijven waar geweld bij is gehanteerd. Misschien geldt dit ook voor dadergroepen die zich bezighouden met georganiseerde autodiefstal. Er is nog een reden om te twijfelen aan betrokkenheid van georganiseerde autodieven en dat is dat veel auto's worden teruggevonden. Uit de LORS–gegevens bleek al dat het niet overwegend de duurdere merken zijn die worden meegenomen. Het lijkt er dus niet op dat de weinige carjackers of homejackers in Nederland in de hoek van de georganiseerde autodiefstal moeten worden gezocht.

Blijft over de groep die de auto's voor andere doeleinden gebruikt, bijvoorbeeld om een ander misdrijf te plegen, om weg te komen na een misdrijf of als snel en goedkoop vervoer. Dat we in Nederland vooral met deze groep te maken hebben is aannemelijk. Steun voor deze stelling is eveneens te vinden in het feit dat veel auto's worden teruggevonden. De beschrijvingen in LORS wijzen in die

richting en ook experts menen dat carjackings het werk zijn van verslaafden die vlug willen scoren of anderen die om wat voor reden dan ook een vervoermiddel willen hebben, bijvoorbeeld voor *joyriding*. Na gebruik laten ze de auto weer ergens achter.

Een vraag die deels samenhangt met het dadertype is de vraag of het bij carjacking en homejacking gaat om bovenregionale vormen van criminaliteit. Is sprake van dadergroepen die in meer dan één politieregio actief zijn? Deze vraag is op grond van de beschikbare gegevens niet eenvoudig te beantwoorden. Uit de systemen is informatie over eventuele 'bovenregionaliteit' niet direct af te leiden. Gezien de categorie daders waar het waarschijnlijk om gaat, ligt het niet voor de hand dat zij bovenregionaal opereren. Voor woningovervallen geldt in elk geval dat het veelal lokale daders zijn die lokaal opereren, zo blijkt uit onderzoek van Kievit en Kaijen (2005). Er is een duidelijke stijging waar te nemen van woningovervallen, van 484 in 2002 naar 591 in 2004. In totaal zijn in 2004 bij die 591 overvallen 22 voertuigen weggenomen waarbij in 17 gevallen sprake was van homejacking. Uit het onderzoek kwamen geen indicaties van 'bovenregionaliteit' naar voren. De lijkt aannemelijk dat ook carjacking beperkt is tot het lokale en regionale niveau.

3.5.5 Gevolgen voor de Nederlandse samenleving

Carjacking en homejacking zijn zeer ernstige misdrijven. Zowel lichamelijk en geestelijk als financieel kunnen deze misdrijven zware gevolgen hebben voor de slachtoffers. De kans om in Nederland slachtoffer te worden van een dergelijk misdrijf is echter bijzonder klein en in die zin zijn de gevolgen voor de Nederlandse samenleving gering. Voor verzekeringsmaatschappijen is het een kostenpost, maar vergeleken bij andere posten is de omvang te verwaarlozen.

3.5.6 Criminaliteitsrelevante factoren

Er zijn twee belangrijke criminaliteitsrelevante factoren op dit terrein die aandacht verdienen. De eerste is het niveau van beveiliging van auto's. Dit kan zowel positief als negatief uitwerken op het aantal carjackings of homejackings. Naarmate het lastiger wordt een auto te stelen op de 'normale manieren' zou het geweldgebruik kunnen stijgen. Een recente ontwikkeling is dat het door *tracking & tracing* technieken eenvoudiger wordt om auto's te volgen en terug te vinden. Deze ontwikkelingen zouden tot een afname van carjackings en homejackings kunnen leiden, hoewel het niet ondenkbaar is dat professionele autodieven er in slagen de apparatuur uit te schakelen.

De tweede criminaliteitsrelevante factor die door respondenten genoemd werd is de verdere uitbreiding van de Europese Unie (EU). De volgende paragraaf gaat hier verder op in.

3.5.7 Verwachtingen voor de toekomst

Ferwerda e.a. (2005) hebben naast een analyse van opsporingsonderzoeken ook interviews gehouden met experts uit onder meer de autobranche, de overheid en de verzekeringswereld. Onder deze experts bestaat de angst dat er een verschuiving zal plaatsvinden naar gewelddadiger vormen van autodiefstal zoals carjacking of homejacking. Dit heeft te maken met de ontwikkelingen op het gebied van de technische beveiliging van auto's en op het gebied van de mogelijkheden van de opsporing. Autodiefstal zou wel eens van een objectmisdrijf kunnen evolueren naar een persoonsmisdrijf. Het is de vraag of dit gaat gebeuren. Deze vraag kan misschien worden beantwoord door te kijken naar dadercategorieën die zich nu bezighouden met autodiefstal zonder geweld.

Uit de literatuur komen een paar dadercategorieën naar voren. De georganiseerde autodiefstal is vooral geïnteresseerd in de duurdere auto's voor de export naar het buitenland. Zij stelen in mindere mate auto's om andere misdrijven mee te plegen zoals ramkraken, overvallen of drugstransporten. Volgens een respondent bij de politie daalt het aantal gestolen auto's, onder andere omdat dezelfde gestolen auto's meerdere keren voor misdrijven worden gebruikt. Er zijn weinig aanwijzingen dat daders die auto's stelen om andere misdrijven mee te plegen overgaan tot carjacking of homejacking. Het ligt niet voor de hand aan te nemen dat ze dat wel gaan doen naarmate de beveiliging toeneemt, zoals eerder wel is gesuggereerd. Moderne beveiligingsmiddelen bemoeilijken niet alleen gewone diefstal maar ook carjacking, bijvoorbeeld omdat technische voorzieningen de kans op het terugvinden van de auto vergroten. Daarnaast wordt ook opgemerkt dat de beveiliging tegen diefstal al jaren steeds geavanceerder wordt, maar dat autodieven er toch steeds weer in slagen deze te omzeilen. Een beveiligingsmiddel is nog niet uitgevonden of er circuleren op internet handleidingen om deze te saboteren.

Buiten de georganiseerde criminaliteit is er een groep minder professionele daders die auto's stelen als middel om andere misdrijven mee te plegen of die even een vervoermiddel nodig hebben. Zij stellen minder hoge eisen en nemen mogelijk hun toevlucht tot de wat oudere, minder goed beveiligde auto's. Hiervan zijn er voorlopig nog genoeg voorhanden. En ook voor hen geldt dat,

mochten ze aan carjacking van duurdere auto's denken, ze geconfronteerd worden met beveiligingsmaatregelen die carjacking lastiger maken.

Een medewerker van het LIV spreekt de vrees uit dat carjacking zal toenemen door de recente uitbreiding van de Europese Unie. Hij wijst erop dat carjackings in België vaak het werk zijn van Oost–Europeanen en Russen. Er lijkt geen reden te zijn waarom ze hun werkterrein niet zouden verleggen naar Nederland. Temeer daar de Belgische politie steviger optreedt dan haar Nederlandse collega's en de rechters in België zeker niet milder zijn dan in Nederland. Hier staat tegenover dat deze groepen al jaren actief zijn in België en dat ze nog steeds hun opwachting in Nederland niet hebben gemaakt. Een ander punt is dat de uitbreiding van de EU ook zorgt voor meer welvaart in de Oost–Europese landen. Waarom zou je iets van ver halen als je het ook dichtbij kan krijgen?

In het NDB van 2004 werd gesteld dat het aantal autodiefstallen met gebruik van geweld door professionele stelersgroepen zou toenemen. Dit zou gezien de ernst van de gevolgen voor de Nederlandse samenleving een dreiging vormen. Deze angst is nog niet bewaarheid geworden. Integendeel: het aantal carjackings en homejackings is eerder afgenomen dan toegenomen. Het ligt ook niet in de verwachting dat geweld bij autodiefstal de komende jaren een ernstig probleem gaat vormen. Wat mogelijk wel een bedreiging kan vormen zijn autodiefstallen gepleegd door middel van woninginbraak, waarbij slechts bij uitzondering geweld wordt gebruikt. Dit onderwerp komt aan de orde in het deelrapport Georganiseerde vermogenscriminaliteit.

4
Misbruik van ICT

4.1 ICT–piraterij

4.1.1 Inleiding

ICT–piraterij is in het NDB 2004 als volgt gedefinieerd: het illegaal kopiëren en verspreiden van cd's, dvd's, films, games, software en andere producten, waardoor auteursrechten worden geschonden. In het NDB 2004 is ICT–piraterij als een dreiging aangemerkt (DNRI, 2004a). ICT–piraterij berokkent economische schade bij branches die betrokken zijn bij het vervaardigen en verhandelen van deze digitale producten (computerbedrijven, muziek– en filmindustrie).

In deze paragraaf wordt de informatie over ICT–piraterij geactualiseerd. Hiervoor is gebruikgemaakt van open bronnen (kranten, internet) en informatiesystemen van de opsporingsdiensten (Herkenningsdienstsysteem HKS, navraag bij de Criminele Inlichtingeneenheid CIE, de EU–inventarisatie van csv's in het kader van het Europese Organised Crime Threat Assessment, OCTA) en er zijn diverse interviews gehouden met deskundigen van de politie en uit de branche.

4.1.2 Aard

Er dient onderscheid gemaakt te worden tussen *softcopy–* en *hardcopy–piraterij.* De softcopy's worden louter in digitale vorm verspreid, in formats zoals mp3, mp4, mpeg, divx en wav, voornamelijk met behulp van het internet via peer–to–peer (P2P), sharingsites, bittorrent, en andere websites. De hardcopy-piraterij betreft het kopiëren en verspreiden van games, muziek en films die gebrand of geperst zijn op een cd, dvd of andere 'drager'. Volgens een respondent bij de Stichting BREIN[10] was de verhouding medio 2007 in Nederland 10 procent hardcopy's en 90 procent softcopy's.

Veruit de meeste voorbeelden van illegale hardcopy's die in Nederland geproduceerd zijn, zijn de gebrande versies. De makers hiervan worden door experts uit de branche beschouwd als de krabbelaars op het vakgebied. Professionele piraterij van hardcopy–dvd's en cd's gebeurt door middel van

[10] De Stichting BREIN (Bescherming Rechten Entertainment Industrie Nederland) is door de branche opgericht om de strijd aan te binden met piraterij. Medewerkers werden geïnterviewd voor dit onderzoek.

persen. De productiekosten liggen beduidend hoger, maar de kwaliteit is aanmerkelijk beter. Deze geperste beeld– en geluidsdragers zijn voor een leek niet van echt te onderscheiden. Als wordt vermoed dat een drager illegaal geperst is, wordt deze door de opsporingsinstantie naar een instantie in Engeland gestuurd, waar men een soort 'vingerafdruk' kan achterhalen, een unieke code die elke persmachine op cd's achterlaat. Volgens respondenten bij de Stichting BREIN zijn er in Nederland tot nu toe maar twee van deze machines aangetroffen: de eerste eind jaren negentig en de laatste in 2007 in Velddriel (www.anti–piracy.nl, geraadpleegd september 2007). Voor de exploitatie ervan zijn grote investeringen noodzakelijk. Volgens informatie op de website van IFPI, het mondiale equivalent van de Stichting BREIN (www.ifpi.org) kost een machine minimaal 15.000 euro. De productie van dragers vereist bedrijfsruimte voor de machine zelf, de grondstoffen (grote zakken met kunststofkorrels) en het eindproduct. Alleen professioneel opererende piraten zijn dus in staat om een dergelijke productie op touw te zetten. In Nederland zijn zoals gezegd maar enkele van dergelijke productieplaatsen aangetroffen en in het meest recente geval ging het om een locatie die nog maar net functioneerde: er werd een grote voorraad grondstoffen aangetroffen, maar er waren heel weinig eindproducten. Voor grootschalige professionele productie van hardcopy's zijn verder in Nederland geen aanwijzingen gevonden. Wel werd enige tijd geleden een uit piraterij afkomstige partij dragers aangetroffen bij een bekende keten van platenzaken. Experts veronderstellen dat het hierbij gaat om een incident, een geval van onoplettendheid bij inkopers. Niets wees erop dat het om bewust beleid zou gaan.

Illegale hardcopy's worden, zeker als het om meer grootschalige handel gaat, in het buitenland geproduceerd. Voor de distributie, veelal in grote partijen, maakt men gebruik van de reeds bekende smokkelroutes, naast het 'normale' legale vervoer, bijvoorbeeld per zeecontainer. De waar wordt uiteindelijk aan de man gebracht via (zwarte) markten, bazaars en dergelijke of via verkoopwebsites (bijvoorbeeld E–bay). Wat betreft productie en distributie zijn experts het erover eens dat Nederland hierin geen belangrijke rol speelt.

Zowel hardcopy's als softcopy's kunnen in de hele wereld worden afgezet. Uiteraard gaat het distribueren van de hardcopy's moeilijker en beduidend minder snel en wordt er een veel kleinere groep potentiële afnemers mee bereikt. Het distribueren van de softcopy's is niet aan tijd en plaats gebonden: binnen een paar seconden kan op iedere plaats in de wereld gedownload worden, in het geval van P2P–websites veelal van meerdere plaatsen, verspreid over de wereld, tegelijk. P2P–websites bevatten als zodanig geen muziek of films die kunnen worden gedownload. Het gaat hier om een netwerk van

afzonderlijke internetgebruikers die een deel van hun eigen computer openstellen om onderling muziek en films uit te wisselen; de P2P–website faciliteert dit proces slechts. Hoewel de beheerders van deze sites door de amusementsbranche als criminelen worden beschouwd, zien ze zichzelf als slimme zakenmensen die een gat in de markt hebben ontdekt. De inkomsten uit de site worden niet gegenereerd door de piraterij zelf, maar door advertenties die op de veelbezochte sites worden verkocht.
Een andere vorm van digitale piraterij is de diefstal van nog in ontwikkeling zijnde versies van nieuwe computerspellen via het hacken van het netwerk van de producent. Anders dan bij P2P–websites staat het criminele karakter daarvan niet ter discussie. Na diefstal van een prereleaseversie van een computerspel kan deze op grootschalige wijze gekopieerd en verspreid worden, waarmee groot geld verdiend kan worden. Hiervan zijn in Nederland wel voorbeelden te vinden. Zo heeft de Nationale Recherche in april 2007 twee broers aangehouden die een computernetwerk binnendrongen van een internationale softwareproducent in Griekenland. Zij hadden het oogmerk om de testversie van een computerspel te stelen dat het bedrijf nog aan het ontwikkelen was, om hiermee geld te verdienen. Uit het onderzoek bleek dat deze hackers zich toegang hadden verschaft tot een twintigtal andere bedrijven, allemaal in de computer-spellenbranche. Vooralsnog zijn dit in Nederland de enige voorbeelden.

4.1.3 Omvang

Voor de schatting van de omvang van illegale markten zijn meestal weinig gegevens voorhanden. De belangrijkste bron is de hoeveelheid illegale materialen die door de opsporingsinstanties, in dit geval politie, FIOD–ECD en Stichting BREIN, wordt aangetroffen. Net zoals dit bij drugsmarkten het geval is, weerspiegelt deze hoeveelheid niet alleen de omvang van de illegale markt, maar ook de inspanningen van de opsporingsinstanties. Als de prioriteiten verschuiven, zal dit ook tot uiting komen in de cijfers over inbeslagnemingen.

Hardcopy's

Volgens geïnterviewde experts heeft de bestrijding van piraterij geen hoge prioriteit bij de Nederlandse opsporingsdiensten. Bij de FIOD–ECD bestond een aantal jaren een Team Piraterij, maar dit blijkt te zijn opgeheven. Volgens deze respondenten worden door de politie en de douane de laatste jaren weinig gerichte opsporingsactiviteiten ontplooid op het gebied van hardcopypiraterij in Nederland. Bij de politie wordt bevestigd dat zaken die te maken hebben met hardcopy's worden doorgegeven aan de branche zelf (in dit geval aan de Stichting BREIN). Als piraterijdragers worden aangetroffen, betreft het veelal 'bijvangst'. Zo werden in mei 2007 in Tilburg enige duizenden illegale dvd's

gevonden tijdens een doorzoeking in het kader van een onderzoek naar heling. Ook wordt opgemerkt dat de grootschalige import van dragers moeilijk te bestrijden is. Hierbij doen zich dezelfde problemen voor als bij de bestrijding van de import van bijvoorbeeld drugs. "Als het namaken op grote schaal gebeurt, is de handhaving moeilijk. Als er op een dag 50.000 containers de haven van Rotterdam binnenkomen, zijn die niet voor honderd procent te controleren", zegt bijvoorbeeld Josaputra (2005).

De bestrijding van piraterij van auteursrechtelijk beschermde materialen (*content*) is in Nederland voor een belangrijk deel neergelegd bij de Stichting BREIN. Deze heeft een eigen opsporingsafdeling, die bijvoorbeeld op markten speurt naar illegale kopieën. De plaatselijke politie ondersteunt hen hierin. Betrapte handelaren moeten hun spullen inleveren en er wordt hun een contract voorgelegd waarin zij beloven zich niet meer met deze handel in te laten. Bij grote partijen of recidive wordt de zaak overgedragen aan de FIOD–ECD. Recentelijk is de inzet bij de Stichting BREIN echter sterk verschoven naar de privaatrechtelijke aanpak van de verspreiding van softcopy's, door de beheerders van sharingsites.

Zoals eerder aan de orde kwam, zijn de illegale hardcopy's die in Nederland geproduceerd zijn, meestal de gebrande versies. Hiervan worden veel kleinere series gemaakt dan van de geperste variant. De aangetroffen voorraad bij inbeslagname is dan ook veelal niet groot: meestal gaat het om enige tientallen tot honderden, en zeer incidenteel om enkele duizenden, aldus respondenten bij de Stichting BREIN. Uiteindelijk zijn er bijvoorbeeld in 2006 tussen vijftien en twintig mensen aangehouden die hun cd's en dvd's verhandelden via internet of zwarte markten. In 2007 waren het er nog minder, ook doordat de Stichting BREIN haar pijlen heeft gericht op de beheerders van sharingsites. Het machinaal persen van illegale dragers komt in Nederland maar sporadisch voor. Zoals hiervoor al vermeld is, zijn er slechts enkele machines aangetroffen.

Softcopy's

De bestrijding van de verspreiding van softcopy's via P2P–websites en dergelijke wordt civielrechtelijk aangepakt door de Stichting BREIN (zie ook paragraaf 4.1.6). Aangezien het hier om bestanden gaat die via internet worden uitgewisseld, is het moeilijk uitspraken te doen over aantallen.
Door het Team High Tech Crime van de NR zijn enige successen geboekt op het gebied van de (poging tot) diefstal van broncodes van nog niet in omloop zijnde computerspellen.

4.1.4 Betrokken personen en groeperingen

In het NDB 2004 is gerapporteerd dat de meer 'traditioneel criminele elementen', die zich veelal bezighouden met een scala aan criminele activiteiten, zich naar alle waarschijnlijkheid ook op het terrein van ICT–piraterij begeven. Uit mediaberichten en interviews met experts is inderdaad gebleken dat de handel in hardcopy's niet altijd op zichzelf staat. Zo zijn er bij opsporings-onderzoeken naar andere delicten (heling, hennepkweek) ook verschillende keren illegale dvd's of cd's aangetroffen.

Volgens internationale rapporten zijn er mondiaal diverse vormen van criminele samenwerking op het gebied van piraterij te onderscheiden, van eenlingen en 'gelegenheidsduo's' tot aan zeer professioneel ingestelde groeperingen. In China, *piracy*–wereldmarktleider, wordt de grootschalige productie van hardcopy's voornamelijk beheerst door criminele samenwerkingsverbanden, waarvan gezegd wordt dat ze strak georganiseerd en gewelddadig zijn. Ook over de andere landen, zoals Rusland, Oost–Europese landen, Brazilië, Mexico en Thailand wordt gesteld dat productie en distributie worden beheerst door criminele samenwerkingsverbanden (Phillips, 2005; IFPI, 2007). Volgens een geïnterviewde uit de filmbranche is de Napolitaanse maffia (Camorra) betrokken bij hardcopy–piraterij.

In Nederland lijkt van georganiseerde criminaliteit in verband met piraterij echter weinig sprake. Dit blijkt ook uit de al genoemde bevinding dat professionele productie van dragers met behulp van persmachines zich in Nederland voor zover bekend slechts enkele keren heeft voorgedaan. Een ander aspect dat duidt op georganiseerde criminaliteit in deze branche, is dat er soms sprake is van (dreiging met) geweld. In internationale rapportages zijn voorbeelden genoemd van het innen van protectiegeld bij houders van marktkraampjes (Epstein, 2005; IFPI, 2006). Er zijn geen aanwijzingen voor dat deze praktijken zich ook in Nederland voordoen. Onderling geweld tussen betrokken groeperingen lijkt zich evenmin voor te doen.

Hoewel een enkele respondent in de amusementsbranche stelde dat de bedrijven die P2P– en bittorentsites hosten als criminele organisaties beschouwd moeten worden, wordt hierover door andere respondenten veelal genuanceerder gedacht. De bedrijven maken hun winst voornamelijk door het verkopen van advertentieruimte op de sites waarop bestanden worden uitgewisseld. Deze uitwisseling is uiteraard illegaal. Van deelname van 'traditionele' criminele samenwerkingsverbanden, die zich eerder al met andere delicten bezighielden, is in deze branche tot op heden niets gebleken. Hierin

wijkt Nederland dus af van sommige andere landen, zoals Italië, waar volgens sommige bronnen de Camorra zich ook met piraterij bezighoudt.

Onlangs heeft de rechter bepaald dat een samenwerkingsverband van vijf personen dat zich bezighoudt met het faciliteren van P2P–websites, niet beschouwd kan worden als een criminele organisatie in de zin van artikel 140 Wetboek van Strafrecht. Overigens zijn deze personen wel veroordeeld vanwege het schenden van auteursrechten, omdat ze schuldig werden bevonden aan het bieden van gelegenheid om bestanden illegaal op de sharingsites te plaatsen; daarmee faciliteerden ze het schenden van auteursrechten.

Onlangs was er in ieder geval sprake van inmenging door een csv, toen Russische criminelen ICT–studenten van de Universiteit Twente) ronselden. Twee hackende broers werden eveneens door de Russen geronseld. Zij kregen de opdracht om in te breken in de systemen van een Griekse gamefabrikant om broncodes te stelen.

4.1.5 Gevolgen voor de Nederlandse samenleving

Piraterij heeft een brede economische impact. Producenten lopen inkomsten mis, lokale markten hebben te lijden onder oneerlijke concurrentie door illegale producten, overheden lopen belastinginkomsten mis en de werkgelegenheid wordt negatief beïnvloed in de branches die door piraterij getroffen worden. Het omzetverlies wordt enigszins gecompenseerd door een heffing op lege schijfjes.[11]

Met piraterij wordt door criminelen geld verdiend dat weer voor andere criminele activiteiten kan worden aangewend. De gemakkelijke beschikbaarheid van illegale content ondermijnt de bereidheid van het publiek om voor het materiaal te betalen.

Ook kan het imago van Nederland in het buitenland in het geding zijn, doordat ons land geassocieerd wordt met een deel van de hostingsites voor uitwisseling van films en muziek. Overigens komt volgens internationale rapporten ICT–piraterij in Nederland niet méér voor dan in de ons omringende landen (BSA, 2006; IFPI, 2007).

Een internationaal rapport vermeldt ook gevolgen voor degenen die illegale *content* en software gebruiken. Zo zou bij bedrijven die illegale software

[11] Website van Stichting Thuiskopie, www.thuiskopie.nl

gebruiken, de bedrijfscontinuïteit op het spel staan (Business Software Alliance, 2006). Door de illegale producten zou een verhoogde kans op storingen, hacken en andere problemen ontstaan. Doordat de ondersteuning van de fabrikant ontbreekt, ontvangen deze bedrijven geen updates van hun software.

4.1.6 Criminaliteitsrelevante factoren

Goede infrastructuur en veel gebruikers zonder morele bezwaren

Nederland kent een goede infrastructuur met snelle breedbandverbindingen en een groot aantal internetgebruikers. Veel mensen hebben de mogelijkheid om zelf muziek, films en games gratis te downloaden, waardoor ze deze niet meer hoeven te kopen. De software van de sharingsites is ook behoorlijk verbeterd, wat het bedieningsgemak ten goede is gekomen. Het is niet meer nodig over veel ICT–expertise te beschikken om muziek of films te downloaden. Daarnaast zijn de opslagkosten (op de harddisks) afgenomen. Kortom, het verspreiden van de softcopy's is tegenwoordig veel eenvoudiger en sneller dan enige tijd geleden. Hierdoor is Nederland een aantrekkelijk land voor de vestiging van hostingsites voor filesharing en P2P. Naast de goede infrastructuur bestaat er volgens de Stichting BREIN ook een aanzienlijke 'binnenlandse markt'. Uiteraard bedienen de sites gebruikers in heel de wereld, maar de 1,7 miljoen downloaders van muziek, games en films in Nederland alleen vormen toch een aantrekkelijke thuisbasis. Bij veel jeugdigen (de voornaamste gebruikers) bestaat weinig moreel bezwaar tegen downloaden, onder andere omdat er niet direct een aanwijsbaar slachtoffer te zien is. Er wordt veel gedownload en daarvoor zijn ook vele sites beschikbaar.

Lage prioriteit in de opsporing, maar nieuwe mogelijkheden in civiele wetgeving

Tot voor kort was Nederland voor hostingsites ook interessant vanwege het feit dat de opsporingsdiensten nauwelijks optraden tegen het faciliteren van dergelijke sites. Vooral een gerechtelijke uitspraak uit 2007 (Stichting BREIN – KPN, Hof Amsterdam, 5 januari 2007) heeft de mogelijkheid geboden om ook tegen de facilitators van de websites op te treden. Internetserviceproviders (ISP's) zijn door deze uitspraak verplicht persoonsgegevens van webhosters vrij te geven aan belanghebbenden, indien er auteursrechten geschonden zijn, en deze websites op hun verzoek te sluiten.

Niet alle ISP's werken echter mee aan de verstrekking van de persoonsgegevens van facilitators van de hostingsites. Stichting BREIN merkt hierover op de website op: "Nederland staat bekend als veilige haven voor illegale sites, dat komt mede door een aantal hostingproviders die het niet zo nauw nemen. Daar moet

verandering in komen." (www.anti–piracy.nl, oktober 2007). Dat kan door strafrechtelijke aanpak. Deze werd bijvoorbeeld toegepast toen de bittorrent–site OiNK uit de lucht werd gehaald, met medewerking van FIOD–ECD. Het kan ook door *civielrechtelijk optreden*. Op 22 oktober 2007 werd een van de grootste illegale videostreamingsites ter wereld (Tv–links.co.uk) op vordering van Stichting BREIN door de ISP Leaseweb afgesloten. De beheerder is in Engeland aangehouden. Door dergelijke acties wordt geprobeerd Nederland onaantrekkelijk te maken voor ICT–piraterij. De aanpak van Stichting BREIN en FIOD–ECD werpt vruchten af: de filesharingwebsites die Nederland aantrekkelijk vonden vanwege de faciliteiten, vertrekken uit Nederland en gaan naar Canada, Rusland en andere landen.

Dit neemt niet weg dat er nog steeds een aantal hostingsites bestaan die beheerd worden door Nederlanders en een mondiale impact hebben, zoals de website Mininova.org; deze staat in de top tien van wereldwijd meest bezochte sites.

Hardcopy in de verdrukking

Een argument voor het kopen van een cd in de winkel is dat er een hoesje bij is met informatie en bijvoorbeeld songteksten. Om deze reden wordt door sommige artiesten veel aandacht besteed aan het uiterlijk van de dragers. Op deze manier wordt geprobeerd de omzet van legale dragers te bevorderen. De meeste gebruikers die niet het volle pond willen betalen (bijvoorbeeld voor het doosje), zijn in staat te downloaden. Er is daardoor nog maar een kleine groep die bereid is geld te betalen voor een illegale hardcopy. Hiervoor moet, anders dan voor softcopy's die via internet verspreid worden, betaald worden, omdat ze nog steeds op de 'ouderwetse' wijze getransporteerd worden, met de bijkomende kosten, vergrote pakkans en verlies door diefstal (McIllwain, 2005).

Daarbij komt dat sinds 2004 de opsporingsdiensten, vooral de Stichting BREIN, succesvol geweest zijn in de aanpak van de hardcopypiraterij. Dit heeft erin geresulteerd dat er van grootschalige illegale cd– en dvd–handel in Nederland nauwelijks sprake is. Ten aanzien van hardcopy's is de pakkans groter dan in het begin van deze eeuw. De medewerkers van Stichting BREIN struinen markten en braderieën af op zoek naar illegale cd's en dvd's. Bij het constateren van een overtreding wordt de politie ingeschakeld. Deze houdt de verdachte aan en de illegale *content* wordt in beslag genomen en vernietigd. Tot een aantal van 2500 cd's of dvd's handelt de Stichting BREIN via civielrechtelijke weg af. Bij aantreffen van hogere aantal wordt de zaak overgeheveld naar de FIOD–ECD. Dit doet men door de handelaar een overeenkomst te laten tekenen waarin hij zich ertoe verplicht voorgoed te stoppen met de handel in of productie van illegale dvd's of cd's, met een dwangsom van 500 euro per geval. Bij recidive zal de Stichting

BREIN direct proberen deze dwangsom te innen. Bij ernstige recidivisten is het door een gerechtelijke uitspraak (Rechtbank Amsterdam, 24 april 2007) zelfs mogelijk om deze personen te gijzelen. Medewerkers van de Stichting BREIN gaven aan zelf ook verrast te zijn door deze uitspraak. Tot november 2007 is dit middel nog niet ingezet.

Beveiliging van content

In het verleden dacht men het kopiëren tegen te kunnen gaan door het gebruik van kopieerbeveiligingen. Een voorbeeld hiervan is DRM–technologie. Inmiddels is gebleken dat dergelijke technieken niet het gewenste resultaat hebben, doordat ze technisch vrij eenvoudig te omzeilen zijn. Daarnaast werkt de techniek in vele gevallen niet, of heeft deze ongewenste gevolgen zoals het niet functioneren van cd's of zelfs defecte afspeelapparatuur. Hierdoor is er bij het publiek weinig vertrouwen in deze technieken. Daarom wordt de laatste tijd weinig (of niet) geïnvesteerd in dergelijke beveiligingen.

4.1.7 Verwachtingen voor de toekomst

De hardcopypiraterij lijkt voor Nederlandse csv's een weinig aantrekkelijke criminele branche om in te investeren. In het criminele metier zijn eenvoudiger methoden om snel geld te verdienen. Waar wel geld in te verdienen valt (voornamelijk door reclame–inkomsten), is het beheren van sites die de bestandsuitwisseling faciliteren. Ook deze sites worden in Nederland tegenwoordig met succes aangepakt. Dit heeft tot gevolg dat, ondanks goede faciliteiten, Nederland steeds onaantrekkelijker wordt en men deze sites naar het buitenland (Canada, Rusland) verhuist. Voor de hostingsites geldt dat het expertise en investering vereist om zo'n site te beginnen en in de lucht te houden. Het is de vraag of csv's hierin zouden willen investeren.

4.2 Phishing

4.2.1 Inleiding

In het NDB 2004 werd phishing gedefinieerd als een werkwijze waarbij gebruik wordt gemaakt van een misleidende website. Heden ten dage wordt deze werkwijze beschouwd als een traditionele vorm van phishing. Er zijn andere typen vistechnieken gangbaar geworden, waarbij geen misleidende website meer nodig is. In navolging van de vervolgstudie NDB 2006 (DNRI, 2006a) is ervoor gekozen om phishing te omschrijven als:

Het met behulp van digitale activiteiten wederrechtelijk toe–eigenen en/of gebruiken van (delen van) de identiteitsgegevens van een internetgebruiker, met het doel om een strafbaar feit te begaan waarvan de internetgebruiker het slachtoffer is.

Voor het onderzoek naar phishing zijn de volgende werkzaamheden verricht:
- Raadplegen van literatuur en het internet.
- Raadplegen van Blueview, het landelijk bevragingssysteem waarmee gegevens uit handhavings– en opsporingssystemen opgezocht kunnen worden.
- Interviews met experts binnen opsporingsdiensten, waaronder het Team High Tech Crime en Team Digitale Expertise van Dienst Nationale Recherche en medewerkers van Govcert.NL.
- Tijdens een vergadering van het Financial Institutions–Information Sharing and Analysis Center (FI–ISAC) van de Nederlandse vereniging van Banken is met de aanwezigen een vragenlijst doorgenomen door de onderzoekers[12].
- Bijwonen van de bijeenkomst: Payment card fraud expert meeting, door Europol in Den Haag georganiseerd op 20 september 2007.

4.2.2 Aard

Het misleiden van internetgebruikers om hen ertoe te bewegen persoonlijke gegevens prijs te geven, kent vele vormen. In de vervolgstudie NDB uit 2006 werden drie verschijningsvormen van phishing onderscheiden (DNRI, 2006d):
- traditionele phishing;
- pharming;
- spy–phishing.

In een traditioneel geval van phishing wordt een e–mail verzonden naar internetgebruikers. De e–mail lijkt afkomstig van een financiële instelling of een bedrijf. De ontvanger wordt ertoe overgehaald om via een link in de e–mail een nagemaakte website te bezoeken en op die website persoonlijke gegevens in te typen.

Het benaderen van potentiële slachtoffers gaat op een steeds persoonlijkere manier (*spear–phishing*). Er wordt bijvoorbeeld een phishingmail gestuurd naar medewerkers van een bedrijf, waarbij het lijkt of er intern een e–mail is verstuurd (Binational Working Group on Cross–Border Mass Marketing Fraud, 2006).

---

[12] De Nederlandse Vereniging van Banken (NVB) behartigt de belangen van haar leden in diverse gremia. De NVB richt zich onder meer op de bestrijding van criminaliteit waar banken en (indirect) hun klanten het slachtoffer van zijn. Ter bestrijding van High–tech crime is binnen de NVB het Financial Institutions–Information Sharing and Analysis Center (FI–ISAC) ingesteld, dat zich onder andere bezighoudt met de informatie–uitwisseling over en analyse van computercriminaliteit.

Ook maken internetcriminelen gebruik van databanken of sociale netwerken om mensen met dezelfde interesses te benaderen (*intelligence lead phishing*, zie Symantec, 2007a).

Bij dit soort gerichte aanvallen is de kans op ontdekking kleiner. Anti–virussoftware herkent dergelijke e–mails niet als phishingmails en door het persoonlijke karakter van het bericht zullen slachtoffers minder wantrouwend zijn.

Bij *pharming* worden slachtoffers die online contact opnemen met een legale instelling of bedrijf, heimelijk omgeleid naar een nagemaakte versie van de website van die instelling of dat bedrijf. Vervolgens wordt gevraagd om persoonlijke gegevens. De omleiding wordt veroorzaakt door *malware*[13] waarmee de computer van het slachtoffer besmet is geraakt. Slachtoffers komen op verkeerde plekken terecht, doordat geknoeid is met de doorverwijzingen die worden gebruikt bij het opzoeken van domeinnamen.

Phishing met *malware* zonder dat gebruik wordt gemaakt van nagemaakte webpagina's, wordt *spy*–phishing genoemd. Het gedrag van computer-gebruikers wordt bespioneerd, bijvoorbeeld met behulp van *keyloggers*, waarmee toetsaanslagen worden vastgelegd, die vervolgens heimelijk worden verzonden naar de oplichters. Besmetting met *malware* voor spy–phishing, maar ook ten behoeve van pharming, vindt vooral plaats via e–mailberichten, bezoek aan websites, downloaden van software, gebruik van zoekmachines en gebruik van *instant messaging*.

Spy–phishing verschilt fundamenteel van de andere vormen, omdat slachtoffers niet worden misleid; er zijn geen nagemaakte webpagina's in het spel waarop persoonlijke gegevens worden ingetypt (DNRI, 2006d).

Uit de interviews kwam naar voren dat bovengenoemde phishingtechnieken steeds vaker worden gecombineerd. Slachtoffers krijgen een e–mail met de aansporing om beveiligingsupdates te downloaden. Bij installatie van de software wordt de internetbrowser van de slachtoffers aangepast. Hierdoor is het niet meer mogelijk de originele website van de bank te bereiken, maar wordt een nagemaakte website getoond waarop persoonlijke gegevens van het slachtoffer moeten worden ingevuld.

De ontwikkeling van phishingtechnieken heeft de laatste twee jaar niet stilgestaan. internetcriminelen verzinnen nieuwe manieren om hun

[13] Malware is een samentrekking van malicious software.

phishingaanvallen effectiever en succesvoller uit te voeren. Misleidende e–mails zijn bijvoorbeeld nauwelijks meer van echt te onderscheiden. Twee trends die zich in dat opzicht verder hebben ontwikkeld, zijn *phishing by proxy* en *man–in–the–middle phishing*. *Phishing by proxy* is erop gericht de werkelijke locatie van de phishingwebsite te verbergen en deze zo lang mogelijk in de lucht te houden. Bij deze phishingtechniek worden *botnets*[14] ingezet als *proxyservers*. Grote aantallen IP–adressen worden aan een phishingURL gekoppeld en vormen zo een tussenstap in de toegang tot de nagemaakte website. Het laten blokkeren van dergelijke sites en het opsporen van de daders is hierdoor zeer complex. Nadat een aantal beheerders van grote *botnets* is gearresteerd door de politie, is de trend tegenwoordig om niet een paar grote *botnets* maar meer kleinere onder controle te hebben om ontdekking te voorkomen en controle over meer zombies te houden door de inzet van meerdere opdracht– en besturingskanalen.

Bij *man–in–the–middle* phishing is het voor phishers ook mogelijk toegang te krijgen tot websites die beveiligd zijn met *twofactor*– authenticatie. Bij *twofactor*–authenticatie wordt na het invoeren van de inloggegevens nog een tweede code ingegeven, die veelal per transactie wordt gegeneerd. Deze methode is veiliger dan het gebruik van een enkelvoudig wachtwoord (onefactor–authenticatie, zie: DNRI, 2006d; Govcert.NL, 2007). Bij de *man–in–the–middle attack* zijn phishers in staat de tweede code te onderscheppen. Nadat de gegevens voor eigen criminele doeleinden zijn aangewend, worden ze door de phishers zelf doorgespeeld aan de klant, waardoor het voor de klant lijkt of de opdracht op de gewone manier is aangekomen.

Wireless netwerken (wifi) zijn de laatste jaren meer gemeengoed geworden, en op een groeiend aantal openbare plaatsen kan tegenwoordig draadloos verbinding worden gemaakt met het internet. De schaduwkant van draadloze netwerken is hun inbraakgevoeligheid. Veel consumenten beveiligen hun thuisnetwerk niet of nauwelijks. Bovendien stopt het signaal van het thuisnetwerk niet bij de voordeur en is onbekend tot waar het signaal precies reikt. Zo kunnen phishers in de buurt het signaal oppikken, inbreken in het netwerk en *malware* op computers plaatsen en/of identiteitsgegevens ontfutselen. Ook op openbare plaatsen waar meerdere mensen op eenzelfde wireless netwerk inloggen, kunnen phishers via het netwerk gemakkelijk inbreken op andermans computer (Kuran & Tugcu, 2007; Williams, 2006).

---

[14] 'Botnet' staat voor 'robotnetwerk'. Het is een verzameling van geïnfecteerde computers die op afstand onder controle staan van internetcriminelen. Botnets kunnen ingezet worden om bijvoorbeeld phishing e–mails te versturen of andere computers te infecteren.

Een nieuwe verschijningsvorm van phishing is *vishing*, ook wel *voice–phishing* genoemd. Met de opkomst van VoIP (Voice–over–IP, spraak via internet) is het mogelijk op een goedkope manier anoniem te bellen via internet. Voor criminelen is het mogelijk met behulp van VoIP een professionele telefooncentrale na te bootsen, waarbij inloggegevens ingegeven worden via de telefoontoetsen. Criminelen maken hier over het algemeen op twee manieren gebruik van. In het eerste geval wordt een e–mail verzonden naar een potentieel slachtoffer in dezelfde vorm als bij de traditionele phishing. In plaats van een frauduleuze link wordt een servicetelefoonnummer aangeboden waarnaar de klant moet bellen. Vervolgens wordt de indruk gewekt dat hij in het systeem moet inloggen bij de financiële instelling, waarbij gevraagd wordt naar bankrekeningnummers en passwords (Symantec, 2007b; McAfee, 2007; Fortinet, 2007). Een andere verschijningsvorm van vishing is als potentiële slachtoffers door criminelen worden gebeld met de vraag hun persoonsgegevens te bevestigen, omdat anders bijvoorbeeld hun bankrekening wordt opgeheven. Doordat gevraagd wordt persoonsgegevens te bevestigen, wordt een gevoel van vertrouwen bij de slachtoffers gewekt. Dit komt mede door de natuurlijke neiging van mensen om echte personen die zich presenteren via de traditionele telefoonlijn, te vertrouwen (Planet Internet, 2007; Symantec, 2007b).

Door middel van software en *VoIP* kunnen criminelen een geautomatiseerde telefooncentrale nabootsen die moeilijk van echt te onderscheiden is. Bovendien communiceren sommige financiële instellingen op dergelijke manieren met hun klanten. Gezien de toegenomen populariteit en ontwikkeling van VoIP valt dan ook te verwachten dat het gebruik hiervan voor criminele doeleinden de komende jaren zal toenemen (Bergstein, 2006; Binational Working Group on Cross–Border Mass Marketing Fraud, 2006; McAfee, 2007).

In het verlengde van deze vorm van phishing via *VoIP* ligt het gebruik van sms voor phishing. Door McAfee (2007) is hiervoor de term *SMiShing* geïntroduceerd. Een bankklant krijgt bij deze variant de vraag persoonlijke gegevens te bevestigen per sms. Wanneer internetten per mobiele telefoon gemeengoed zal zijn geworden, kan in de sms ook een (mobiele) internetlink worden verstuurd die leidt naar een nagemaakte website.

Alle bovengenoemde phishingtechnieken hebben tot doel de buitgemaakte gegevens te misbruiken. Met behulp van de buitgemaakte gegevens kunnen criminelen allerhande financiële transacties uitvoeren. Om hun eigen identiteit geheim te houden en toch geld te kunnen overmaken naar hun rekening, maken ze gebruik van tussenpersonen. Deze vaak onwetende tussenpersonen (*money mules*) worden via een spammail of websites als monsterboard.nl

gerekruteerd. Er wordt hun een baan aangeboden bij een financieel bedrijf. De taak van de medewerker is zijn rekening ter beschikking te stellen, waarbij het overgemaakte geld door hem wordt doorgestort via een cashtransferdienst, veelal naar Oost–Europese landen.

4.2.3 Omvang

Ten tijde van het NDB 2004 was phishing in Nederland een vrijwel onbekend verschijnsel. Sindsdien hebben zich meerdere phishingincidenten voorgedaan, waarvan een aantal ruim aandacht hebben gekregen in de media (De Telegraaf, 2007; Security.NL, 2007; Nu.NL, 2007).

Ten tijde van de vervolgstudie (DNRI, 2006a) was er nog geen systeem waarmee aangiftes en meldingen in de verschillende politieregisters landelijk konden worden bevraagd. Met de komst van Blueview is dit wel mogelijk. In Blueview is op verschillende zoektermen gezocht naar aangiftes en meldingen omdat korpsen deze verschillend classificeren. Zo plaatsen korpsen phishing onder computercriminaliteit, overige fraude, oplichting, overige vernieling en computervredebreuk. Wordt Blueview met deze zoektermen bevraagd, dan zullen er veel zaken tevoorschijn komen die geen phishing betreffen. Er is daarom voor gekozen in de vrije tekst te zoeken.

De zoekterm 'phishing' leverde 27 aangiftes en meldingen op voor de periode van januari 2005 tot en met oktober 2007. Vervolgens is gezocht op de zoekterm 'computercriminaliteit' in combinatie met 'Rabobank, ABN–Amro of Postbank'. Dit leverde 40 aangiftes en meldingen op. Kijken we naar het aantal aangiftes en meldingen per jaar, dan zien we een lichte stijging. In 2005 zijn er 15 aangiftes en meldingen binnengekomen, 25 in 2006 en 27 in de eerste tien maanden van 2007.

Het totale aantal aangiftes en meldingen dat met bovengenoemde zoektermen naar voren komt (67) zegt niet over het totale aantal phishingslachtoffers. Burgers die slachtoffer zijn geworden van phishing, richten zich in eerste instantie tot hun bank of creditcardmaatschappij. Deze voeren het beleid dat ze slachtoffers volledig schadeloos stellen voor de geleden schade. Voor slachtoffers ontbreekt hierdoor de noodzaak om aangifte te doen. Doen ze wel aangifte, dan is onduidelijk onder welke categorie het delict wordt weggeschreven en of de politiebeambte die de aangifte opneemt, überhaupt weet dat het phishing betreft. Aangifteregistraties bieden hierdoor nog steeds geen uitkomst voor het vaststellen van de omvang van phishing.

Om meer inzicht te krijgen in de omvang van phishing zijn, net als in de vervolgstudie van 2006, gesprekken gevoerd met banken en creditcard-maatschappijen. Hieruit kwam naar voren dat de banken en creditcard-maatschappijen in Nederland met naar schatting een honderdtal phishingcampagnes per jaar worden geconfronteerd (DNRI, 2006d).

Wanneer zich een klein phishingincident voordoet, lossen de beveiligings-afdelingen van de banken en creditcardmaatschappijen dit vaak zelf op. Bij de zwaardere incidenten schakelen zij Govcert.NL in, het Computer Emergency Response Team van de Nederlandse overheid. Dit team ondersteunt overheidsorganisaties in het afhandelen en voorkomen van ICT–gerelateerde incidenten. In voorkomende gevallen ondersteunt het ook particuliere organisaties. In het trendrapport 2007 wordt een overzicht gegeven van het aantal phishingincidenten waarbij Govcert.NL door de Nederlandse banken is ingeschakeld. Van februari 2006 tot en met maart 2007 waren dat iets minder dan 70 incidenten, waarbij na september 2006 een duidelijke stijging te zien is (Govcert.NL, 2007).

Regionaal en bovenregionaal werden de laatste jaren vrijwel geen phishinggerelateerde onderzoeken opgepakt. Doordat het internet geen regionale of nationale grenzen kent en de aard van het fenomeen een hoge mate van expertise vereist, worden dergelijke onderzoeken tegenwoordig nationaal opgestart. Bij de Nationale Recherche is sinds februari 2007 het Team High Tech Crime actief. De hoofdtaak van het team HTC is het verrichten van opsporingsonderzoeken ter bestrijding van bijzondere en exclusieve vormen van ICT–gerelateerde criminaliteit. In het jaar 2007 hebben zij twee opsporingsonderzoeken gedaan die betrekking hadden op phishing.

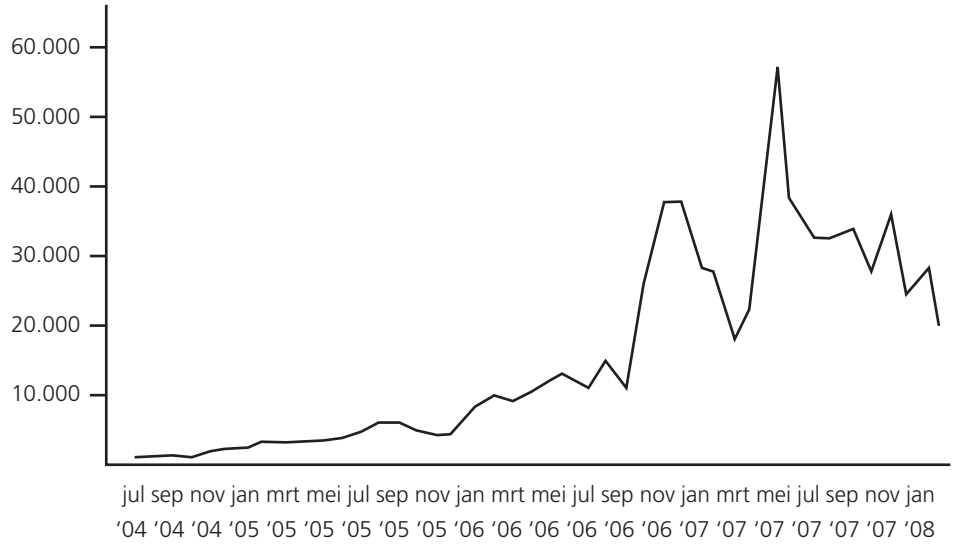
Omdat er weinig gegevens zijn over de omvang van phishing in Nederland en omdat internet zich niet laat begrenzen door landsgrenzen, is er ook gekeken naar de wereldwijde omvang van phishing. In Nederland was phishing ten tijde van het NDB 2004 nog een redelijk onbekend verschijnsel, dat zich op bescheiden schaal manifesteerde. In de vervolgstudie werd al melding gemaakt van een wereldwijde stormachtige ontwikkeling, en deze heeft zich sinds 2006 voortgezet.

De Anti–Phishing Working Group (APWG) houdt statistieken bij over phishing. De APWG is een mondiaal samenwerkingsverband van bedrijven en handhavingsinstanties dat gericht is op het bestrijden van identiteitsdiefstal en fraude als gevolg van phishing, pharming en *e–mail spoofing* (www.apwg.com). Maandelijks wordt een rapport uitgebracht op grond van meldingen van

betrokken partijen. Uit het rapport van de APWG komt naar voren dat het aantal unieke phishingwebsites enorm is toegenomen. In juli 2004 werden er nog 584 unieke sites geconstateerd, waarna een geleidelijke stijging is te zijn tot midden 2006. Daarna wordt het patroon grillig: april 2007 bereikte het aantal meldingen een piek van 55643, terwijl het aantal meldingen in de laatste maanden van 2007 weer afnam. De meest recente gegevens betreffen januari 2008, toen 20305 unieke phishing sites werden gemeld (zie figuur 4.1).

Figuur 4.1

Aantal unieke phishing sites juli 2004 t/m januari 2008



Bron: www.antiphishing.com, juli 2008

Internetbeveilingingsbedrijf Symantec nam in de tweede helft van 2006 166.248 unieke phishingberichten waar, een stijging van 6 procent in vergelijking tot de eerste zes maanden. In totaal hield Symantec meer dan anderhalf miljard phishingberichten tegen, een stijging van 19 procent in vergelijking met de eerste helft van 2006.

Uit het Symantec Security Report komt ook naar voren dat phishers doordeweeks actiever zijn dan in het weekend. Het aantal onderschepte unieke phishingberichten lag in het weekend gemiddeld 27 procent lager dan doordeweeks (Symantec, 2007a). MessageLabs doet net als Symantec aan internetbeveiliging. Volgens deze beveiliger bevatten in 2006 elke 274 e–mails

gemiddeld één poging tot phishing, terwijl dit in 2005 nog één op de 304 e–mails was en in 2004 één op 943 (MessageLabs, 2007).

Door het wereldwijde karakter van internet is het moeilijk te zeggen welk aandeel Nederland in deze stijging heeft. Zo komt uit het Symantec Security Rapport (Symantec, 2007a) naar voren dat 46 procent van de phishingsites zich in de Verenigde Staten bevindt. Nederland staat hierin op de tiende plaats met 2 procent. Dit is te verklaren doordat het grootste aantal gratis webhosts in de VS is gevestigd. Overigens betekent het feit dat een phishingwebsite zich in een land bevindt, niet automatisch dat de eigenaar van de website zich ook in dat land bevindt of dat de slachtoffers vooral in dat land te vinden zouden moeten zijn.

4.2.4 Betrokken personen en groeperingen

Verdachten achter de phishingaanvallen weten hun identiteit goed af te schermen. Het beeld dat verkregen is door het Team High Tech Crime van de Nationale Recherche is dat achter veel phishingaanvallen een aantal studenten uit het voormalige Oostblok zit wie het voornamelijk om het geld te doen is. Dit beeld komt overeen met algemene internationale bevindingen die betrekking hebben op phishing. *Hacking for fame*, waarbij jonge hackers gericht waren op het verwerven van erkenning voor hun digitale expertise, komt nauwelijks meer voor. Het gaat nu veel meer om eenvoudig en snel geld verdienen.

Tegenwoordig is het veel eenvoudiger dan een paar jaar geleden om met hacken te beginnen. Jonge hackers vinden op het internet informatie over hoe te werk te gaan, en kant–en–klare programma's om te hacken kunnen eenvoudig worden gedownload. Deze hackers worden door criminele organisaties benaderd via chatrooms en online fora. Zij worden ingeschakeld om *botnets* te beheren of bieden hun *botnets* daar te koop of te huur aan. Ook worden via deze weg jonge hackers ingehuurd om identiteitsgegevens te achterhalen. Criminele organisaties kopen hun expertise in en gaan daarbij gefragmenteerd te werk. Ingehuurde hackers kunnen zich hierdoor overal op de wereld bevinden zonder elkaar wezenlijk te kennen (McAfee, 2006; Symantec, 2007a). McAfee benadrukt bovendien dat hackers zich steeds meer verplaatsen naar de openbare ruimte, bijvoorbeeld internetcafés, universiteiten en bibliotheken, om zo hun anonimiteit te waarborgen.

Het beeld dat McAfee en Symantec schetsen, komt overeen met de bevindingen uit de Nederlandse onderzoeken. Een aantal Oost–Europese studenten werken samen om een phishingaanval uit te voeren. Uit hun internetverkeer blijkt dat ze de taken hebben verdeeld en de benodigde expertise hebben uitbesteed. Zo

hebben ze *botnets* gehuurd, e–mailadressen ingekocht en personen benaderd die voor hen de *malware* kunnen schrijven. Ze hebben blijkbaar ook de beschikking over kapitaal dat ze kunnen investeren in hun criminele onderneming. Opvallend is dat ze elkaar niet allemaal persoonlijk kennen. Het contact loopt via het internet en daar hebben ze elkaar ook ontmoet.

Omdat het erg moeilijk is om een goed zicht op de daders achter de phishingaanvallen te krijgen, blijft het lastig om vast te stellen of er sprake is van georganiseerde criminaliteit. Empirisch kan meestal niet worden vastgesteld dat er meerdere personen bij betrokken zijn, of dat de samenwerking meer dan eenmalig is. Toch kan worden beredeneerd dat door de complexiteit en het aantal te verrichten handelingen meestal meerdere personen betrokken zullen zijn bij phishing (DNRI, 2006d).

Het Team High Tech Crime heeft in 2007 twee grote opsporingsonderzoeken naar phishing gedaan. Uit deze onderzoeken is gebleken dat Nederlandse natuurlijke personen gerekruteerd worden als katvanger (*moneymule*) om geldbedragen door te sluizen naar Rusland en/of de Oekraïne. Door het gebruik van deze tussenpersonen en tussenkomst van een proxyserver weten de verdachten hun identiteit af te schermen.

Uit verder onderzoek van het Team HTC is gebleken dat IP–adressen waarvan gebruik gemaakt is door de verdachte(n), behoren tot een range IP–adressen die administratief op naam zijn gesteld van het Russian Business Network. Dit is een Russische serviceprovider waar mensen anoniem gebruik kunnen maken van het netwerk. Wereldwijd lopen tientallen opsporingsonderzoeken naar dit Russian Business Network. Het betreft onderzoeken op het gebied van kinderporno, spam, illegale goksites enz. (The Economist, 2007).

4.2.5 Gevolgen voor de Nederlandse samenleving

De schadelijke gevolgen van phishing zijn in te delen in directe en indirecte gevolgen. Directe slachtoffers van phishing zijn voornamelijk internettende burgers en bedrijven die betrokken zijn bij het online kopen en verkopen van goederen en diensten (DNRI, 2006d). Verkregen inlog– en creditcardgegevens kunnen gebruikt worden door criminelen om bankrekeningen te plunderen of online bestellingen te doen. Doordat burgers die het slachtoffer zijn geworden van phishing, contact opnemen met hun bank of creditcardmaatschappij en deze de klanten schadeloos stelt, is voor de klanten de schade gering.
De schade wordt vooral geleden door banken en creditcardmaatschappijen (Symantec, 2007a).

Over de totale schade die door phishing wordt veroorzaakt is voor de Verenigde Staten en het Verenigd Koninkrijk meer bekend dan voor Nederland. In het Verenigd Koninkrijk wordt geschat dat over 2006 in totaal 45,7 miljoen pond van online bankrekeningen werd gestolen. De schattingen voor de Verenigde Staten lopen uiteen van 630 miljoen tot vijftig miljard dollar over 2006 (Dallaway, 2006; Nu.NL, 2007). Gezien de toename van phishingincidenten en de hoogte van de schade in het Verenigd Koninkrijk en de Verenigde Staten zou verwacht mogen worden dat de schade ook in Nederland in de miljoenen euro's loopt.

Tijdens de vervolgstudie zijn expertmeetings gehouden met vertegenwoordigers van zeven banken, waaronder vier van de vijf grote banken in Nederland. Hieruit kwam naar voren dat de totale directe financiële schade in Nederland onder de 100.000 euro is gebleven (DNRI, 2006d). In 2007 is opnieuw een expertmeeting gehouden, waarbij de banken aangaven dat de directe schade niet opweegt tegen de indirecte schade.

Een van de vormen van indirecte schade waar de financiële instellingen mee te kampen kunnen krijgen door phishingincidenten, is imagoschade. Internetbankieren en elektronisch winkelen zijn nog steeds in opkomst en besparen banken en winkels hoge kosten (Jonker & Kettenis, 2007). Wanneer klanten hun vertrouwen in de financiële instelling of internetbankieren verliezen, zijn de kosten niet te overzien. Elke rem op de groei van deze onlinediensten is voor de banken een grote schadepost (Van Overbruggen, 2006; Sullins, 2006).

Een andere indirecte schadepost voor de financiële instellingen zijn de investeringen die zij moeten doen in de beveiliging van hun systemen en diensten (DNRI, 2006d; Van Overbruggen, 2006; Sophos, 2007). Uit een enquête onder topmensen van de grootste internationale financiële instellingen bleek dat de meerderheid van hen phishing en pharming als de grootste bedreiging voor 2006 zag. Bedrijven zijn dan ook bereid om in het voorkomen hiervan te investeren (CBS, 2006).

Ook voor de consumenten is sprake van indirecte schade door phishingincidenten. Net als de banken zullen zij moeten investeren in de beveiliging van hun computer. Financiële instellingen investeren daarom ook veel in het bewust maken van de klanten van de beveiligingsrisico's die zij thuis lopen. Dat phishers succesvol zijn, ligt voor een groot deel aan de gebrekkige beveiliging van het netwerk en de computers van particulieren die hiermee verbonden zijn (CBS, 2006). Financiële instellingen zijn terughoudend over de omvang en kosten van phishing, omdat ze beducht zijn voor de vertrouwensband met hun klanten. Het is daardoor onduidelijk hoeveel de

directe en indirecte schade in Nederland bedraagt. Schattingen die zijn gedaan, zijn bovendien vaak gedaan door bedrijven die hun bestaansrecht danken aan de onveiligheid op de digitale snelweg, zoals leveranciers van beveiligingssoftware (DNRI, 2006d).

4.2.6 Criminaliteitsrelevante factoren

De randvoorwaarden voor phishing zijn de laatste jaren verbeterd. Zo beschikte in 2002 nog 62 procent van de ondervraagde Nederlanders over een pc met internettoegang. In 2007 was dit toegenomen tot 82 procent van de ondervraagden. Van deze internetgebruikers hebben steeds meer mensen tegenwoordig een breedbandverbinding. In 2002 had nog maar 23 procent van de huishoudens een breedbandaansluiting. In 2007 was dit percentage toegenomen tot 89. Breedbandverbindingen zijn sneller dan analoge verbindingen. Gebruikers betalen een vast bedrag per maand en kunnen vervolgens ongelimiteerd internetten. Breedbandgebruikers hebben hun computer hierdoor vaker en langer aanstaan, waarbij de internetverbinding openstaat. Deze gebruikers downloaden en internetten ook meer, waardoor zij makkelijker besmet kunnen worden met *malware*. Pc's met een dergelijke aansluiting zijn hierdoor ideaal voor internetcriminelen om dienst te doen als zombie in een *botnet* (DNRI, 2006d).

Nederlanders zijn de laatste jaren steeds meer gebruik gaan maken van elektronisch winkelen en internetbankieren. Het aantal mensen dat goederen kocht via internet, nam tussen 2002 en 2007 toe met 3 miljoen tot 7,5 miljoen personen. In 2002 zei 40 procent van de internetgebruikers goederen of diensten te kopen via internet. In 2007 was dit 66 procent. Niet alleen elektronisch winkelen neemt sterk toe, ook steeds meer mensen maken gebruik van internetbankieren. In 2007 internetbankiert 72 procent van alle ondervraagde internetgebruikers; dat is 5 procent meer dan een jaar eerder (CBS, 2007).

Uit onderzoek van de Nederlandsche Bank blijkt dat Nederlanders, in tegenstelling tot inwoners van de Verenigde Staten, eerder cash of met een pinpas betalen dan met een creditcard (Jonker, 2005). Volgens de Consumentenbond bezit ook in Nederland ruim twee derde van de Nederlandse huishoudens een creditcard in december 2004. Uit het jaarverslag 2006 van de Nederlandsche Bank blijkt bovendien dat het aantal creditcardbetalingen nog steeds toeneemt. In 1999 werden 44 miljoen betalingen gedaan met een creditcard, in 2006 waren het er 50 miljoen (Nederlandsche Bank, 2007).

Creditcards brengen het risico met zich mee dat de gegevens van de card door criminelen gebruikt worden voor bestellingen en betalingen. Paypal en iDeal zijn

initiatieven om betalen via het internet veiliger te maken, doordat geen creditcardgegevens meer hoeven te worden verstrekt aan de verkoper. Gebruikers van Paypal betalen door het sturen van een e–mail. Ze hebben een account bij Paypal dat gekoppeld is aan hun bankrekening of creditcard. Paypal blijkt echter ook kwetsbaar voor phishers, doordat naar de gebruikers vaak nagemaakte e–mails worden verstuurd met het verzoek de account gegevens te verifiëren. Vervolgens wordt met behulp van de accountgegevens de bankrekening of creditcard geplunderd (McCarthy, 2006). Met iDeal betalen consumenten via internetbankieren bij hun eigen bank, waar wordt ingelogd met twee fasen–authenticatie. In 2006 werd 15 procent van de onlinebetalingen gedaan via iDeal, het aantal creditcardbetalingen online was in 2006 13 procent (Currence, 2007).

Ook consumenten moeten maatregelen nemen tegen internetcriminaliteit. Veel computers zijn niet goed beveiligd en consumenten zijn zich niet bewust van het gevaar dat zij lopen. Wanneer internetgebruikers zouden leren wat de gevaren zijn van phishing, zouden de aanvallen een stuk minder effectief kunnen zijn voor internetcriminelen (Sullins, 2006; Kumaraguru e.a., 2006). De overheid speelt hierin ook een rol; zij probeert door middel van onder meer voorlichtingscampagnes burgers te wijzen op de gevaren van internet (www.veiligbankieren.nl). Ook de banken investeren in het bewust maken van de klanten van de onveiligheid van het internet en de noodzaak tot beveiliging van hun computer thuis.

Met het ontbreken van eenvoudige, betrouwbare mogelijkheden om computers te beveiligen doen cybercriminelen hun voordeel. Niet alleen consumenten kunnen moeilijk achterhalen wie de zender of ontvanger van informatie is, ook opsporingsinstanties hebben hier moeite mee. Vaak leiden aanknopingspunten via meerdere schijven naar het buitenland, wat opsporing tot een tijdrovende zaak maakt. Anders dan criminelen moeten rechercheurs bij grens-overschrijdende onderzoeken problemen overwinnen met communicatie, het regelen van bevoegdheden en technische hulpmiddelen. De internetcrimineel profiteert juist van de snelheid en anonimiteit van het internet.

Voorheen was noch de Nederlandse politie noch het Openbaar ministerie toegerust om computergerelateerde criminaliteit die van internationaal niveau en technisch veeleisend is aan te pakken. Bovendien is ICT–gerelateerde criminaliteit lang een onderbelicht verschijnsel geweest binnen de criminaliteitsbestrijding. Dit resulteerde in een lage pakkans voor phishers. Met de oprichting van het Team High Tech Crime is er nu een instantie die onder andere met de opsporing van dergelijke vormen van criminaliteit is belast.

De ontwikkeling van de technologie biedt volop kansen voor phishers. Zo zijn wireless netwerken (wifi) de laatste jaren meer gemeengoed geworden. Op een nog steeds groeiend aantal openbare plaatsen kan tegenwoordig draadloos verbinding worden gemaakt met het internet (Kuran & Tugcu, 2007). De gebrekkige en geringe beveiliging van draadloze netwerken en computers biedt phishers hierdoor vele mogelijkheden om op afstand in te breken in een computer en identiteitsgegevens te stelen. Daarnaast bieden communicatietechnieken zoals VoIP en sms nieuwe mogelijkheden voor phishers. Mobiele telefoons die te vergelijken zijn met portable computers (*smartphones*) hebben hun intrede gedaan. Doordat via deze telefoons dezelfde handelingen verricht kunnen worden als op 'gewone' computers, lopen gebruikers ook dezelfde risico's (McAfee, 2006).

4.2.7 Verwachtingen voor de toekomst

Ten tijde van het NDB 2004 was nog weinig bekend over phishing. Anno 2008 heeft het fenomeen zich ontwikkeld, onder andere door technische vooruitgang en de groeiende internetmarkt, zoals beschreven in de vorige paragraaf. Voor de toekomst valt te verwachten dat reeds ingezette trends verder zullen doorzetten. Anderzijds mag verwacht worden dat maatregelen die genomen worden om phishing tegen te gaan, enig effect zullen hebben.

Op sites als myspace.com en hyves worden zo veel persoonlijke details van gebruikers onthuld, dat daardoor vele mogelijkheden voor phishers worden geschapen. *Malware* kan verstopt worden in links of downloads en phishers kunnen hun doelgroep selecteren op basis van interesses (McAfee, 2006). Momenteel zijn de phishingaanvallen via deze sites nog op één hand te tellen, maar gezien de toenemende populariteit van deze *social networking* sites lopen ze in de toekomst zeker een risico (MessageLabs, 2006). Ook wordt een toename verwacht van de verspreiding van *malware* en phishingberichten via *instant messaging*. Inmiddels zijn de netwerken van Yahoo! en msn aan elkaar gekoppeld, wat de reikwijdte van deze netwerken heeft vergroot. Wanneer ook andere grote IM–systemen zoals AOL en GoogleTalk op elkaar gaan aansluiten, biedt dit weer meer mogelijkheden voor phishers (DNRI, 2006d; MessageLabs 2006).

Multiplayer online games zoals World of Warcraft, Lineage en Second Life winnen de laatste jaren aan populariteit. Zo heeft World of Warcraft inmiddels meer dan acht miljoen betalende spelers en kan de virtuele economie van Second Life concurreren met die van een klein land (Blizzard, 2007; Wharton, 2005). Spelers maken een virtueel karakter aan en begeven zich in een onlinewereld waar ze virtuele goederen of geld kunnen vergaren. Binnen Second

Life kunnen echte dollars geruild worden voor Linden–dollars, het betaalmiddel binnen Second Life. Virtuele goederen en virtuele dollars kunnen andersom ook ingeruild worden voor echte valuta zoals dollars of euro's. Doordat er steeds meer geld omgaat in deze werelden, zijn ook MMOGs interessante slachtoffers voor phishers geworden. Phishers plaatsen, door middel van een mail of link op een forum, *malware* op de computer van de gamer. Zo leggen ze de toetsaanslagen vast en ontvreemden ze inloggegevens (Security.NL, 2007).

Doordat de virtuele identiteit van een speler gekoppeld is aan zijn echte identiteit, kunnen phishers de speler persoonlijke gegevens ontfutselen. Daarmee kunnen ze creditcardgegevens achterhalen of virtuele goederen of valuta stelen om deze op veilingsites te verkopen. Trend Micro, maker van beveiligingssoftware, heeft in 2006 al ruim 3600 gamegerelateerde spyware–uitbraken geregistreerd (Trendmicro, 2007). Zij verwachten dat dit aantal de komende jaren zal toenemen. Hoe groot het gevaar van dit soort phishinguitbraken zal zijn voor de Nederlandse samenleving, is moeilijk in te schatten.

Behalve de genoemde criminaliteitsrelevante factoren, waarvan de meeste in de richting wijzen van méér mogelijkheden voor phishing, is sprake van een toenemende vaardigheid onder phishers om ontdekking te voorkomen. In de vervolgstudie (DNRI, 2006d) werd al benadrukt dat voor de toekomst een verdere toename van spy–phishing werd verwacht en dit blijkt uit te komen. Door middel van *malware* worden inloggegevens onderschept zonder dat de gebruiker er iets van merkt. Het is dan niet nodig om gebruikers via een vorm van *social engineering* te verleiden deze gegevens prijs te geven. De klassieke vormen van phishing komen steeds minder voor, onder andere doordat internetgebruikers zich steeds bewuster worden van het bestaan van misleidende e–mails (Jakobsson & Ratkiewicz, 2006). Het is te verwachten dat steeds meer geavanceerde en specifieke *malware* zal worden ontworpen. *Botnets* zullen kleinschaliger worden. Als nog gebruikgemaakt wordt van misleidingstactieken, dan zullen deze naar verwachting ook steeds 'slimmer' worden: criminelen zullen mensen benaderen als lid van een bepaalde gemeenschap. Beperkten phishers zich vroeger tot vooral Engelstalige landen, inmiddels zijn er over heel de wereld phishingmails bekend in de landstaal (Sullins, 2006).

De gesignaleerde ontwikkelingen vormen een verklaring voor de stijgende lijn van het aantal aangiftes voor phishing en meldingen over websites bij internetbeveiligingsbedrijven en andere instanties. Alom wordt verwacht dat phishing de komende jaren nog zal toenemen. Uit een enquête gehouden onder topmensen van de grootste financiële instellingen ter wereld door Deloitte

kwam naar voren dat een meerderheid in de nabije toekomst nieuwe aanvallen verwacht, waarbij de tactieken voor identiteitsdiefstal door middel van phishing steeds geavanceerder zullen worden (Deloitte, 2006; CBS, 2006).

De directe schade die in Nederland door phishing wordt veroorzaakt, lijkt tot nu toe mee te vallen. De indirecte schade waarmee de banken worden geconfronteerd, is echter aanzienlijk. Omdat het aantal phishingaanvallen in de toekomst naar verwachting zal toenemen, kan verwacht worden dat zowel de directe als de indirecte schade zal stijgen. Moeilijk is echter in te schatten hoeveel de schade zal bedragen en in welke mate deze zal stijgen. Zien we de VS als voorland, dan zouden we een grote stijging van de schade kunnen verwachten. Omdat in de VS het internetbankieren anders is ingericht dan in Nederland, is het echter de vraag of beide situaties wel vergelijkbaar zijn.

Uit de huidige opsporingsonderzoeken van het Team High Tech Crime blijkt dat de personen achter de grote phishingaanvallen Oost–Europeanen zijn, waarbij wordt aangenomen dat het gaat om (oud–)IT studenten. Om een goede phishingaanval uit te voeren is wel enige kennis van zaken nodig. Deze is niet alleen in Oost–Europa voorhanden. Ook in andere delen van de wereld zijn genoeg mensen te vinden die een goede kennis van IT combineren met een verlangen snel geld te verdienen. Dat er geld te verdienen is met phishing, lijkt voorlopig zeker het geval.

5
Werkwijzen van criminele samenwerkingsverbanden

In dit hoofdstuk staan de bevindingen ten aanzien van drie werkwijzen van criminele samenwerkingverbanden, namelijk het misbruik maken van ondernemingen waarover ze controle hebben, desinformatie als een contrastrategie en documentvervalsing.

5.1 Misbruik van ondernemingen

5.1.1 Inleiding

Voor de eerste versie van het Nationaal dreigingsbeeld is in 2004 uitgebreid onderzoek gedaan naar criminele afscherming en verweving. Een van de indicatoren voor de verwevenheid van boven– en onderwereld was de zeggenschap die criminelen hadden over ondernemingen.

Als er gesproken wordt over *verweving van boven– en onderwereld* dan wordt daarmee gerefereerd aan een zekere relatie of verbondenheid tussen zware of georganiseerde misdaad enerzijds en bedrijfsleven anderzijds (DNRI, 2004b).

Criminelen kunnen als eigenaar, bestuurslid of aandeelhouder zeggenschap in ondernemingen hebben en daardoor invloed uitoefenen. Deze zeggenschap is voor criminele samenwerkingsverbanden van belang omdat zij deze ondernemingen of instanties kunnen gebruiken bij de uitvoering van hun criminele activiteiten. In het vertrouwelijke rapport *Criminele afscherming en verweving* is hier uitvoerig op in gegaan (DNRI, 2004b). Ook Bruinsma & Bovenkerk (1996), Huisman e.a. (2003; 2005) en Van de Bunt & Kleemans (2007) besteden veel aandacht aan misbruik van ondernemingen. Kleemans, Brienen en Van de Bunt (2002) merken dan ook op dat georganiseerde criminaliteit niet ondanks maar dankzij de wettige omgeving bestaat. De steun van de wettige omgeving kan noodzakelijk zijn voor het maken van producten en het afnemen van producten en diensten. Ook kan de wettige omgeving bewust, maar vaak ook onbewust, diensten verlenen die van belang zijn voor het functioneren van criminele samenwerkingsverbanden (p. 79–80).

Om dit te voorkomen heeft de overheid een aantal preventieve maatregelen genomen, zoals de verklaring van geen bezwaar (VVGB), de verklaring omtrent het gedrag rechtspersonen (VOGr) en de Wet bevordering integriteits-beoordelingen door het Openbaar Bestuur (BIBOB). Ondanks deze maatregelen rijst de vraag in hoeverre leden van criminele samenwerkingsverbanden in de gelegenheid zijn om ondernemingen voor criminele doeleinden te benutten. Om hierin enig zicht te krijgen is nagegaan in welke mate leden van criminele samenwerkingsverbanden zeggenschap over ondernemingen hebben. Deze analyse vormt een herhaling van de analyse gepresenteerd in de deelstudie *Criminele Afscherming en Verweving* (DNRI, 2004b). Hierover wordt gerapporteerd in paragraaf 5.1.3.

5.1.2 Preventieve overheidsmaatregelen

Verklaring van geen bezwaar (VVGB)

Een van de maatregelen van de overheid om te voorkomen dat leden van criminele samenwerkingsverbanden zeggenschap krijgen over ondernemingen is de verklaring van geen bezwaar. Iedereen in Nederland die een besloten of naamloze vennootschap of societas europea (Europese NV) wil oprichten of de statuten van een opgericht vennootschap wil wijzigen moet een verklaring van geen bezwaar (VVGB) bij de minister van Justitie aanvragen. Dit gebeurt via de notaris. Deze vraagt de VVGB aan bij de dienst Justis van het ministerie van Justitie en levert hiervoor alle inlichtingen aan die noodzakelijk zijn voor het beoordelen van de aanvraag (art. 68, lid 1, art. 179 lid 1, boek 2 BW).

De verklaring mag alleen worden geweigerd indien er, gelet op de voornemens of de antecedenten van personen die het beleid van de vennootschap zullen (mede) bepalen, gevaar bestaat dat de vennootschap zal worden gebruikt voor ongeoorloofde doeleinden of dat haar werkzaamheid zal leiden tot benadeling van haar schuldeisers (artikel 68 lid 2 en artikel 179 lid 2 van Boek 2 BW). Bij gerede twijfel aan de morele of financiële betrouwbaarheid of integriteit van de bij de vennootschap betrokken personen die het beleid (mede)bepalen kan worden aangenomen dat het voornoemde gevaar bestaat (Ministerie van Justitie, 2005).

De beoordeling van de betrouwbaarheid en de integriteit vindt plaats aan de hand van een onderzoek naar de voornemens en naar de criminele en financiële antecedenten van de bij de vennootschap betrokken (mede–) beleidsbepalende (rechts)personen. De voornemens zijn van belang omdat daaruit kan blijken of een op te richten vennootschap voor ongeoorloofde doeleinden kan worden gebruikt, dan wel dat de werkzaamheden tot benadeling van schuldeisers kunnen leiden.

Criminele antecedenten zijn van belang omdat deze onder andere kunnen indiceren dat de vennootschap zal worden gebruikt voor ongeoorloofde doeleinden. Financiële antecedenten zijn van belang omdat deze kunnen indiceren dat de werkzaamheid van de vennootschap zal leiden tot benadeling van schuldeisers en wellicht zal worden gebruikt voor ongeoorloofde doeleinden (Ministerie van Justitie, 2005).

Bij twijfel over de integriteit van de oprichters of (mede–) beleidsbepalers van de vennootschap kan en zal in veel gevallen informatie worden opgevraagd bij relevante instanties (zoals Justitie) en bij de aanvrager zelf. Een VVGB wordt in beginsel niet geweigerd indien de betrokkene aannemelijk kan maken dat er geen gevaar (meer) bestaat dat de vennootschap zal worden gebruikt voor ongeoorloofde doeleinden of dat haar werkzaamheden zullen leiden tot benadeling van schuldeisers (Ministerie van Justitie, 2005).

Tabel 5.1

Aantal aanvragen en weigeringen VVGB

Jaar	Aantal aanvragen	Aantal weigeringen	Percentage weigeringen
2001	72.483	650	0,90
2002	70.359	234	0,33
2003	68.042	271	0,40
2004	68.638	755	1,10
2005	72.781	1.275	1,75
2006	85.397	574	0,67
2007	43.758	264	0,60

Deze *misbruiktoets* wordt uitgevoerd wordt door de dienst Justis van het ministerie van Justitie, de justitiële uitvoeringsdienst Toetsing, Integriteit en Screening.

In tabel 5.1 is een overzicht gegeven van het aantal weigeringen vanaf het jaar 2001 tot en met 2007. In het aantal afgewezen verzoeken zijn ook de intrekkingen en buitenbehandelingstellingen meegerekend. Het komt namelijk geregeld voor dat aanvragen ingetrokken worden naar aanleiding van vragen die de dienst Justis stelt aan de aanvrager van het verzoek.

De VVGB voldoet niet doordat alles wat na de oprichting van een vennootschap plaatsvindt zich buiten het toezicht van de overheid voltrekt. Het ministerie van Justitie ontwikkelt in het project Herziening Toezicht Rechtspersonen (HTR) een

nieuwe systematiek van toezicht op rechtspersonen. Hiermee wordt in de plaats van de VVGB een vorm van permanente screening geïntroduceerd.

In het nieuwe systeem worden notarissen en Kamers van Koophandel verplicht om alle kerngegevens over bestuurders van rechtspersonen aan het ministerie van Justitie te melden. Justitie gaat deze gegevens permanent koppelen met bestanden van de Belastingdienst, het Uitvoeringsorgaan Werknemers-verzekeringen (UWV) en andere instanties. Door het wegvallen van de preventieve toetsing wordt het makkelijker en goedkoper om een BV op te richten, maar hiertegenover staat dat de controle scherper en meer permanent wordt (Veldkamp & de Vries, 2007).

Verklaring omtrent het gedrag voor rechtspersonen (VOGrp)

Op 1 april 2004 is de Wet justitiële gegevens in werking getreden. In deze wet is een regeling opgenomen voor de Verklaring Omtrent het Gedrag (Wet Justitiële en strafvorderlijke gegevens, Afdeling 5). Per 1 april 2004 kunnen niet alleen natuurlijke personen maar ook rechtspersonen een Verklaring Omtrent het Gedrag aanvragen. Hiermee kunnen rechtspersonen hun integriteit tonen aan partners, bedrijven en overheidsinstanties.

De VOGrp is een verklaring van de minister van Justitie die door het Centraal Orgaan Verklaring Omtrent het Gedrag (COVOG) wordt afgegeven. Het COVOG viel voorheen onder de dienst Bestuurszaken van het ministerie van Justitie, maar sinds 1 januari 2005 onder de dienst Justis.

Het onderzoek dat naar aanleiding van een aanvraag VOGrp plaatsvindt, richt zich op alle bij de aanvraag genoemde rechtspersonen en alle natuurlijke personen met sleutelposities binnen deze rechtspersoon; dit zijn de bestuurders, maten, vennoten of beheerders (Ministerie van Justitie, 2006).

Het COVOG raadpleegt in het onderzoek het Justitieel Documentatie Systeem (JDS). In JDS staan gegevens over transacties en de afwikkeling van strafbare feiten, van onherroepelijke veroordelingen tot sepots. Daarnaast kunnen gegevens uit politieregisters en uit de Documentatie Vennootschappen in het onderzoek worden betrokken. Tenslotte kan het COVOG inlichtingen bij het Openbaar ministerie en de reclassering inwinnen. Al deze gegevens worden in samenhang gewogen en beoordeeld.

Als blijkt dat ten aanzien van de rechtspersoon of de onderzochte natuurlijke personen in de registers een strafbaar feit is vermeld, dat, *"… indien herhaald en gelet op het risico voor de samenleving en de overige omstandigheden van*

het geval een belemmering kan vormen voor een behoorlijke uitoefening van de taak of de bezigheden waarvoor de VOG wordt gevraagd…", wordt de VOG geweigerd (Staatscourant, 2004).

In het NDB 2004 noemde de DNRI de VOGrp een nieuw instrument dat nog gemeengoed zou moeten worden (DNRI, 2004b). Inmiddels is gebleken dat de VOGrp niet in alle gevallen verplicht is gesteld. Niettemin is het aantal aanvragen VOGrp de laatste jaren toegenomen (zie tabel 5.2.).

Tabel 5.2

Aantal aanvragen VOGrp	
Jaar	Aantal
2004	729
2005	1.113
2006	2.525
2007 (1e helft)	1.835

Wet Bevordering Integriteitsbeoordelingen door het Openbaar Bestuur

Op 1 juni 2003 is de Wet Bevordering Integriteitsbeoordelingen door het Openbaar Bestuur (Wet BIBOB) in werking getreden. De Wet BIBOB moet voorkomen dat de overheid, door het verlenen van vergunningen of het verstrekken van subsidies of het gunnen van overheidsopdrachten, onbedoeld criminele activiteiten faciliteert.

Momenteel kan de Wet BIBOB worden toegepast op Drank– en Horecawet-vergunningen, op bepaalde vergunningen voor de exploitatie van coffeeshops, smart– en growshops, seksinrichtingen en speelautomatenhallen, op milieu– en bouwvergunningen, opiumontheffingen, personen– en goederenvervoer en de verkoop van onroerend goed door woningcorporaties aan particulieren.

Bij aanbestedingen kan de Wet BIBOB worden toegepast op aanbestedingen die vallen binnen de sectoren Bouw, Milieu en ICT. Voor subsidies zijn geen specifieke sectoren aangewezen.

Overheidsinstellingen hebben met de inwerkingtreding van de Wet BIBOB extra weigerings– en intrekkingsgronden gekregen. Artikel 3 van de Wet BIBOB maakt het mogelijk om een beschikking te weigeren of in te trekken als er ernstig gevaar bestaat dat de beschikking mede gebruikt zal worden om strafbare feiten te plegen

of crimineel geld wit te wassen. Als het onderzoek door het bestuursorgaan niet voldoende uitsluitsel biedt, kan Bureau BIBOB worden ingeschakeld. Dit bureau voert een onderzoek uit dat drie soorten adviezen kan opleveren: 'ernstig gevaar', 'enige mate van gevaar' en 'geen gevaar'. Vervolgens zal het bestuursorgaan mede op basis van dat advies een besluit moeten nemen (Staatsblad, 2002).

Ten tijde van het NDB 2004 was de Wet BIBOB net in werking getreden en was het BIBOB–beleid van de gemeenten nog in ontwikkeling of in de opstartfase. Gemeenten kunnen in een BIBOB–beleidslijn neerleggen voor welke (individuele) gevallen een advies kan worden aangevraagd. In 2006 had 61procent van de bestuursorganen een dergelijke beleidslijn. Gemeenten vanaf 50.000 inwoners hadden relatief vaak een BIBOB–beleidslijn vastgesteld in vergelijking met kleinere gemeenten (De Voogd, Doornbos & Huntjens, 2007).

In tabel 5.3 is te zien dat het aantal BIBOB–adviezen langzaam toeneemt. Op 1 augustus 2006 waren in totaal 264 BIBOB–aanvragen ingediend. Niet alle aanvragen hebben geleid tot een BIBOB–advies, bijvoorbeeld omdat de vergunningaanvrager zich terugtrok of omdat de aanvraag onvolledig was.

Tabel 5.3

Aantal BIBOB–adviezen per jaar

	2003 (vanaf 1 juni)	2004	2005	2006 (tot 1 augustus)	Totaal
Aantal aangevraagde adviezen	7	61	95	101	264
Aantal uitgebrachte adviezen	2	50	72	96	193

Bron: De Voogd e.a. (2007). p. 48

Van de uitgebrachte adviezen was bij 60 procent sprake van ernstig gevaar dat de vergunning misbruikt zou worden om criminele activiteiten te ontplooien. De aanvragers werden in verband gebracht met zogenaamde katvangers– en dekmantelconstructies, maar ook met omvangrijke witwaspraktijken en ernstige fraude.

In 14 procent van de gevallen bestond 'enige mate van gevaar' voor misbruik. Veelal had de aanvrager antecedenten, maar waren deze niet relevant voor het doel waar de vergunning voor werd aangevraagd. In de overige onderzoeken (26%) is geen belastende informatie gevonden.

Veruit de meeste BIBOB–adviesaanvragen hebben betrekking op de sector horeca (154), 40 hadden te maken met seks en 14 met coffeeshops. Voor de sectoren milieu, ICT en bouw waren er elk een tiental aanvragen (De Voogd, Doornbos & Huntjens, 2007).

Het is moeilijk om een uitspraak te doen over de mate waarin de ongewilde facilitering van criminele activiteiten door bestuursorganen is afgenomen. Uit de evaluatie van de Wet BIBOB kwam wel duidelijk naar voren dat binnen de bestuursorganen een hogere mate van bewustzijn van de risico's van criminele facilitering bestaat. Dit heeft geleid tot weigeringen van vergunningen of intrekking van verleende beschikkingen. Dit wil echter nog niet zeggen dat er minder gevallen van ongewilde criminele facilitering zijn voorgevallen, aangezien verondersteld mag worden dat criminelen methoden ontwikkelen om de Wet BIBOB te omzeilen. Uit de evaluatie kwam ook naar voren dat nog onduidelijk is welke neveneffecten de Wet BIBOB kan hebben. Verschuiving van criminaliteit naar andere sectoren is op dit moment nog nauwelijks waar te nemen, maar kan niet worden uitgesloten. Ook kan een verschuiving optreden naar gemeenten waar de Wet BIBOB (nog) niet wordt toegepast (De Voogd e.a., 2007).

5.1.3 Zeggenschap over ondernemingen

Bovengenoemde preventieve overheidsmaatregelen zijn erop gericht om misbruik van ondernemingen tegen te gaan. De vraag rijst hoe vaak het voorkomt dat leden van criminele samenwerkingsverbanden toch in de gelegenheid zijn om ondernemingen voor criminele doeleinden te benutten. In het deelrapport *Criminele afscherming en verweving* werd deze vraagstelling als volgt geformuleerd:

> 'In welke getale hebben personen die bij de politie bekend staan vanwege betrokkenheid bij georganiseerde criminaliteit zeggenschap over ondernemingen?' (DNRI, 2004b, p. 113)

Voor het onderzoek is gebruik gemaakt van de EU–inventarisatie van criminele samenwerkingsverbanden door de Dienst Nationale Recherche Informatie. Deze inventarisatie wordt elk jaar uitgevoerd en vormt de basis voor de Nederlandse bijdrage aan het Europese dreigingsbeeld georganiseerde criminaliteit (DNRI, 2007b). De analyse is een herhaling van een analyse van 2004, die gebaseerd was op een steekproef uit de EU–inventarisatie (DNRI, 2004b). Anno 2008 kan gebruik gemaakt worden van het volledige bestand. Alle namen van verdachten die voorkomen in de inventarisatie zijn gekoppeld aan het register van de Kamers van Koophandel.

Dit levert een bestand op waarin van de verdachten uit de EU–inventarisatie voor 2006 kan worden vastgesteld of zij betrokken zijn bij een onderneming. Tevens werden gegevens verzameld over de branche waarin het bedrijf actief is en over de rol van de betrokkene. Het bestand biedt eveneens mogelijkheden voor analyse op het niveau van csv's en voor analyses over het verloop van betrokkenheid in de tijd. Zo zijn ook vroegere inschrijvingen in de Kamer van Koophandel opgenomen. Uiteraard biedt een dergelijke analyse geen soelaas als er gebruik wordt gemaakt van verhullende constructies, zoals inschrijving op naam van een stroman.

Het totale aantal personen uit de EU–inventarisatie voor 2006 is 2273, waarvan er 577 (25,4%) ingeschreven stonden in de registers van de Kamers van Koophandel (peildatum 7 april 2007). Deze hadden in totaal 1516 inschrijvingen op hun naam staan.

In 2004 is van 367 personen nagegaan of zij bij de Kamers van Koophandel waren ingeschreven. Bij 101 personen was dit het geval: 27,5 procent.
Het kan voorkomen dat meerdere personen uit de EU–inventarisatie bij dezelfde onderneming zijn ingeschreven of dat personen meerdere malen bij dezelfde onderneming ingeschreven staan. Onderzocht is daarom bij hoeveel unieke ondernemingen de leden uit de EU–inventarisatie betrokken zijn. Op 7 april 2007 stonden zij ingeschreven bij 1136 unieke ondernemingen.

Tabel 5.4

Ondernemingen naar rechtsvorm

Rechtsvorm	Aantal	Percentage	Percentage 2004
Besloten vennootschap	514	45,2	38
Eenmanszaak	272	23,9	35
Stichting	183	16,1	16
Vennootschap onder firma	65	5,7	5
Vereniging	44	3,9	3
Overig	48	4,2	3
	1.136	**100**	**100**

In tabel 5.4 staat de verdeling van de ondernemingen waarin leden van csv's zijn betrokken weergegeven en vergeleken met de resultaten van 2004. Het aandeel van BV's is toegenomen, het aantal eenmanszaken is wat afgenomen en het aantal stichtingen is stabiel gebleven. Stichtingen en verenigingen onderscheiden

zich van andere rechtsvormen doordat gemaakte winsten niet aan personen die bij de organisatie betrokken zijn, kunnen worden uitgekeerd. Uit de literatuur (Landman, 1998, FEC, 2004, Bieleman et al. 2008) blijkt dat ook stichtingen voor criminele doeleinden worden aangewend. Zo komt uit het onderzoek van Bieleman et al. naar voren dat stichtingen onder andere betrokken waren bij subsidiefraude, faillissementsfraude, belastingfraude en oplichting. Het toezicht op stichtingen en verenigingen is vooralsnog erg beperkt. Er is geen systeem van permanent toezicht en voor de oprichting is geen VVGB verplicht gesteld. Dit in tegenstelling tot de besloten en naamloze vennootschappen die naast de VVGB ook de verplichting hebben om hun jaarstukken te publiceren.

De Kamers van Koophandel geven iedere inschrijving in het handelsregister een code waarmee de activiteit wordt aangeduid: de BIK, Bedrijfsindeling Kamers van Koophandel. De eerste twee cijfers van de BIK code geven de sectie weer (Kamer van Koophandel, 2005). Hierbinnen is weer een onderverdeling naar branches te maken. In tabel 5.5. zijn het aantal unieke bedrijven weergegeven verdeeld naar sectie.

Tabel 5.5

Ondernemingen waarbij csv–leden betrokken zijn naar sectie (april 2007)	
Sectie	Aantal
Financiële instellingen (uitgezonderd verzekeringswezen en pensioenfondsen)	220
Overige zakelijke dienstverlening	136
Groothandel en handelsbemiddeling (niet in auto's en motorfietsen)	94
Logies–, maaltijden– en drankenverstrekking (horeca)	71
Verhuur van en handel in onroerend goed	71
Handel in en reparatie van auto's en motorfietsen; benzineservicestations	66
Financiële beurzen, effectenmakelaars, assurantietussenpersonen etc.	61
Werkgevers–, werknemers– en beroepsorganisaties; levensbeschouwelijke en politieke organisaties	54
Detailhandel en reparatie van consumentenartikelen	50
Cultuur, sport en recreatie	49
Bouwnijverheid	48
Overig	139
Onbekend (geen code)	77
Totaal	**1.136**

De verdeling naar sectie en specifieker naar branche kent veel overeenkomsten met de verdeling uit 2002. Toen voerden de holdings/beheer de lijst aan, gevolgd door de groothandels, auto en horeca. In tabel 5.5 is een soortgelijke verdeling te constateren.

Kijken we specifieker naar de branches dan voeren de financiële holdings de boventoon met 17 procent van alle ondernemingen. Deze worden gevolgd door administratiekantoren voor aandelen en obligaties (3,5%), overige holdings (2,4%) en cafés (2,0 %).

Van de 1136 bedrijven verrichten er 279 (25%) naast hun hoofdactiviteiten nog één of twee nevenactiviteiten in de volgende secties, (in volgorde van voorkomen):

- groothandel en handelsbemiddeling (niet in auto's en motorfietsen);
- overige zakelijke dienstverlening;
- handel in en reparatie van auto's en motorfietsen;
- benzineservicestations;
- detailhandel en reparatie van consumentenartikelen;
- financiële instellingen (uitgezonderd verzekeringswezen en pensioenfondsen);
- verhuur van en handel in onroerend goed;
- bouwnijverheid;
- overig.

Onder de leden van criminele samenwerkingsverbanden is onderscheid gemaakt tussen kernleden en overige leden. Een persoon wordt beschouwd als kernlid als hij of zij een cruciale, veelal sturende rol heeft bij het initiatief nemen tot en organiseren van het plegen van strafbare feiten. Onder een overig lid wordt een persoon verstaan die een eigen bijdrage levert aan de criminele activiteiten van het criminele samenwerkingsverband en contacten onderhoudt met een of meer leden, maar niet als kernlid kan worden aangemerkt (DNRI, 2004b). Ook waren er enkele leden waarvan het onbekend was of ze tot de kernleden of overige leden gerekend konden worden. Van de 577 personen die bij één of meerdere ondernemingen ingeschreven stonden, is bekeken of zij als kernlid of overig lid bekend stonden. 327 personen stonden als kernlid bekend (57%), 244 personen als overig lid (42%) en van 6 personen was dit onbekend (1%). Vergelijken we dit met de gehele verdeling dan stonden van de 2273 personen 1163 bekend als kernlid (51%), 1065 als overig lid (47%) en de rest was onbekend (2%). Hier zijn dus geen opvallende verschillen tussen de cijfers van 2004 en 2006.

Naast de gegevens over welke ondernemingen op 7 april 2007 ingeschreven staan hadden wij ook de beschikking over historische gegevens vanaf 1 juni 2006. Deze

kunnen een meerwaarde geven doordat hierin ook de uitgeschreven ondernemingen en de reden van uitschrijving zijn opgenomen. In dit bestand ging het om 1308 unieke bedrijven en 652 unieke personen. Deze personen stonden in totaal 1736 maal ingeschreven bij het register van de Kamer van Koophandel.

In de EU–inventarisatie zijn 331 verschillende criminele samenwerkingsverbanden onderscheiden. Hiervan heeft bijna drie kwart (246) één of meerdere leden die staan ingeschreven bij de Kamer van Koophandel.

Per csv is gekeken of een lid ingeschreven staat bij meerdere ondernemingen. Opvallend was dat een aantal csv's veel leden hadden die actief waren binnen veel verschillende bedrijven. Zo was er één csv dat actief was bij 93 ondernemingen, gevolgd door csv's met 68, 55, 52 en 34 ondernemingen.

Misbruik van ondernemingen

Uit de hierboven gepresenteerde analyse mag niet geconcludeerd worden dat de leden van csv's de ondernemingen die op hun naam staan daadwerkelijk gebruiken bij het ontplooien van hun criminele activiteiten.

Met de beschrijvingen uit de EU–inventarisatie is bekeken of de csv's die binnen een groot aantal ondernemingen actief waren, deze ondernemingen ook zouden kunnen gebruiken voor criminele activiteiten. Zo bleek onder andere dat een csv dat als hoofdactiviteiten BTW– en faillissementsfraude had, actief was binnen 52 ondernemingen. Waaronder groothandels, financiële holdings en organisatieadviesbureaus. Een ander csv dat actief was binnen 34 ondernemingen hield zich vooral bezig met BTW–fraude en witwassen. Hiervoor maakte het gebruik van tweedehands auto's. De leden van dit csv hadden voornamelijk ondernemingen die handelden in personenauto's. Een ander csv was actief binnen de hennepteelt en had een aantal milieudelicten gepleegd. Personen uit dit csv waren ingeschreven bij een afvalinzamelingsbedrijf en een grondverzetsbedrijf. Dit geeft inzicht in de *gelegenheid* die (leden van) criminele samenwerkingsverbanden hebben om misbruik te maken van ondernemingen. Of ze die gelegenheid in de praktijk ook benutten is daarmee nog niet gezegd. Om daar enig zicht op te krijgen zijn analyses verricht op de gegevens van de EU–inventarisaties van 2006. Er is één vraag die specifiek gericht is op het gebruik van een onderneming door csv's, voor zover dit bij het opsporingsteam bekend is. Gevraagd is naar: *"Gebruik/misbruik van … legale organisaties voor het ontplooien van criminele activiteiten (bovenwereld)"*. In overzicht 5.6 zijn de bevindingen naar branche weergegeven. Net als in voorgaande jaren worden vooral horecaondernemingen en transport– en vervoersbedrijven genoemd in verband met het gebruik door criminelen bij criminele activiteiten.

Tabel 5.6

Percentage van de opsporingsonderzoeken waarin misbruik van bedrijven is geconstateerd, naar branche		
Branche	Percentage van criminele samenwerkingsverbanden (2004)	Percentage van criminele samenwerkingsverbanden (2006)
Transport	8,6	7,6
Onroerend goed	5,0	4,5
Import / export	3,6	3,9
Auto	3,2	2,2
Horeca	2,7	5,6
Openbaar bestuur	1,8	1,9
Bouwnijverheid	1,4	1,3
Reis	0,9	0,4
Automatisering	0,5	0,4
Meubel	0,5	0,4
Speelautomaten	0,5	0,4
Textielnijverheid	0,5	0,9
Anders	10,4	5,0

5.1.4 Verwachtingen voor de toekomst

Vergelijken we de resultaten voor 2007 met die uit 2004, dan zijn geen opmerkelijke verschillen te constateren. Daaruit kan de conclusie worden getrokken dat leden van criminele samenwerkingsverbanden nog steeds in de gelegenheid zijn om misbruik te maken van ondernemingen. Opvallend daarbij is dat driekwart van de csv's de mogelijkheid heeft om één of meerdere ondernemingen te misbruiken.

De Wet BIBOB en de VOGrp waren in 2004 nog maar kort geïntroduceerd. Inmiddels wordt van beide preventieve maatregelen steeds meer gebruikt gemaakt. Uit onze analyse kunnen we niet concluderen dat dit heeft geleid tot een daling van het aantal personen uit de EU–inventarisatie dat zeggenschap heeft over een onderneming. Ook de verplichting van een 'Verklaring van geen bezwaar' voor oprichters van BV's en NV's lijkt geen hoge drempel op te werpen. Verdergaande maatregelen zouden ertoe kunnen leiden dat het aantal csv–leden dat ingeschreven staat bij de Kamer van Koophandel afneemt, maar dit hoeft

nog niet te betekenen dat ze minder misbruik maken van ondernemingen. Ze zouden over kunnen gaan tot het inzetten van stromannen. Met de introductie van de Herziening Toezicht Rechtspersonen (HTR) waarbij de permanente screening wordt ingevoerd zou de drempel verhoogd moeten worden. Toekomstig onderzoek zal moeten uitwijzen of deze doelstelling wordt bereikt.

5.2 Desinformatie als contrastrategie

'Onze angst is dat een criminele groepering de volgende keer een kilo cocaïne in je tuin of je huis neerlegt. Het is lastig om dan uit te leggen dat je daar niets mee van doen hebt.' (medewerker OM in Husken, 2007, p. 197)

5.2.1 Inleiding

Desinformatie is in de *Vervolgstudie Nationaal Dreigingsbeeld* (DNRI, 2006a) genoemd als een van de vormen van 'offensieve afscherming'. Hierbij nemen criminelen niet alleen maatregelen om te voorkomen dat hun illegale activiteiten verborgen blijven voor politie en justitie ('defensieve afscherming'), maar bestrijden zij ook actief het overheidsoptreden. De andere twee vormen van offensieve afscherming zijn inschakeling van de media (bijvoorbeeld om de publieke opinie te bespelen door zichzelf als onschuldig slachtoffer van een kwaadwillende overheid neer te zetten) en het gebruik van invloedrijke derden[15]. Opgemerkt werd dat de verschillende vormen door elkaar lopen. In deze paragraaf spreken we over desinformatie, waarbij deze ook via de media kan lopen en uiteraard ook via 'invloedrijke derden' zoals journalisten en advocaten. Onder desinformatie wordt verstaan "bedrieglijke schijninformatie waarmee de feiten al dan niet moedwillig worden verdraaid of vervalst" (DNRI, 2006a, p. 60). Het doel hiervan is het verstoren van strafrechtelijke onderzoeken, het kweken van wantrouwen ten aanzien van politie en justitie en het beschadigen van reputaties van ambtenaren. Opgemerkt werd dat als het om desinformatie gaat, dit meestal pas achteraf blijkt als het waarheidsgehalte is onderzocht. Intussen kan de valse informatie invloed hebben gehad op verschillende niveaus. Als de reputatie van een officier van justitie wordt beschadigd door valse geruchten, dan zou een strafrechtelijk onderzoek verstoord kunnen worden, doordat de betreffende officier vervangen moet worden hangende een onderzoek. Uiteindelijk zouden dergelijke geruchten het vertrouwen in politie en justitie kunnen ondermijnen. In de *Vervolgstudie Nationaal dreigingsbeeld* is

[15] Deze onderwerpen werden niet als een dreiging gekwalificeerd en zijn daarom geen onderdeel van deze actualisering.

geconcludeerd dat de verspreiding van desinformatie als een 'voorwaardelijke' dreiging kon worden gezien, met name vanwege de ernst van de gevolgen en de verwachting dat desinformatie zou toenemen in de volgende jaren (DNRI, 2006a, p. 66). Onder een voorwaardelijke dreiging wordt verstaan dat het fenomeen op het moment van schrijven nog niet als dreiging kon worden benoemd, maar mogelijk wel in de nabije toekomst, onder bepaalde condities, een concrete dreiging kon gaan vormen (DNRI, 2006a; p.17).

In het kader van de commissie Van Traa werd al aangegeven dat de georganiseerde misdaad verschillende contrastrategieën benut, waaronder 'desinformatie via de media'. Criminelen zouden hebben ontdekt dat ze door middel van het verspreiden van geruchten zand in de justitiële machine kunnen strooien (Fijnaut e.a., 1996, Bijlage VII). Deze vorm van offensieve afscherming zou vooral gebruikt worden door de meer ontwikkelde criminele groepen. Als hun vrijheid of het voortbestaan van hun organisatie in het geding is, en als ze over de mogelijkheden beschikken, zouden deze criminelen gebruik maken van desinformatie. Met name de 'Hollandse netwerken' worden in dit verband genoemd. De topcriminelen uit deze netwerken beschikken vaak over contacten met journalisten, die ze ook kunnen gebruiken om valse geruchten de wereld in te sturen. Contact met de media vormt echter ook een risico voor criminelen, omdat het ook minder gewenste aandacht van politie en justitie kan trekken. Zo had het feit dat een van de grootste hasjhandelaren in de tachtiger jaren bekend werd via de media, ook grote nadelen voor de continuïteit van zijn bedrijf (Middelburg, 1996; p. 186).

Het is op dit punt van belang om stil te staan bij de overlap tussen desinformatie en het gebruik van de media. Inmiddels lijkt het onderhouden van contacten met journalisten onderdeel geworden van de praktijk van een kleine bovenlaag van criminelen. Sommige grote criminelen zijn, net als hun advocaten, 'bekende Nederlanders' geworden. Ze zijn gewend geraakt aan contacten met journalisten en gebruikten die om de publieke opinie en de politiek te beïnvloeden om zelf in een gunstig daglicht te komen en de tegenstander, politie en justitie juist minder gunstig voor te stellen (Middelburg, 1996; Husken en Lensink, 2007). Zoals andere publieke persoonlijkheden zijn zij er zich van bewust dat beelden die via de media worden gecreëerd 'even echt zijn als de werkelijkheid'[16]. Criminelen maken gebruik van de media om hun visie te geven op zaken waarbij ze betrokken zijn. Hoewel hierbij uiteraard sprake is van het gebruik van de media voor eigen belang (vandaar dat gesproken wordt van 'contrastrategie'), betekent dit nog niet dat er altijd sprake is van 'desinformatie'.

[16] Zoals de Franse filosoof Baudrillard heeft opgemerkt.

Recentelijk is bijvoorbeeld gesignaleerd dat de verdediging in strafzaken probeert om het Openbaar Ministerie van ongeoorloofde opsporingsmethoden te betichten, een onderwerp dat sinds de IRT–affaire altijd een zekere actualiteit heeft behouden. Advocaten uiten dergelijke beschuldigingen niet alleen in de rechtszaal, maar ook nadrukkelijk via kranten en televisieprogramma's. Hoewel dit bij het OM en de politie tot zorgen leidt vanwege het potentieel ondermijnend effect op het vertrouwen in de rechtsstaat, kan in dit soort gevallen niet gesproken worden van desinformatie. Behalve dat recentelijk nog gebleken is dat ook de rechter niet alle opsporingsmethoden acceptabel vindt[17], kan in het algemeen gesteld worden dat het optreden van deze advocaten in de media in het verlengde van de belangenbehartiging voor hun cliënt ligt. Ook als sommige van de 'beschuldigingen' achteraf niet door de rechter worden geaccepteerd, kunnen advocaten oprecht van mening zijn dat er iets niet deugt in het opsporingsonderzoek. Zij vinden het op hun weg liggen om dit naar voren te brengen, ook via de media. Iets anders wordt het als verdachtmakingen willens en wetens valselijk worden gefabriceerd en in omloop gebracht met de bedoeling om de waarheidsvinding juist te verhinderen, zeker als hierbij gebruik wordt gemaakt van valse verklaringen of ander bewijsmateriaal. Dan is pas echt sprake van desinformatie. Het begrip desinformatie behoeft dus een scherpe afbakening. Situaties waarin verdachten dingen zeggen die achteraf niet blijken te kloppen, worden er niet toe worden gerekend.

Hiermee is het domein van dit onderzoek in grote lijnen afgebakend. Desinformatie is het willens en wetens door leden van criminele samenwerkingsverbanden verspreiden van onjuiste of verdraaide informatie over vertegenwoordigers van politie en justitie, die er op gericht is om zand te strooien in de machinerie van politie en justitie. Het gaat niet alleen om het verspreiden van desinformatie via de media. Verdachten en getuigen die (valse) verklaringen afleggen over bijvoorbeeld corruptie of het gebruik van niet toegestane onderzoeksmethoden door de opsporingsdiensten vallen binnen het domein. Een aantal andere situaties waarin sprake is van het geven van onjuiste informatie valt dus buiten dit domein, zoals het afleggen van valse verklaringen door verdachten en getuigen en andere zaken die meer inherent zijn aan het criminele bedrijf, zoals het creëren van dwaalsporen of het doen van valse meldingen om de politie af te leiden. Een randgeval is wellicht de hypothetische situatie waarbij criminelen op de hoogte zijn van een bepaald feit over een vertegenwoordiger van justitie en deze wetenschap inzetten als ze in het nauw komen. Te denken valt aan een officier van justitie die zich in zijn privé–situatie

[17] NRC 5 februari 2008.

schuldig maakt aan huiselijk geweld. Het betreft dan weliswaar juiste informatie maar die wordt alleen ingezet om justitie te dwarsbomen. In zo'n geval kan moeilijk van 'desinformatie' worden gesproken. Het betreft overigens een theoretische mogelijkheid, concrete gevallen zijn niet bekend bij het schrijven van dit rapport.

In de *Vervolgstudie Nationaal Dreigingsbeeld* is onderzoek gedaan naar desinformatie in de periode 1990 tot medio 2006 (DNRI, 2006a). Voor het actualiseren van deze gegevens is informatie verzameld over de jaren 2006 en 2007. Dat is niet eenvoudig geweest, wat deels wordt veroorzaakt door de definitie als zodanig: Pas als bewezen is dat bepaalde informatie vals is en moedwillig door csv's in omloop werd gebracht om 'zand in de machine' te strooien, is er sprake van desinformatie. Bovendien wordt nergens centraal bijgehouden wanneer of in welke vorm er gevallen van desinformatie hebben plaatsgevonden. Kwantitatief materiaal is dus niet voorhanden. Om toch aan informatie te komen, zijn diverse interviews met teamleiders van opsporings-onderzoeken en officieren van justitie gehouden. Daarnaast hebben de projectleiders van de andere NDB– deelrapporten op hun respectievelijke onderzoeksgebieden gezocht naar eventuele gevallen. Dit heeft overigens niets opgeleverd. Ook in de EU–inventarisatie van criminele samenwerkingsverbanden werden geen gevallen gevonden.

5.2.2 Aard

De meest spraakmakende, maar tevens mislukte, casus van desinformatie is die waarbij een bekende Amsterdamse crimineel probeerde om met behulp van een vals proces–verbaal via de media de indruk te wekken dat de politie gebruik had gemaakt van niet toegestane opsporingsmethoden. De vervalsing kon al snel worden bewezen. Dit geval (waarbij mogelijk wel gebruik is gemaakt van echte documenten die op een of andere manier naar buiten gebracht moeten zijn) laat zien dat desinformatie grote risico's inhoudt voor politieonderzoeken. Als de betreffende crimineel de vervalsing zo goed had gemaakt dat het veel meer moeite had gekost hem aan te tonen, was het verhaal een eigen leven gaan leiden en had het onderzoek gemakkelijk schade op kunnen lopen. Overigens moest er ook in dit geval veel moeite worden gedaan om het verhaal dat de politie tegen de regels had gehandeld, in de media weer recht te zetten. Hiermee had deze poging dus toch een bepaalde mate van succes (De Telegraaf, 2 februari 2008).

In de interviews is meerdere malen deze recente casus (2007) als een 'schoolvoorbeeld' van desinformatie aangehaald.

Desinformatie kan in theorie op allerlei manieren plaatsvinden. Respondenten noemen diverse scenario's, van uiterst simpel (Meld Misdaad Anoniem bellen met de mededeling dat rechercheur X informatie lekt) tot zeer gecompliceerd (een campagne via de media en het fabriceren van verschillende bronnen met ondersteunend 'bewijs'). Naast het verspreiden van desinformatie via de media zou dit ook kunnen gebeuren via informanten die de Criminele Inlichtingen Eenheid op het verkeerde been zetten.
Behalve de hiervoor genoemde casus met het vervalste PV worden echter vrijwel geen concrete gevallen gemeld die te maken hebben met criminele samenwerkingsverbanden. Bij de Rijksrecherche werd wel melding gemaakt van beschuldigingen via Meld Misdaad Anoniem, maar het gaat daarbij volgens de inschatting van geïnterviewden veelal om individuele bellers die uit rancune handelen. Zo had een pooier een drugsverslaafde ingehuurd om een valse verklaring te geven over een agent die geld zou hebben aangenomen. Toen de tipgever nader aan de tand werd gevoeld, gaf hij toe dat hij was omgekocht.
Of de betrokken persoon tot de georganiseerde criminaliteit moet worden gerekend is niet helemaal duidelijk. In theorie zijn er dus legio varianten mogelijk op het thema "desinformatie", maar de variatie in concrete zaken die aan het licht gekomen zijn, is aanmerkelijk minder groot.

5.2.3 Omvang

In de vervolgstudie uit 2006 kon desinformatie niet in kwantitatieve termen worden gevangen. Bovendien deed de politie nauwelijks onderzoek naar het fenomeen. Wel werd aangegeven dat het verspreiden van desinformatie door leden van criminele samenwerkingsverbanden in Nederland daadwerkelijk aan de orde is geweest. Het ging hier om beschadigingsacties gericht tegen individuele personen, maar ook om het publiekelijk beschuldigen van politieonderdelen die verwerpelijke of niet toegestane opsporingsmethoden zouden hebben gebruikt (DNRI, 2006a, p. 62).

Ook nu zijn geen kwantitatieve gegevens aangetroffen, dat wil zeggen de EU–inventarisatie noch andere bronnen leverden concrete casussen op.
Dat neemt natuurlijk niet weg dat er sprake kan zijn van een *dark number*, ofwel gevallen van desinformatie die niet boven water zijn gekomen. De kans hierop is echter niet groot, omdat te verwachten is dat mensen die vals beschuldigd worden zich zullen verweren.

Of er in algemene zin sprake is van toe– of afname, kan door het gebrek aan een goede registratie en het ontbreken van vergelijkbare cijfers niet worden vastgesteld. Uit gesprekken met deskundigen komt de indruk naar voren dat desinformatie door criminele samenwerkingsverbanden slechts sporadisch voorkomt.

5.2.4 Betrokken personen en groeperingen

Er is slecht één casus van enige importantie aangetroffen. Deze was gerelateerd aan een vertegenwoordiger van de 'Hollandse netwerken', namelijk de groep rond Charles Zwolsman. Voor het effectief verspreiden van desinformatie is ervaring met het omgaan met de pers noodzakelijk. Ook in de vervolgstudie werd aangegeven dat offensieve afscherming, en daarmee desinformatie, vrijwel altijd hooggeorganiseerde en relatief grote criminele organisaties betreffen die (overwegend) uit autochtonen bestaan. Dat wil zeggen, dadergroepen die overwegend uit etnische Nederlanders bestaan (DNRI, 2006a: p. 62). De geïnterviewden konden geen voorbeelden geven van buitenlandse groeperingen die geprobeerd hebben desinformatie te verspreiden via de Nederlandse media. Wel werd gesteld dat de toenemende 'integratie' van buitenlandse criminelen er toe zou kunnen leiden dat ook zij gebruik gaan maken van contacten met de pers, wat nog niet hetzelfde is als desinformatie.

5.2.5 Gevolgen voor de Nederlandse samenleving

Aangezien desinformatie niet vaak voorkomt, kan ook geen sprake zijn van ernstige gevolgen voor de Nederlandse samenleving. Er worden weleens politiemensen valselijk beschuldigd en dit heeft uiteraard voor de betreffende persoon vervelende gevolgen. Incidenteel leidt dit ook tot vertraging van een politieonderzoek. Voor zover na valt te gaan is hierbij meestal geen georganiseerde criminaliteit in het geding.

Dat neemt niet weg dat toch rekening gehouden moet worden met de mogelijkheid dat desinformatie zich voor kan doen en ernstige gevolgen zou kunnen hebben. Als bijvoorbeeld de vervalsing van het proces–verbaal in de genoemde casus uit 2007 beter was geweest, was het lastiger geweest om de zaak te ontzenuwen en was hier wellicht ook meer tijd mee gemoeid geweest. De geïnterviewden stellen dat het risico op desinformatie niet al te groot is als politie en justitie een zo groot mogelijke mate van openheid betrachten over hun doelen en middelen. Zo kunnen valse beschuldigingen altijd worden ontzenuwd. Ondanks deze geruststellende woorden zijn de geïnterviewden van mening dat politie en justitie alert moeten blijven op de mogelijkheid dat processen door desinformatie worden verstoord.

Het idee dat desinformatie een potentiële mogelijkheid is waar criminelen gebruik van zouden kunnen maken leidt, ondanks de kleine aantallen, tot onrust onder medewerkers bij politie en justitie. Dit blijkt ook uit het citaat aan het begin van deze paragraaf.

5.2.6 Criminaliteitsrelevante factoren

Zoals in de inleiding aan de orde kwam, maken vooraanstaande personen, waaronder 'topcriminelen', steeds vaker gebruik van de media om hun belangen te behartigen. In het geval van criminele samenwerkingsverbanden kunnen die belangen zeer groot zijn. Criminelen en hun vertegenwoordigers vinden een welwillend oor bij journalisten, omdat misdaad een goed verkopend onderwerp is voor de pers. Het is echter toch niet gebleken dat hierdoor vaak desinformatie optreedt.

In het algemeen lijkt desinformatie, in de scherpe definitie zoals hier gehanteerd, geen erg aantrekkelijke optie voor criminele samenwerkingsverbanden. Effectieve desinformatie moet zeer zorgvuldig worden opgezet en is dus tamelijk gecompliceerd. En dan zal het rendement nog van korte duur zijn, omdat valse beschuldigingen immers kunnen worden ontzenuwd.

Omdat er steeds meer eenvoudig toegankelijke media bijkomen, zoals kliklijnen, nieuwsgroepen en weblogs, is in de vervolgstudie de verwachting uitgesproken dat het gebruik van desinformatie zal gaan toenemen (DNRI, 2006a). Er zijn echter geen gevallen geconstateerd rond deze nieuwe media.

Zoals in de interviews werd gesteld, is ook de reactie van de overheid een factor die van invloed is: door een hoge graad van openheid krijgt desinformatie niet veel kans. Respondenten noemen de wet Bijzondere Opsporingsbevoegdheden (BOB) als een factor die de transparantie bevordert.

5.2.7 Verwachtingen voor de toekomst

Aangezien desinformatie door criminele samenwerkingsverbanden slechts sporadisch voor lijkt te komen, valt er niet veel te zeggen over de ontwikkelingen in de komende jaren. Er lijkt echter geen reden om aan te nemen dat er zich plotseling veel meer gevallen zullen voordoen in de nabije toekomst. Transparantie van politie en OM zal de kans op succesvolle desinformatie verkleinen.

De ontwikkeling van nieuwe media, zoals het internet met zijn vele discussie– en nieuwsgroepen, weblogs en dergelijk biedt nieuwe mogelijkheden om op een eenvoudige en anonieme manier valse geruchten de wereld in te sturen. Dit zou er toe kunnen leiden dat het effect van afzonderlijke gevallen juist kleiner wordt (DNRI, 2006a). Er treedt als het ware een zekere 'verdunning' op, omdat er erg veel moeilijk controleerbare informatie circuleert.

5.3 Documentvervalsing

5.3.1 Inleiding

In het NDB 2004 zijn een aantal criminele werkwijzen benoemd die een dreiging zouden kunnen vormen. Het gaat hier om uiteenlopende zaken als corruptie, witwassen, het gebruik van geweld, het gebruik van ICT en document-vervalsingen. Criminelen kunnen dankzij valse of vervalste documenten hun activiteiten vergemakkelijken. Daarbij lijkt het erop dat valse of vervalste documenten volop beschikbaar zijn. Deze worden in Nederland vervaardigd, maar kunnen ook uit het buitenland komen. In bepaalde Aziatische landen worden de modernste technieken gebruikt, waardoor de vervalsingen haast niet meer van echt zijn te onderscheiden. Dat wil overigens niet zeggen dat de vervalsingen die in Nederland worden geproduceerd van mindere kwaliteit zijn. Ook criminele groeperingen in Nederland maken gebruik van nieuwe technologische ontwikkelingen en weten met behulp van software hoogwaardige vervalsingen af te leveren. Het gebruik van ICT wordt dan ook apart als een aandachtspunt genoemd. In de slotconclusie wordt de verwachting uitgesproken dat criminelen veelvuldig gebruik zullen maken van valse of vervalste documenten in de komende jaren (DNRI, 2004a).

Het domein van deze studie wordt als volgt afgebakend: het gaat om documentvervalsing in relatie tot georganiseerde criminaliteit. Onder documenten verstaan we *Nederlandse identiteitsbewijzen*. Het betreft hier alleen Nederlandse paspoorten, Nederlandse identiteitskaarten, Nederlandse verblijfsvergunningen en Nederlandse rijbewijzen. Hiermee wijkt dit rapport enigszins af van het eerste NDB, waarin het begrip ‘documenten’ breder werd opgevat. Naast identiteitsbewijzen werden ook vervalste vrachtbrieven en facturen, die andere doelen dienen, tot het onderzoeksgebied gerekend, hoewel in de uitwerking ook de nadruk lag op identiteitsdocumenten. We betrekken zowel *valse* als *vervalste* identiteitsdocumenten in de beschouwing. Onder valse documenten verstaan we documenten die volledig zijn nagemaakt, terwijl vervalste documenten authentieke documenten zijn waarin bijvoorbeeld de persoonsgegevens gewijzigd zijn.

Voor deze actualisering zijn interviews gehouden binnen de politie en er zijn gesloten bronnen geraadpleegd. Specifieke literatuur op dit terrein bleek niet voorhanden. Informatie over documentvervalsing is waarschijnlijk wel aanwezig in publicaties, maar het was niet mogelijk om hier op een gestructureerde wijze op te zoeken.

5.3.2 Aard

Het vervalsen van documenten is in het NDB 2004 vooral beschreven als een high–tech delict, op basis van de toen beschikbare bronnen. Met behulp van geavanceerde software en apparatuur kunnen vervalsingen worden gemaakt die moeilijk van echt zijn te onderscheiden. Dit gebeurt voornamelijk in het buitenland. Recente politie–informatie uit Nederland laat een ambachtelijk beeld zien van documentvervalsing in de 21ste eeuw. Huiszoekingen bij vervalsers laten zien dat ze voornamelijk werken met naalden, scharen, garens, correctiepennen, linialen, lijm, laminaatpapier, gestolen of nagemaakte stempels en fototangen, pasfoto's en typemachines. Hiermee lijkt documentvervalsing voor een groot gedeelte nog ouderwets handwerk. Het wordt met name toegepast bij het vervalsen van paspoorten door het met de hand veranderen van persoonsgegevens, het aanbrengen van andere pasfoto's of het volledig vervangen van een houderpagina. Daarnaast worden ook personal computers, laptops en scanners aangetroffen. ICT lijkt vaker te worden ingezet voor het opstellen van diverse soorten aanvragen, het maken van valse werkgeversverklaringen en het reproduceren van visa of buitenlandse documenten. Opvallend is ook dat bij documentvervalsers vaak niet alleen Nederlandse maar ook buitenlandse documenten worden aangetroffen. Soms is het mogelijk setjes van documenten te bestellen. De vervalser levert dan een paspoort met een bijbehorend rijbewijs en burgerservicenummer.

Een andere methode om aan identiteitsbewijzen te komen is het onrechtmatig aanvragen hiervan. Zo kan iemand zich valselijk uitgeven voor een gerechtigde aanvrager. Het daarop door de overheid verstrekte document is dan echt, alleen de drager is niet gemachtigd het document te bezitten. Een variant hierop is dat een legaal persoon een paspoort voor zichzelf aanvraagt maar daarbij pasfoto's van iemand anders overlegt.

Ook is een aantal postpakketten met valse of vervalste identiteitsdocumenten onderschept. Deze documenten waren in het buitenland geproduceerd, onder meer in voormalige Oostbloklanden en Thailand. Uit deze landen komen hoog-waardige producten, zoals ook al in het eerste NDB naar voren kwam (DNRI, 2004a).

5.3.3 Omvang

Door het ontbreken van een centraal registratiesysteem voor identiteitsfraude, is niet na te gaan hoe het probleem zich de afgelopen jaren heeft ontwikkeld. Er zijn wel registratiesystemen voor echtheidskenmerken, maar deze bevatten geen kwantitatieve gegevens of informatie over de vervalsers zelf. Schattingen

over de omvang van het probleem vallen dan ook vrijwel niet te maken zonder specifiek onderzoek. Op basis van het onderzoeksmateriaal kan in ieder geval worden gesteld dat tijdens huiszoekingen bij paspoortvervalsers of hun handlangers altijd meerdere paspoorten worden aangetroffen. Dit varieert van enkele tientallen tot meer dan honderd stuks. Ook de onderschepte postpakketten uit het buitenland bevatten doorgaans tientallen bewerkte paspoorten.

Verblijfsvergunningen zijn volgens respondenten goedkoper dan paspoorten; de gebruiker kan er dan ook niet internationaal mee reizen. Een verblijfsvergunning kost gemiddeld zo'n 500 euro. De prijs van een vervalst Nederlands paspoort variëren van 300 tot 2000 euro. De vervalser zelf koopt een onbewerkt, gestolen paspoort op voor een bedrag tussen de 25 en 90 euro. Een echt rijbewijs dat werd behaald door iemand die zich voordeed als een ander persoon, kostte 2000 euro.

5.3.4 Betrokken personen en groeperingen

Een groot deel van de valse identiteitspapieren die in Nederland worden aangetroffen zijn gemaakt in het buitenland. In de CBA's van de dienst Nationale Recherche worden Oost–Europeanen genoemd als vervalsers, met name Bulgaren. Ook Litouwse drugshandelaren bleken betrokken bij het vervalsen van documenten.

In Nederland lijkt het vervalsen van paspoorten een exclusief mannelijk beroep. Vrouwelijke verdachten komen alleen voor in zaken waarin valselijk een nieuwe aanvraag werd ingediend. De vervalsers die op jaarbasis tientallen documenten weten te produceren zijn allemaal van het mannelijk geslacht en van niet–Nederlandse afkomst. Hetzelfde geldt voor hun afnemers.

Het vervalsen zelf is overigens laagdrempelig te noemen. Meerdere individuen komen in de politiedossiers voor die zelf geprobeerd hebben om op eenvoudige wijze een valse identiteit te creëren. Dat kon bijvoorbeeld door een pasfoto te vervangen. Daarnaast zijn ook echt professionele vervalsers te onderkennen. Dat blijkt niet alleen uit het uitgebreide gereedschap dat zij ter beschikking hebben, maar ook aan hun productiviteit: soms tientallen documenten per week.

Professionele vervalsers werken vrijwel nooit alleen. Zij hebben voortdurend nieuwe grondstoffen (authentieke documenten) nodig om te kunnen produceren. Zij kennen diverse personen die op stelselmatige basis authentieke documenten kunnen leveren. Te denken valt aan beroepsinbrekers, straatrovers of drugsverslaafden die weten dat zij hun buitgemaakte paspoorten bij deze of

gene vervalser aan de man kunnen brengen. In andere gevallen betrekt de paspoortvervalser zijn documenten weer via een tussenpersoon die dan als heler fungeert. Vaak is zo'n heler ook betrokken bij de in– en verkoop van andere gestolen goederen.

Sommige vervalsers zijn erg voorzichtig en maken gebruik van 'katvangers', dat wil zeggen personen die de goederen voor hen willen bewaren. Op deze wijze proberen zij zo min mogelijk met belastend materiaal in contact te komen.

De paspoortvervalser moet zijn goederen aan de man zien te brengen en opdrachten binnenkrijgen. Hiertoe kan hij zelf allerlei contacten onderhouden. Maar het komt ook voor dat hij een zaakwaarnemer heeft, iemand die koper en aanbieder bij elkaar weet te brengen. Zo iemand kan daarmee enkele tientallen euro's per verhandeld paspoort verdienen.

In een enkel geval heeft een crimineel in Nederland contact met vervalsers in het buitenland. Over deze personen is weinig meer bekend dan uit sporadische telefoontaps valt op te maken. Ook hier geldt dat het mannen betreft. Zij kunnen allerlei soorten documenten leveren, ook in grotere getale.

Paspoortvervalsing lijkt soms op een publiek geheim, aldus respondenten. Binnen bepaalde wijken en etnische gemeenschappen weten veel mensen dat je voor het kopen van een vals paspoort in een of ander café of bij een bepaalde persoon terecht kan.

Het is vaak onduidelijk in hoeverre de vervalsers betrokken zijn bij andere vormen van criminaliteit. In meerdere onderzoeken kunnen de vervalsers ook in verband worden gebracht met het bezit of de handel in verdovende middelen. Anderen hebben nauwe banden met mensensmokkelaars.

De informatie is gebaseerd op wat bekend is over vervalsers bij geïnterviewde politiemensen. In deze interviews wordt ook gesteld dat over de vervalsers als zodanig niet veel bekend is, omdat ze bij politieonderzoeken veelal niet in beeld komen. Het verhoor van gebruikers van valse documenten levert vaak niet veel informatie op over de producenten.

5.3.5 Gevolgen voor de Nederlandse samenleving

Het vervaardigen van valse of vervalste identiteitsbewijzen kan niet los worden gezien van de toepassingen die deze hebben. Misdaadondernemers die structureel en op grote schaal illegale handel bedrijven beschikken veelal over valse identiteitsdocumenten waarmee ze hun illegale activiteiten mogelijk maken. "Het illegale en criminele gebruik van identiteitsdocumenten is de laatste jaren sterk toegenomen. Dit betreft met name het frauduleus gebruik met betrekking tot geldleningen/rekeningen, fraude, betaalmiddelen, money laundering, verdovende middelen (koeriers), vuurwapenhandel, (georganiseerde) illegale migratie, onder valse dekmantel politiek asiel aanvragen etc." (1994, p. 2). Ook in het NDB 2004 werd gesteld: "Valse of vervalste documenten dragen ertoe bij dat criminele activiteiten doorgang kunnen vinden, zoals mensensmokkel, mensenhandel, milieucriminaliteit, smokkel van goederen en ladingdiefstal." (DNRI, 2004a, p.110). Valse documenten kunnen ook worden gebruikt voor het huren van woningen en bedrijfsgebouwen en voor het regelen van inschrijvingen bij de Kamer van Koophandel.

De gevolgen van het gebruik van valse identiteitsdocumenten zijn dus erg divers. In het geval dat illegalen ongestoord de Nederlandse grens weten te passeren, tast dit het toelatingsbeleid aan. Economische gevolgen zijn oneerlijke concurrentie en verstoring van de arbeidsmarkt.

Uit onderzoeken naar valse en vervalste rijbewijzen bleek dat mensen die onvoldoende geschoold waren aan het verkeer deelnamen. Ook werden op basis van deze rijbewijzen certificaten voor taxichauffeurspassen aangevraagd.

De valse identiteitsbewijzen kunnen worden ingezet om betaalrekeningen te openen. Vervolgens wordt het maximale bedrag geleend waarna de rekeninghouder een andere identiteit aanneemt. Ook voor hypotheekfraude is een valse identiteit onontbeerlijk. Hierbij wordt in combinatie met een vervalste werkgeversverklaring een hypotheek van honderdduizenden euro's opgenomen.

Uit politieonderzoek blijkt dat in Nederland vervalste paspoorten opduiken in verschillende delen van de wereld zoals Syrië, Tanzania, Frankrijk, Engeland, Cyprus en Duitsland. Hierdoor kan het vertrouwen in het Nederlandse paspoort als authentiek identiteitsdocument worden ondermijnd.

5.3.6 Criminaliteitsrelevante factoren

Al jaren wordt in Nederland en elders geprobeerd om een paspoort te ontwikkelen dat niet of zeer moeilijk is na te maken of te vervalsen door er andere persoonsgegevens of een andere foto in te zetten. Deskundigen zien dit als een belangrijke ontwikkeling. Door biometrische kenmerken op te nemen zou het uitlenen en overdragen van paspoorten onmogelijk gemaakt kunnen worden. Het inzetten op opsporing van paspoortvervalsers wordt als minder efficiënt gezien.

5.3.7 Verwachtingen voor de toekomst

In 2004 werd de verwachting uitgesproken dat criminelen in toenemende mate gebruik zouden gaan maken van valse identiteitsdocumenten. In de interviews in 2007 werd dit idee bevestigd, maar in welke mate gebruik van valse papieren gemeengoed aan het worden is in het criminele milieu is nog een open vraag.

Literatuurlijst

Adviescommissie Politie en Integriteit (2000). *Van gezagsdrager naar integriteitsdrager, een visie op politie–integriteit voor de komende jaren.* 's–Gravenhage: Nederlands Politie Instituut (NPI).

Bergstein, B. (2006). Internet con artists turn to 'vishing', *USA today*, 7–12–2006. Geraadpleegd op 9 mei 2007 op http://www.usatoday.com.

Bieleman, B., Snippe, J., Stoep, R. van der, Naayer, H. & Zwieten, M. van (2008). *Stichtingen/verenigingen en criminaliteit*. Groningen–Rotterdam: Intraval.

Binational Working Group on Cross–Border Mass Marketing Fraud (2006). *Report on Phishing: A Report to the minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States*. Verkregen op 27 november 2007 op http://www.usdoj.gov.

Blizzard (2007), World of warcraft ® surpasses 8 million subscribers worldwide, 11 januari. Geraadpleegd op 9 mei 2007 op http://www.blizzard.com.

Bovenkerk F., Red. (1996). *De georganiseerde criminaliteit in Nederland.* Deventer: Gouda Quint.

Bruinsma, G. & Bovenkerk, F. (1996). *Deel II onderzoeksgroep Fijnaut: Branches. Bijlage IX van het verslag van de Parlementaire enquêtecommissie opsporingsmethoden. Inzake opsporing*. Den Haag: Sdu Uitgevers.

Bunt, H.G. van de & Kleemans, E.R. (2007). *Georganiseerde criminaliteit in Nederland. Derde rapportage op basis van de Monitor Georganiseerde Criminaliteit*. Den Haag: Boom juridische uitgevers.

Business Software Alliance (2006). *Third Annual BSA en IDC Global Software Piracy Study, may 2006* [Electronic Version]. Geraadpleegd op 26 april 2007 op http://www.bsa.org.

CBS (2006). *Digitale economie 2006*. Voorburg/Heerlen: CBS.

CBS (2007). *Telefoneren via Internet neemt snel toe*. Verkregen op 27 november 2007 op http://www.cbs.nl.

Commissie Toegangsbeheer Schiphol (2005). *Veiligheid en beveiliging door één deur, rapportage over het toegangsbeheer en het passensysteem mede in relatie tot het tegengaan van (veelvoorkomende) criminaliteit*. Den Haag, 15 juni 2005.

Currence (2007). *Gebruik iDEAL stijgt explosief*. Verkregen op 27 november 2007 op http://www.currence.nl.

Dallaway, E. (2006). Phishing costs UK banks £45.7m in 2006, *Infosecurity–magazine*. Verkregen op 27 november 2007 op http://www.infosecurity-magazine.com.

Deloitte (2006). *Deloitte 2006 Global Security Survey*. Verkregen op 26 november 2007 op http://www.agrapportenservice.nl.

DNR (2008a). *Criminaliteitsbeeldanalyse heroïne 2007*. Driebergen: Korps landelijke politiediensten, dienst Nationale Recherche.

DNR (2008b). *Criminaliteitsbeeldanalyse synthetische drugs 2007*. Driebergen: Korps landelijke politiediensten, dienst Nationale Recherche.

DNR (2008c). *Criminaliteitsbeeldanalyse mensenhandel en mensensmokkel 2007*. Driebergen: Korps landelijke politiediensten, dienst Nationale Recherche.

DNRI (2004a). *Nationaal dreigingsbeeld zware of georganiseerde criminaliteit: Een eerste proeve*. Zoetermeer: Korps landelijke politiediensten, dienst Nationale Recherche Informatie.

DNRI (2004b). *Criminele afscherming en verweving, verslag van een onderzoek voor het nationaal dreigingsbeeld zware of georganiseerde criminaliteit.* Zoetermeer: Korps landelijke politiediensten, dienst Nationale Recherche Informatie (vertrouwelijk).

DNRI (2004c). *Infrastructuren van grensoverschrijding, verslag van een onderzoek voor het nationaal dreigingsbeeld zware of georganiseerde criminaliteit*. Zoetermeer: Korps landelijke politiediensten, dienst Nationale Recherche Informatie (vertrouwelijk).

DNRI (2004d). *Criminele samenwerking, verslag van een onderzoek voor het nationaal dreigingsbeeld zware of georganiseerde criminaliteit*. Zoetermeer: Korps landelijke politiediensten, dienst Nationale Recherche Informatie (vertrouwelijk).

DNRI (2004e). *Oost–Europese criminaliteit en EU–uitbreiding, verslag van een onderzoek voor het nationaal dreigingsbeeld zware of georganiseerde criminaliteit*. Zoetermeer: Korps landelijke politiediensten, dienst Nationale Recherche Informatie (vertrouwelijk).

DNRI (2006a). *Vervolgstudie Nationaal dreigingsbeeld: Nadere beschouwing van potentiële dreigingen en witte vlekken uit het Nationaal dreigingsbeeld 2004*. Zoetermeer: Korps landelijke politiediensten, dienst Nationale Recherche Informatie.

DNRI (2006b). *Landelijke criminaliteitskaart 2005*. Zoetermeer: Korps landelijke politiediensten, dienst Nationale Recherche Informatie.

DNRI (2006c). Corruptie van allochtone dienstverleners. *Deelrapport Vervolgstudie Nationaal dreigingsbeeld zware of georganiseerde criminaliteit.* Zoetermeer: Korps landelijke politiediensten, dienst Nationale Recherche Informatie (politie intern).

DNRI (2006d). *Identiteitsfraude met behulp van phishing op het internet, verslag van een onderzoek voor de vervolgstudie NDB*. Zoetermeer: Korps landelijke politiediensten, dienst Nationale Recherche Informatie.

DNRI (2007a). *Jaaroverzicht 2006 Financial Intelligence Unit*. Zoetermeer: Korps landelijke politiediensten, dienst Nationale Recherche Informatie.

DNRI (2007b). *Nederlandse criminaliteit met een georganiseerd karakter in 2006–2007*. Zoetermeer: Korps landelijke politiediensten, dienst Nationale Recherche Informatie.

Dohmen, J. (2007). Onderzoeker: corruptielijst ondeugdelijk. *NRC–Handelsblad,* 26 september.

Duyne, P.C. van (1997). Organized crime, corruption and power. In: *Crime, Law and Social Change*, 26 (38) p. 201–238. New York: Springer.

Economist, The (2007). *A walk on the dark site*, 30 augustus. Verkregen op 27 november 2007 op http://www.economist.com

Epstein, E.J. (2005). *The Big Picture*. New York: Random House.

FEC (2004). *Quick scan Non–profitorganisaties en terrorismefinanciering*. Financieel Expertise Centrum.

Feenstra, C. (1994). *Plan van aanpak LCIDO*. Zoetermeer: Divisie Centrale Recherche Informatie.

Ferwerda, H., Arts, N., Bie, E. de & Leiden, I. van (2005). *Georganiseerde autodiefstal. Kenmerken en achtergronden van een illegale branche in beeld gebracht.* Den Haag: Ministerie van Justitie, WODC.

Fijnaut, C.J.C.F., Bovenkerk, F., Bruinsma G.J.N. & Bunt, H.G. van de (1996). *Eindrapport georganiseerde criminaliteit in Nederland. Bijlage VII van het verslag van de Parlementaire enquetecommissie opsporingsmethoden. Inzake opsporing*. Den Haag: Sdu Uitgevers.

Fortinet (2007). *Vishing: nieuwe vorm van phishing met hulp VoIP*. Geraadpleegd op 7 mei 2007 op http://www.fortinet.com.

Govcert.NL (2007). *Trendrapport 2007, Cybercrime in trends en cijfers*. Verkregen op 27 november 2007 op http://www.govcert.nl.

Huberts, L.W.J.C. & Nelen, J.M. (2005). *Corruptie in het Nederlandse openbaar bestuur, Omvang, aard en afdoening*. Utrecht: Lemma.

Huberts, L.W.J.C. & Lasthuizen, K. (2005). Tussen corruptie en corruptieparadox. *Justitiële Verkenningen*, 31(7), p. 9–23. Den Haag: Boom Juridische Uitgevers.

Huisman, W., Huikeshoven, M. & Bunt, H.G. van de (2003). *Marktplaats Amsterdam: Op zoek naar de zwakste schakel in de logistiek van criminele processen aan de hand van Amsterdamse rechercheonderzoeken*. Den Haag: Boom Juridische Uitgevers.

Huisman, W., Huikeshoven, M., Nelen, H., Bunt, H.G van de & Struiksma, J. (2005). *Het Van Traa–project: Evaluatie van de bestuurlijke aanpak van georganiseerde criminaliteit in Amsterdam*. Den Haag: Boom Juridische Uitgevers.

Hulten, M. van (2002). *Corruptie: Onbekend, onbemind, alomtegenwoordig*. Amsterdam: Boom Juridische Uitgevers.

Husken, M. (2007). *De criminele carrière van Mink K*. Amsterdam: Forum.

Husken, M. & Lensink, H. (2006). Rob B. Fiscalist van de Onderwereld. *Vrij Nederland*, 7 februari 2006.

Husken, M. & Lensink, H. (2007). De Holleeder–pers, misdaadverslaggevers over hun rol in het dossier. *Vrij Nederland 68*, 17–28 april 2007, p. 86–91.

IFPI (2007). *Digital Music Report 2007* [Electronic version]. International Federation of the Phonographic Industry. Verkregen op 26 april 2007 van http://www.ifpi.org.

Jakobsson, M. & Ratkiewicz, J., (2006). *Designing ethical phishing experiments: a study of (ROT13) rOnl query features*. Edinburgh: WWW 2006. Verkregen op 27 november 2007 op www.informatics.indiana.edu.

Jonker, N. & Kettenis, T. (2007). *Explaining cash usage in the Netherlands: the effect of electronic payment instruments*. De Nederlandsche Bank working paper, no. 136/ 2007. Verkregen op 27 november 2007 van: http://www.dnb.nl.

Jonker, N. (2005). *Payment instruments as perceived by consumers– a public survey*, De Nederlandsche Bank working paper, no. 53/ 2005. Verkregen op 27 november 2007 van http://www.dnb.nl.

Josaputra, A.L. (2005). *Georganiseerde misdaad beheerst namaak*, Ongepubliceerd proefschrift, Universiteit van Leiden.

Kamer van Koophandel (2005). *Bedrijfsindeling Kamer van Koophandel*. Verkregen op 26 november 2007 op http://assets.kvk.nl.

Kamerstukken II 2003–2004, 29454 nr 1.

Kievit, P. & Kaijen, G. (2005). *Eigen haard is goud waard*. Woningovervallen 2004. Zoetermeer: Korps landelijke politiediensten. Dienst Nationale Recherche Informatie.

Kleemans, E.R. (2007). Organised crime, transit crime, and racketeering. n: M. Tonry & C.J.C. Bijleveld (eds). C*rime and Justice in the Netherlands. Crime and Justice: A Review of Research* 35 p. 163–215.

Kleemans, E.R., Brienen, M.E.I. & Bunt, H.G. van de (2002). *Georganiseerde misdaad in Nederland: Tweede rapportage op basis van de WODC–monitor*. Den Haag: Boom Juridische Uitgevers.

Kumaraguru, P., Rhee, Y.W., Acquisti, A., Cranor, L., Hong, J. & Nunge, E. (2006). *Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System*. Verkregen op 27 november 2007 van www.cs.cmu.edu.

Kuppens, J., Vries Robbé, E. de, Leiden, I. van & Ferwerda, H. (2006). *Zware jongens op de weg. Een onderzoek naar georganiseerde diefstal in de wegtransportsector*. Arnhem: Advies– en Onderzoeksgroep Beke.

Kuran, M.S. & Tugcu, T. (2007). A *survey on emerging broadband wireless access technologies*, Computer Networks, doi:10.1016/j.comnet.2006.12.009. Verkregen op 27 november 2007 van http://netlab.cmpe.boun.edu.tr.

Landman, R.R.J. (1998). *Crimineel gebruik stichtingen*. Zoetermeer: Divisie Centrale Recherche Informatie (vertrouwelijk).

Lankhorst, F. & Nelen, J.M. (2004). *Professionele dienstverlening en georganiseerde criminaliteit: Hedendaagse integriteitsdilemma's van advocaten en notarissen*. Amsterdam: Vrije Universiteit, Faculteit der Rechtsgeleerdheid, Sectie Criminologie.

McAfee (2006), *McAfee virtual criminology report, organised crime and the Internet*. Verkregen op 27 november 2007 van http://www.mcafee.com.

McAfee (2007), *The future of security*, Sage, vol.1, no. 2. Verkregen op 27 november 2007 van http://www.mcafee.com.

McCarthy, L. (2006). *Own Your Space: Keep Yourself and Your Stuff Safe Online*, Addison–Wesley Professional: Boston.

McCusker, R. (2006). Transnational organised cyber crime: distinguishing threat from reality, *Crime, Law and social change*, vol. 46: 257–273.

McIllwain, J.S. (2005). Intellectual Property Theft and Organized Crime: The Case of Film Piracy. *Trends in Organized Crime*, 8, 4, p. 15–40.

MessageLabs (2006). Intelligence Veiligheidsjaarverslag 2005. *Cybercriminelen gaan steeds doelgerichter te werk*. Verkregen op 27 november 2007 van http://www.messagelabs.nl.

MessageLabs (2007), *MessageLabs Intelligence veiligheidsjaarverslag 2006. Een jaar vol spamgevaar: de persoonlijke aanval wint terrein*. Verkregen op 27 november 2007 van http://www.messagelabs.nl.

Middelburg, B. (1996). Onderwereldstrategieën contra de media. In: Bovenkerk F. (Red.). *De georganiseerde criminaliteit in Nederland*. Deventer: Gouda Quint, p. 185–193.

Ministerie van BZK, 2007. *Kerngegevens Nederlandse Politie* 2006. Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Ministerie van Justitie (2005). *Beleidsregels preventief toezicht op vennootschappen 2005*. Den Haag. Verkregen op 26 november 2007, http:// www.justitie.nl.

Ministerie van Justitie (2006). *De Verklaring Omtrent het Gedrag*. Verkregen op 26 november 2007 van http://www.minjust.nl.

Miranda, H. & Degen, J. (2001). *Stelen op bestelling. Een onderzoek naar autodiefstal door middel van showroomkraak*. Zoetermeer: Korps landelijke politiediensten, dienst Nationale Recherche Informatie.

Miranda, H. & Degen, J. (2004). *Stelen op bestelling 2003. Autodiefstal in georganiseerd verband*. Zoetermeer: Korps landelijke politiediensten, dienst Nationale Recherche Informatie.

Nederlandsche Bank, De (2007). *Jaarverslag Nederlandsche Bank 2006*. Amsterdam: De Nederlandsche Bank N.V.

Nelen, J. & Nieuwendijk, A. (2003). *Geen ABC, Analyse van rijksrecherche-onderzoeken naar ambtelijke en bestuurlijke corruptie*. Den Haag: Boom Juridische uitgevers.

NRC Handelsblad (2008). *Nepbom komt voor Schiphol iets te vroeg*, 7 februari.

Nu.NL (2007). *Online identiteitsdiefstal kost miljarden*, 15 januari. Verkregen op 27 november 2007 op http://www.nu.nl.

Openbaar Ministerie (2005). Aanpak georganiseerde misdaad: De strafrechterlijke aanpak van georganiseerde misdaad in Nederland 2005–2010. Den Haag: Openbaar Ministerie.

Overbruggen, T. van (2006). Gevoel van onveiligheid grote drempel voor online bankieren. In: *Banking Review*, p. 94–96. Verkregen op 27 november 2007 op http://www.bankingreview.nl.

Phillips, T (2005). Knockoff: The deadly trade in counterfeit goods. The true story of the world's fastest growing crime wave. London: Kogan Page Ltd.

Planet Internet (2007). Na phishing nu ook vishing en smishing. Verkregen op 07–05–2007 van http://www.planet.nl.

Regiopolitie Brabant–Noord (2007). *Regionale Criminaliteitsbeeldanalyse Zware en Georganiseerde Criminaliteit 2005–2006*, z.p. (vertrouwelijk).

Regiopolitie Drenthe (2007). *Regionale Criminaliteitsbeeldanalyse Zware en Georganiseerde Criminaliteit 2005–2006*, z.p. (vertrouwelijk).

Regiopolitie Gelderland–Midden (2007). *Regionale Criminaliteitsbeeldanalyse Zware en Georganiseerde Criminaliteit 2005–2006*, z.p. (vertrouwelijk).

Regiopolitie Haaglanden (2007). *Regionale Criminaliteitsbeeldanalyse Zware en Georganiseerde Criminaliteit 2005–2006*, z.p. (vertrouwelijk).

Regiopolitie Limburg–Zuid (2007). *Regionale Criminaliteitsbeeldanalyse Zware en Georganiseerde Criminaliteit 2005–2006*, z.p. (vertrouwelijk).

Regiopolitie Midden en West Brabant (2007). *Regionale Criminaliteitsbeeldanalyse Zware en Georganiseerde Criminaliteit 2005–2006*, z.p. (vertrouwelijk).

Regiopolitie Limburg–Zuid (2007). *Regionale Criminaliteitsbeeldanalyse Zware en Georganiseerde Criminaliteit 2005–2006*, z.p. (vertrouwelijk).

Regiopolitie Zuid–Holland–Zuid (2007). *Regionale Criminaliteitsbeeldanalyse zware en georganiseerde criminaliteit 2005–2006*, z.p. (vertrouwelijk).

Security.NL (2007). Duizenden World of WarCraft accounts via keyloggers gekaapt, 10 april. Verkregen op 9 mei 2007 van http://www.security.nl.

Security.NL (2007). *Trojaans paard plundert rekening ABN Amro klanten*, 15 augustus. Verkregen op 27 november 2007 van http://www.security.nl.

Sophos (2007). *Phishing, phaxing, vishing and other identity threats: The evolution of online fraud, a Sophos Whitepaper.* Verkregen op 27 november 2007 van http://www.sophos.com.

Spapens, A.C.M., Bunt, H.G. van de & Rastovac, L. (2007). *De wereld achter de wietteelt*. Den Haag: Boom Juridische Uitgevers

Staatsblad (2002). *Wet bevordering integriteitsbeoordelingen door het openbaar bestuur*, nr 347, paragraaf 1.2.

Staatscourant (2004). Beleidsregels VOG NP–RP 2004, Staatscourant 31 maart 2004, nr. 63, p. 12.

Sullins, L.L. (2006). "Phishing" for a solution: domestic and international approaches to decreasing online identity theft. *Emory International Law review*, vol. 20, p. 397–434.

Symantec (2007a). *Symantec Internet Security Threat Report; Trends for July–December 06*, Volume XI, 2007. Verkregen op 27 november 2007, http://eval.symantec.com.

Symantec (2007b). *Persbericht Internetbedreigingen in 2006 en een vooruitblik op 2007*. Verkregen op 27 november 2007, http://www.symantec.com.

Telegraaf, De (2007). *Banensite misbruikt voor phishing aanval*, 23 augustus.

Telegraaf, De (2008). *Charles Zwolsmans smokkelgeheimen*, 2 februari.

Transparancy International (2007). *Global corruption report*. http://www.transparency.org.

Trendmicro (2007). *Diefstal Linden dollars en WoW–wapens toenemend risico*. Verkregen op 09 mei 2007 van http://nl.trendmicro–europe.com.

Veldkamp, B.P. & Vries, T. de (2007). *Ontwikkeling risicodetectie model ten behoeve van het project HTR*, Fase 1. Enschede: Universiteit Twente.

Veldstra, B. (2006). Justitie: P2P sites zijn onderdeel criminele organisatie, *De Volkskrant*, 20 juni 2006.

Verlaan, J. & Dohmen, J. (2003). *Kreukbaar Nederland. Van bouwput naar beerput*. Amsterdam: Prometheus.

Voogd, M.C. de, Doornbos, F. & Huntjens, L.C.L. (2007). *Evaluatie Wet BIBOB, eenmeting*. Verkregen op 26 november 2007, http://www.justitie.nl.

Wharton (2005). *The New New Economy: Earning Real Money in the Virtual World*, Wharton School Publishing. Verkregen op 9 mei 2007 van http://knowledge.wharton.upenn.edu.

Williams, P. (2006). Cappuccino, muffin, wifi– but what about security?, *Network Security*, nr.10, p. 13–17 [Electronic version].

Bijlage 1

Overzicht van geïnterviewden

Corruptie

- Regiopolitie Amsterdam/Amstelland; hoofd Bureau Interne Onderzoeken (BIO);
- Adviseur met eigen bureau;
- Douane; hoofd Douane Informatie Centrum (DIC);
- Expertisecentrum Havens (ECH) Rotterdam; drie medewerkers;
- Koninklijke marechaussee, Expertise Centrum Luchthavens; medewerker;
- Koninklijke marechaussee; hoofd afdeling Veiligheid & Integriteit Rotterdam;
- Landelijk Parket; officier van justitie voor Rijksrechercheonderzoeken;
- Rijksrecherche, Hoofd Operationele Zaken en Adjunct; planning en controle OZ;
- Autoriteit Financiële Markten; twee medewerkers;
- FIOD–ECD Amsterdam;
- Koninklijke Notariële Beroepsorganisatie; bestuurssecretaris;
- Nederlandse Orde van Advocaten; beleidsadviseur en landelijke deken;
- FIU Nederland, MOT/BLOM meldingen; medewerker;
- Regiopolitie Amsterdam/Amstelland Bureau Zware Criminaliteit, BRT; teamleider.

Geweld tussen csv's:

- Vrije Universiteit; Universitair docent.

Intimidatie Getuigen

- KLPD – Dienst Specialistische Recherche Toepassingen.

Getuigenbeschermingsprogramma; medewerker

- Intimidatie politie en justitie;
- Landelijk Parket; Hoofdofficier van justitie;
- Landelijk Parket; Landelijk officier van justitie synthetische drugs & precursoren.

Phishing:

- Govcert.NL; medewerker;
- KLPD – dienst Nationale Recherche, Team Digitale Expertise; medewerker;
- KLPD – dienst Nationale Recherche, Team High Tech Crime; hoofd;
- FI–ISAC bijeenkomst van hoofden beveiliging van banken (tien deelnemers).

Piraterij

- Stichting BREIN; hoofd opsporing en een jurist;
- KLPD – dienst Nationale Recherche, Team Digitale Expertise; hoofd.

Desinformatie

- KLPD; Persvoorlichter;
- KLPD – dienst Nationale Recherche; Teamleider;
- Openbaar Ministerie; persvoorlichter;
- Parket Den Haag; Hoofdofficier van justitie;
- Parket Generaal; Beleidsmedewerker;
- Stichting M.; manager;
- KLPD, Bureau Veiligheid en Integriteit; hoofd.

Valse documenten

- RDW; medewerker.

Actualisering van dreigingen uit 2004

POLITIE
Korps landelijke politiediensten