Risicoanalyse georganiseerde criminaliteit : uitwerking instrumentarium en toepassing op de ICT-ontwikkelingen

Kortekaas, J.J.C.

Risicoanalyse georganiseerde criminaliteit

Risicoanalyse georganiseerde criminaliteit

Uitwerking instrumentarium en toepassing op de ICT-ontwikkelingen

Jan Kortekaas

2005 Elsevier Overheid, 's-Gravenhage

ISBN 90 5901 603 3
NUR 600

Inhoudsopgave

1. Inleiding

1.1. Context

Criminaliteitsbeheersing staat hoog op de maatschappelijke en politieke agenda.[1] De roep om meer repressie is groot. Toch is het nog maar de vraag of repressie wel toereikend is om de criminaliteit substantieel te reduceren. Sommige politici, beleidsmakers, politiefunctionarissen en academici dringen in ieder geval aan op het voorkomen van criminaliteit (preventie) in plaats van het opsporen van reeds gepleegde criminaliteit. Hierachter schuilt een tweeledige gedachte. Een eerste is dat voorkomen beter is dan genezen. Een tweede is dat het strafrecht slechts een beperkte bijdrage kan leveren aan criminaliteitsbeheersing. En, hoewel de samenleving veel heil verwacht van de politie, kan zij niet overal aanwezig zijn en heeft zij slechts een beperkt aantal bevoegdheden en instrumenten. Ook burgers, private partijen en andere overheidsorganisaties hebben daarom een rol bij de beheersing van criminaliteit.[2]

Bij grootschalige evenementen, zoals het Europese voetbalkampioenschap in 2000 en een Europese top van regeringsleiders, anticiperen de overheid en de politie op mogelijke problemen. Ondenkbaar is dat zij deze al improviserend en repressief gaan oplossen. Zij anticiperen daarentegen niet tot nauwelijks op veranderingen in criminaliteit. Natuurlijk kunnen ze wachten totdat de veranderingen zich voordoen en deze dan repressief proberen om te buigen. Maar, dan lopen ze voortdurend achter de feiten aan. Hoe eerder de overheid, de politie en andere partijen (belanghebbenden) preventieve maatregelen treffen, hoe effectiever deze kunnen zijn.[3] In sommige gevallen is vroegtijdige preventie niet mogelijk of wenselijk. In dat geval kunnen zij zich wel voorbereiden voor het geval de veranderingen zich voordoen (preparatie). Het uitgangspunt voor dit proefschrift is dat vroegtijdige preventie en preparatie door alle belanghebbenden de voorkeur hebben boven repressie door politie en justitie.

Vroegtijdige preventie en preparatie zijn alleen mogelijk wanneer de belanghebbenden voortdurend alert zijn op ontwikkelingen die kunnen leiden tot veranderingen in criminaliteit. Men spreekt in dit kader wel van het van buiten naar binnen redeneren.[4] Zo is al enige jaren sprake van een mogelijke toetreding van Turkije tot de Europese Unie (EU). Vanwege de rol van Turkije in enkele mondiale misdaadmarkten, kan het zinvol zijn dat de belanghebbenden nu al anticiperen op ongewenste veranderingen door deze in kaart te brengen. Wanneer ze tevens een beeld hebben van de waarschijnlijkheid en de mate waarin zich ongewenste effecten kunnen voordoen, kunnen ze in een vroeg stadium overwegen om wel of geen maatregelen te treffen tegen die veranderingen.

Voor vroegtijdige preventie en preparatie is dus inzicht nodig in de trits ‘ontwikkeling(en) – veranderingen – ongewenste effecten’ en in de waarschijnlijkheid van de veranderingen.

---

[1] {Werken aan vertrouwen, 2002}.

[2] Zie bijvoorbeeld {Projectgroep opsporing, 2001}, {Hauber, 2001, 339-341}, {Commission of the European Communities, 2001}, {Albrecht & Kilchling, 2002, 25}, {Williams & Godson, 2002, 312}, {Van Swaaningen, 2001}, {Van de Bunt, 1999, 14}, {Frissen, 1999, 35}.

[3] {Hauber, 2001, 326}, {Albrecht & Kilchling, 2002}.

[4] Cachet spreekt over anticiperende veiligheidszorg en bepleit eveneens het van buiten naar binnen rederenen {Cachet & Sluis, 2000, 167, 171, 173}.

Het risicoanalyse-instrumentarium is hiervoor bij uitstek geschikt. Een risico classificeert immers gedrag, gebeurtenissen, veranderingen (en dergelijke) in termen als gevaarlijk, ernstig of ongewenst. Veranderingen in criminaliteit zijn omgeven met onzekerheid en het begrip risico impliceert per definitie onzekerheid. Differentiatie is daarbij mogelijk naar zowel de waarschijnlijkheid als de ongewenste effecten.

Het gebruik van het risicoanalyse-instrumentarium ten behoeve van criminaliteitsbeheersing is niet nieuw. Sommigen spreken zelfs over risicojustitie.[5] Toch gebruikt de politie het instrumentarium nu vooral om individuen te identificeren die voor extra toezicht of opsporing in aanmerking komen (detectie). Ook benut de politie het instrumentarium soms bij eenmalige gebeurtenissen, zoals het Europese kampioenschap voetballen in 2000 en de invoering van de euro. Geen ervaring bestaat met de inzet ervan om de risico's van veranderingen in criminaliteit inzichtelijk te maken als gevolg van ontwikkelingen in de samenleving.[6]

Het totale criminaliteitspalet leent zich voor een risicoanalyse. Criminaliteit is echter een breed terrein en er zijn vele soorten te onderkennen, elk met eigen kenmerken. De effecten van een ontwikkeling kunnen daardoor variëren per soort. Bovendien vereist elk soort een aparte aanpak. Dit proefschrift richt zich op georganiseerde criminaliteit. De reden is dat beheersing hiervan één van de beleidsthema's is voor de Nederlandse politie en prioriteit heeft binnen de Europese Unie en de Verenigde Naties.[7] Daarentegen staat preventie ervan nog in de kinderschoenen.[8] Een risicoanalyse kan daarvoor het benodigde inzicht verschaffen.

Vele ontwikkelingen komen in aanmerking voor een risicoanalyse. Eén cluster van ontwikkelingen springt in het oog, namelijk de ICT-ontwikkelingen. Deze creëren tal van nieuwe mogelijkheden voor het bedrijfsleven, de overheid, de politie en de burgers. Zij hebben echter tevens een schaduwzijde. Criminelen kunnen immers ook profiteren. De ICT-ontwikkelingen zijn al jaren geleden ingezet. Desondanks heeft men de daaruit voortkomende risico's van veranderingen in georganiseerde criminaliteit nog niet systematisch in beeld gebracht.

Dit hoofdstuk verkent allereerst de vragen die het gebruik van het risicoanalyse-instrumentarium voor vroegtijdige preventie en preparatie oproept (paragraaf 1.2). Deze zijn geclusterd naar de onderwerpen: a) risicoanalyse ten behoeve van criminaliteitsbeheersing, b) risicoanalyse van veranderingen in criminaliteit, c) preventie en preparatie en d) georganiseerde criminaliteit. Die verkenning vormt het vertrekpunt voor de specificatie van het doel, de probleemstelling en de afbakening (paragraaf 1.3). Paragraaf 1.4 verantwoordt de opzet van het proefschrift en geeft een toelichting op de structuur ervan.

[5] Zie subparagraaf 1.2.1.

[6] In augustus 2004 heeft de dienst Nationale Recherche Informatie van het KLPD een eerste proeve van een 'Nationaal Dreigingsbeeld zware of georganiseerde criminaliteit' opgeleverd. Daarin worden wel enkele maatschappelijke ontwikkelingen vertaald naar veranderingen in georganiseerde criminaliteit.

[7] {Ministerie BZK, 1998}, {Criminaliteitsbeheersing, 2001}, {Van der Heijden, 2000}, {Commission of the European Communities, 2001}.

[8] {Ministerie van Justitie, 2001}, {Commission of the European Communities, 2001}.

1.2. Probleemanalyse

1.2.1. Risicoanalyse ten behoeve van criminaliteitsbeheersing

In de vorige paragraaf is aangenomen dat het risicoanalyse-instrumentarium bruikbaar is voor criminaliteitsbeheersing en dat, naast de overheid en de politie, ook anderen daarbij een rol hebben. Sommigen betwisten echter deze aannames.

Van Swaaningen, Vijver, Ericson en Haggerty plaatsen het gebruik van risicoanalyses in de bredere context van de risicomaatschappij. De Duitse socioloog Beck heeft dit concept geïntroduceerd. In de risicomaatschappij staan volgens Beck uiteenlopende maatschappelijke risico's en het beheersbaar houden daarvan centraal. Daarentegen zijn de risico's steeds omvangrijker en steeds minder beheersbaar als gevolg van de complexiteit en dynamiek van de samenleving. Het leven en handelen in onzekerheid is daardoor een fundamentele karakteristiek van de risicomaatschappij. Als reactie op de gepercipieerde afname van veiligheid en zekerheid, neemt de vraag ernaar toe. Daardoor groeit de behoefte aan risicoanalyses.[9]

Ericson en Haggerty constateren in hun boek 'Policing the risk society' dat de bestaande concepten voor het politiewerk niet afdoende zijn. In de risicomaatschappij heeft de politie (in Canada) zich de rol aangemeten om risico's te communiceren naar maatschappelijke instanties. Voor veelvoorkomende criminaliteit, zoals verkeersdelicten, inbraken en dergelijke is de politie als het ware informatiemakelaar. De politie gebruikt de beschikbare informatie en kennis in dat kader niet alleen voor de opsporing. Zij gebruikt het ook voor risicomanagement door andere instanties, waaronder verzekeringsmaatschappijen en woningbouwverenigingen. Ericson en Haggerty uiten wel twijfels bij de wenselijkheid van deze nieuwe rol van de politie.[10]

Van Swaaningen stelt dat criminaliteitsbeheersing het laatste decennium fundamenteel van karakter is veranderd. "Naast het oude, op rechtsstatelijke beginselen en het individuele 'schuld-en-boete-complex' gebaseerde strafrecht bestaat momenteel een heel ander systeem van criminaliteitsbeheersing dat is gebaseerd op risicomanagement, 'contracten', responsabilisering van derden en bestuur op afstand".[11] De risicobenadering van criminaliteit noemt men ook wel risicojustitie. "Risicojustitie gaat [….] over het op basis van wetenschappelijk onderzoek voorspellen van criminaliteit en recidivekansen, het ontwikkelen van effectieve methoden om deze statistische risico's in te perken en om het doelmatig organiseren van dergelijke interventies".[12]

De critici vragen zich af of risicojustitie wel helpt om de criminaliteit te beheersen en of het wel past in een democratische rechtsstaat. In plaats van repressie achteraf, verschuift de aandacht naar beheersing van de risico's vooraf. Het strafrecht mag dan een beperkt instrument zijn, maar het gaat bij criminaliteitsbeheersing niet alleen om doeltreffendheid en doelmatigheid. Het strafrecht heeft ook een functie als "[….] belichaming [….] van vergeldingsbehoeften, van normatieve aanspraken en van de bescherming van de

[9] {Hajer & Schwarz, 1997}, {Van der Vijver, 1998}, {Ericson & Haggerty, 1997}, {Van Swaaningen, 2001}.
[10] {Ericson & Haggerty, 1997}.
[11] {Van Swaaningen, 2001}.
[12] {Van Swaaningen, 2001}.

democratische beginselen van de rechtsstaat".[13] Als gevolg van risicojustitie richten de maatregelen zich niet op een verdachte, een status die met waarborgen is omkleed. Zij richten zich op personen die op basis van risicoprofielen zijn geselecteerd, een status zonder waarborgen. En niet alleen justitiële instanties houden zich met riskante personen bezig, maar ook niet-justitiële instanties. De centrale gedachte achter risicojustitie is verder dat criminaliteit één van de risico's is van onze samenleving. De potentiële slachtoffers moeten en kunnen zich hiertegen indekken. De overheid stuurt en controleert daarbij slechts op afstand, terwijl criminaliteitsbeheersing een fundamentele taak is van de overheid. Verder is het nog maar de vraag of gevaar calculeerbaar is en risico's voorspelbaar zijn.[14]

1.2.2. Risicoanalyse van toekomstige veranderingen in criminaliteit

Een risicoanalyse ten behoeve van vroegtijdige preventie en preparatie vereist inzicht in de trits 'ontwikkeling(en) – veranderingen – ongewenste effecten' en in de waarschijnlijkheid van de veranderingen.[15] De (toekomstige) veranderingen vormen daarbij het analyseobject.

De identificatie, selectie en interpretatie van ontwikkelingen vormen een afzonderlijk probleemveld. Het is ondoenlijk om alle ontwikkelingen te identificeren en te beoordelen op relevantie voor veranderingen. Er is een selectie nodig. Als we er een hebben geselecteerd, moeten we de ontwikkeling zelf en de richting daarvan nog interpreteren. Hoe ziet bijvoorbeeld de situatie in Afghanistan, een belangrijk land voor de mondiale heroïnemarkten, er over enkele jaren uit? Daarbij is het bovendien nog een gegeven dat de ontwikkelingen onderling interfereren en niet zomaar zijn te isoleren. Zo versterken internationalisering en de ICT-ontwikkelingen elkaar, maar overlappen ook. Toekomstgericht onderzoek is daarom lastig en omstreden. Toch bestaan diverse technieken om op systematische wijze na te denken over de toekomst, bijvoorbeeld het scenariodenken.[16]

Ook de vertaling van een ontwikkeling naar veranderingen in criminaliteit vormt een afzonderlijk probleemveld. Als we al in staat zijn om te schetsen hoe de situatie in Afghanistan er over enkele jaren uit kan zien, dan weten we nog niet wat daarvan de consequenties zijn voor bijvoorbeeld de heroïnemarkt. Die interpretatie is bij voorkeur gebaseerd op verklarende en voorspellende theorieën. Deze zijn echter zeldzaam in de sociale wetenschappen en criminologie. Voorzover ze bestaan, belichten ze een smal gebied en zijn merendeels ontworpen voor de veelvoorkomende vormen van criminaliteit.[17] Bovendien hanteren de theorieën en modellen elk een eigen invalshoek. En als we de ontwikkelingen al hebben vertaald naar veranderingen, moeten we nog de waarschijnlijkheid ervan beoordelen. Ook hier zouden verklarende en voorspellende theorieën behulpzaam zijn, maar deze ontbreken.

---

[13] {Van Swaaningen, 2001}.

[14] {Van Swaaningen, 2001}. Ook anderen benadrukken dat naast effectiviteit ook normatieve overwegingen een rol moeten spelen bij criminaliteitsbeheersing. Dit mede in verband met de zwaarte van de middelen die de overheid inzet {Van de Bunt, 1999}, {Frissen, 1999}.

[15] Zie paragraaf 1.1.

[16] Zie {'t Hart, 1998}, {Dunn, 1994} en {In 't Veld & Van der Knaap, 1994} voor enkele technieken en problemen daarbij.

[17] {Hauber, 2001, 326-327, 329}, {Bovenkerk, 2001, 13}. Ook Bruinsma benoemt in een ander kader dat criminologische inzichten ontoereikend zijn om concrete gegevens in een interpretatiekader te plaatsen, criminaliteit te verklaren, te vergelijken en te toetsen {Bruinsma, 1996}.

De aanname in dit proefschrift is dat de gelegenheidstheorie, oorspronkelijk aangeduid als 'routine activity theory', een geschikte theorie is om veranderingen in criminaliteit te identificeren en de waarschijnlijkheid daarvan te bepalen. Deze theorie is toegespitst op het macroniveau[18] en dat sluit aan bij het doel van de risicoanalyse, namelijk bijdragen aan vroegtijdige preventie en preparatie.[19] Een nadeel is dat de theorie is gebaseerd op 'predatory crime', in Nederland getypeerd als vermogenscriminaliteit.[20] Van Dijk e.a. stellen echter dat de theorie breder bruikbaar is. Dit blijkt ook uit de toepassing door Van den Anker en Hoogenboom voor milieucriminaliteit en voor georganiseerde criminaliteit door Bovenkerk en Van Dijk.[21] De gelegenheidstheorie is evenmin voorspellend van aard, maar verschaft wel aangrijpingspunten voor de vertaling van ontwikkelingen naar veranderingen (zie hierna).

Cohen en Felson zijn de grondleggers van de gelegenheidstheorie. De aandacht daarin gaat primair uit naar de gelegenheden waaronder criminele gebeurtenissen plaatsvinden. Dit in tegenstelling tot theorieën die uitgaan van de daders of slachtoffers. Cohen en Felson stellen dat "[….] the convergence in time and space of three elements (motivated offenders, suitable targets, and the absence of capable guardians) appears useful for understanding crime rate trends". Zij bestuderen in hoeverre de dagelijkse routinematige activiteiten de criminaliteit beïnvloeden. Het gaat dan bijvoorbeeld om de activiteiten thuis en op het werk. Om de criminaliteit te begrijpen, moeten we dus het dagelijks leven bestuderen[22] en de ontwikkelingen daarin. Dat laatste sluit aan bij de behoefte om ontwikkelingen in de samenleving te vertalen naar veranderingen in criminaliteit.

De gelegenheidstheorie benoemt dus drie elementen die moeten convergeren, ook wel aangeduid als gelegenheidsfactoren. Een *gemotiveerde dader* is ieder individu met zowel een criminele voorkeur als met de vaardigheid om die voorkeur te realiseren. Een *geschikt doelwit* zijn personen of goederen die vanuit het perspectief van de dader waarde hebben of begerenswaardig zijn. Een *bekwame bewaker* is hij die in staat is om te vermijden dat de gemotiveerde dader strafbare feiten pleegt. Veelal zijn het gewone burgers, buren, werknemers en dergelijke in plaats van de politie en particuliere beveiligers. De convergentie van een geschikt doelwit én de afwezigheid van een bekwame bewaker heeft volgens Cohen en Felson een grotere invloed op criminaliteit dan een vergroting van de structurele condities die daders motiveren.[23]

De interpretatie van de gelegenheidstheorie loopt op onderdelen uiteen. Van Dijk e.a., Van den Anker en Hoogenboom en Bovenkerk noemen het aspect 'convergentie in tijd en plaats' niet expliciet. Wel hebben zij het over aan- of afwezigheid van de drie elementen. De elementen dader en sociale controle in plaats van 'capable guardians', noemen de genoemde auteurs allen. Verschillen ontstaan bij een 'geschikt doelwit'. Van Dijk e.a. noemen dit element nog wel. Van den Anker en Hoogenboom hebben het over 'geschikte mogelijkheden'. Bovenkerk heeft het over 'objectieve gelegenheid voor criminaliteit'. Verder verschillen zij van mening over de mate waarin de elementen de criminaliteit beïnvloeden. Van Dijk e.a. nemen de stelligheid van Cohen en Felson over: zij bepalen het

[18] {Clarke & Felson, 1993, 9}, {Van den Anker & Hoogenboom, 1997} en {Van Dijk e.a., 1996, 105}.
[19] Zie paragraaf 2.5 voor de onderbouwing hiervan.
[20] Naylor beschrijft de verschillen tussen predatory crime en georganiseerde criminaliteit {Naylor, 1997, 3-4}.
[21] {Van Dijk e.a., 1996, 132, 255}, {Van den Anker & Hoogenboom, 1997}, {Bovenkerk, 2001}.
[22] {Cohen & Felson, 1979}, {Felson & Rutgers, 2001}, {Mitchell Robinson, 2001}.
[23] Idem.

niveau van criminaliteit. Van den Anker en Hoogenboom nuanceren dit en stellen dat deze het niveau van criminaliteit mede bepalen. Bovenkerk nuanceert dit nog meer: er is kans op criminaliteit wanneer zij aanwezig zijn.[24] Van den Anker en Hoogenboom introduceren het begrip gelegenheidsstructuur. Dit omschrijven zij als "[….] een mogelijkheid, omstandigheid, of gesteldheid die geschikt is voor het verrichten van een bepaalde criminele handeling".[25] De relatie tussen dit begrip en hun interpretatie van de gelegenheidstheorie is niet duidelijk.

Dit proefschrift sluit zoveel mogelijk aan bij de oorspronkelijke uitwerking van Cohen en Felson. Zij benoemen drie elementen (gelegenheidsfactoren): gemotiveerde dader, geschikt doelwit en 'de afwezigheid van een bekwame bewaker'. Deze zijn verder aangeduid als de gelegenheidsfactoren 'dader', 'doelwit' en 'sociale controle'. Andere factoren bepalen waar en wanneer de convergentie van die drie gelegenheidsfactoren plaatsvindt. Cohen en Felson richten daarbij hun aandacht op de dagelijkse activiteiten.[26] Deze laatste categorie factoren vormt dus een apart type gelegenheidsfactor, verder aangeduid als 'locatie en tijdstip'.

Niet duidelijk is wat gelegenheid inhoudt. We zouden een ontwikkeling in de samenleving kunnen beschouwen als een gelegenheid. In deze optiek creëren bijvoorbeeld de ICT-ontwikkelingen een gelegenheid voor (een verandering in) criminaliteit. Een andere benadering is om juist de convergentie op een bepaalde locatie en een bepaald tijdstip te beschouwen als gelegenheid. Een voorbeeld daarvan is de aanwezigheid van een laptop op een locatie en tijdstip waar ook een dader is, ondanks de aanwezigheid van digitale camera's. Hiervoor is de convergentie op een locatie en tijdstip als een apart type gelegenheidsfactor benoemd. Bovendien beïnvloeden ontwikkelingen in de samenleving alle gelegenheidsfactoren, inclusief de locatie en het tijdstip van convergentie. Daarom is de voorkeur gegeven aan de eerste benadering. De gelegenheid is in dat perspectief dus de veroorzaker van een verandering. In dit proefschrift gaat het dan om een ontwikkeling in de samenleving, meer specifiek om de ICT-ontwikkelingen.

Hoewel de gelegenheidstheorie geen voorspellende theorie is, geeft zij wel aangrijpingspunten voor de vertaling van ontwikkelingen naar veranderingen. We kunnen bijvoorbeeld nadenken of de ICT-ontwikkelingen van invloed zijn op de gelegenheidsfactoren en tot welke veranderingen dat zou kunnen leiden. De ICT-ontwikkelingen hebben bijvoorbeeld als gevolg dat er nieuwe objecten zijn gekomen voor criminelen, zoals laptops (doelwit). Zij scheppen verder nieuwe instrumenten voor preventie tegen inbraken en voor de politie (sociale controle). Tevens leiden zij ertoe dat mensen vaker thuiswerken en hun laptop meenemen (locatie en tijdstip). Hierdoor kunnen zich allerlei wijzigingen voordoen in vermogenscriminaliteit. Wijzigingen in doelwitten, daders, locaties en tijdstippen kunnen we beschouwen als aparte soorten veranderingen. Dat ligt anders voor sociale controle. Wijzigingen daarin kunnen weliswaar van invloed zijn op criminaliteit, maar vormen een verandering in de omgeving in plaats van in criminaliteit. Deze blijven daarom verder buiten beschouwing, maar spelen wel een rol bij de beoordeling van de waarschijnlijkheid (zie hierna). Naast deze soorten veranderingen die voortkomen uit de gelegenheidsfactoren, moeten we ook rekening houden met veranderingen in criminaliteitsvormen. Ook

[24] {Van Dijk e.a., 1996, 132}, {Van den Anker & Hoogenboom, 1997}, {Bovenkerk, 2001, 148}.
[25] {Van den Anker & Hoogenboom, 1997}.
[26] {Cohen & Felson, 1979}, {Felson & Rutgers, 2001}, {Mitchell Robinson, 2001}.

daarin zijn uiteraard veranderingen mogelijk.[27] Op basis van deze redenering kunnen we daarom vijf soorten veranderingen benoemen, namelijk in: a) doelwitten, b) daders, c) locaties, d) tijdstippen en e) criminaliteitsvormen.

Naast de typering naar soorten, kunnen we veranderingen ook rubriceren op basis van de aard ervan (zie figuur 1.1). Er kunnen nieuwe criminaliteitsvormen (daders et cetera) bijkomen. Hacken is bijvoorbeeld een relatief nieuwe vorm van criminaliteit en houdt verband met de ICT-ontwikkelingen. Naast nieuw, kan het ook gaan om wijzigingen in de omvang, de aard, en/of de ernst van bestaande criminaliteitsvormen. Overigens is het onderscheid tussen nieuw of bestaand niet altijd scherp aan te brengen. Hacken is weliswaar een relatief nieuwe vorm van criminaliteit, maar het hacken van creditcardgegevens vormt evenzogoed een verandering in een bestaande vorm van criminaliteit (creditcardfraude). Ook het onderscheid naar aard en ernst valt niet altijd goed te maken. De aard van de criminaliteit bepaalt veelal ook de ernst. Verder neemt (de omvang van) de ernst toe als een bestaande criminaliteitsvorm toeneemt. Bovendien vormt de ernst van een verandering eigenlijk een uitwerking van de ongewenste effecten van een verandering en niet van de verandering zelf (zie verderop). Daarom blijft dit aspect buiten beschouwing.

Verandering in bestaande of nieuwe criminaliteits-vorm:	**Aard van de verandering:**		
	Verandering in omvang criminaliteitsvorm	*Verandering in aard criminaliteitsvorm*	*Verandering in ernst criminaliteitsvorm*
Bestaand	Toename creditcardfraude	Verschuiving van vervalsing fysieke naar digitale credit-cardfraude Verschuiving van drugs-handel naar mensensmokkel	Verschuiving van auto-diefstal zonder geweld naar autodiefstal met geweld (onder dwang afgeven van sleutels)
Nieuw	Hacken van website om aan (creditcard)gegevens te komen Biotechnologiecriminaliteit		

Figuur 1.1 Denkbare veranderingen in criminaliteitsvormen

De beide genoemde invalshoeken kunnen we combineren (zie figuur 1.2). De aandacht in dit proefschrift gaat vooral uit naar de eerdergenoemde soorten veranderingen. Deze soorten zijn nader onder te verdelen naar de aard van de verandering.

[27] De gelegenheidstheorie is van oorsprong gericht op vermogenscriminaliteit. Georganiseerde criminaliteit omvat echter een breed spectrum van criminaliteitsvormen.

Soort verandering	Verbijzondering
1 Doelwitten	1a Nieuw soort doelwit
	1b Toename criminaliteit met betrekking tot bestaand soort doelwit
	1c Verschuiving tussen soorten doelwitten
2 Daders	2a Nieuwe soort daders
	2b Toename bestaande soort dader
	2c Verschuiving tussen soorten daders
3 Locaties	3a Nieuwe soort locatie
	3b Toename bestaande soort locatie
	3c Verschuiving tussen bestaande soorten locaties
4 Tijdstippen	4a Nieuw tijdstip
	4b Toename op bestaand tijdstip
	4c Verschuiving tussen tijdstippen
5 Criminaliteitsvormen	5a Nieuwe criminaliteitsvorm
	5b Toename in bestaande criminaliteitsvorm
	5c Verschuivingen tussen criminaliteitsvormen

Figuur 1.2 Typologie van veranderingen

De gelegenheidstheorie is niet alleen bruikbaar voor de vertaling van ontwikkelingen naar veranderingen, maar ook voor de beoordeling van de waarschijnlijkheid. De mate van invloed van een ontwikkeling op één of meer gelegenheidsfactoren bepaalt immers de waarschijnlijkheid van de verandering. De gelegenheidsfactoren kunnen we daarom ook gebruiken als risicofactoren.[28]

De gelegenheidstheorie geeft daarentegen *geen* aangrijpingspunten voor de bepaling van de ongewenste effecten van veranderingen. Wel aangrijpingspunten verschaffen de kenmerken van de veranderingen. Wanneer bijvoorbeeld een verschuiving zou plaatsvinden van autochtone naar buitenlandse daders, zouden we dat als ongewenst kunnen betitelen. Of een verandering die leidt tot meer corruptie zouden we als ongewenst kunnen benoemen. Op deze wijze zijn echter de effecten van de verandering in de samenleving niet duidelijk. Een andere benadering is om de ongewenste effecten te bepalen op grond van de belangen die worden aangetast. Een toename van mensensmokkel leidt bijvoorbeeld tot meer uitgaven voor de opvang van vluchtelingen en een daling van de acceptatie van het asielbeleid. Op deze wijze ontstaat wel inzicht in de ongewenste effecten in de samenleving.

De tweede benadering sluit beter aan bij de gedachte om ook anderen te betrekken bij criminaliteitsbeheersing.[29] De expliciete benoeming van de belangen die in het geding zijn, kan bijdragen aan de bewustwording bij andere partijen. Zij kunnen zo in hun belangenafweging ook de ongewenste effecten van criminaliteit betrekken. Een strenger asielbeleid vergroot bijvoorbeeld de noodzaak voor vluchtelingen om zich te wenden tot mensensmokkelaars. Mensensmokkel is daardoor een neveneffect van het asielbeleid, maar ondermijnt het ook. Een tweede voordeel is dat deze benadering aangrijpingspunten biedt om expliciete doelstellingen te benoemen voor criminaliteitsbeheersing. Hierdoor is de effectiviteit beter te beoordelen en kan men achteraf de aannames die daaraan ten

[28] Zie paragraaf 2.2 voor een uitwerking van dit begrip.
[29] Zie paragraaf 1.1.

grondslag lagen toetsen. Een derde voordeel is dat beleidsmakers criminaliteitsbeheersing kunnen richten op de meest ongewenste effecten. De preventie van bijvoorbeeld mensensmokkel kan zich richten op: alle vormen van mensensmokkel, smokkelaars die de buitenlandse betrekkingen het meest schaden of op smokkelaars die de overheid op hoge kosten jagen voor de opvang. De benadering past daarnaast beter bij de fase van agendavorming, waar het voor een groot deel gaat om belangenafwegingen en -tegenstellingen (zie subparagraaf 1.2.3). De tweede benadering sluit daarom goed aan bij een risicoanalyse die een bijdrage moet leveren aan vroegtijdige preventie en preparatie door belanghebbenden.

Deze benadering roept wel de vraag op waar de grens ligt in de analyse. Eén verandering in criminaliteit kan immers een keten van andere veranderingen in gang zetten en direct of indirect een grote diversiteit van belangen aantasten. Stel dat de drugshandel toeneemt. Een drugshandelaar voorziet verslaafden van drugs. Deze verslaafden kunnen gezondheidsproblemen krijgen, overlast veroorzaken of criminaliteit plegen om aan drugs te komen. Zijn dit allemaal de ongewenste effecten van de drugshandel of juist van de verslaving? Zonder vraag naar drugs is er immers ook geen aanbod van drugs. Omgekeerd geldt natuurlijk dat er zonder aanbod van drugs geen vraag is. Drugshandel kan ook leiden tot andere ongewenste effecten. De drugshandel schaadt de reputatie van Nederland in het buitenland. De drugshandelaren wassen de verdiende gelden wit, hetgeen op zich al weer leidt tot een keten van ongewenste effecten. Bestrijding van de drugshandel kost de samenleving bovendien veel geld. Drugshandel valt deels onder georganiseerde criminaliteit, deels ook niet. Wat zijn nu de ongewenste effecten van dat deel van de drugshandel waar georganiseerde criminaliteit zich op richt? En bij welke toename van de drugshandel treden die daadwerkelijk op? Verder kunnen we te maken krijgen met verschuivingen tussen criminaliteitsvormen. Welke effecten moeten we beoordelen bij een verschuiving van drugshandel naar wapenhandel en mensensmokkel? De keuzen zijn deels analytisch van aard wanneer ze randvoorwaardelijk zijn om een transparante analyse te kunnen uitvoeren. Maar, voor een groot deel is die keuze normatief. Dat laatste geldt zeker wanneer we gewichten toekennen aan de belangen om te komen tot een eindoordeel in termen van ernstig of niet-ernstig. Deze normatieve keuze ligt niet op het terrein van een wetenschappelijke onderzoeker. Wel kan hij op zoek gaan naar formele uitgangspunten. Hij kan ook de gezagsdragers de keuzen voorleggen en vragen naar de gewichten van de afzonderlijke belangen. De tweede benadering vereist dus een kader om de ongewenste effecten te bepalen.

De vertaling van een ontwikkeling naar veranderingen en de beoordeling van de ongewenste effecten en waarschijnlijkheid daarvan, zijn dus niet eenvoudig. Het *achteraf* evalueren van de juistheid van de analyse is evenmin eenvoudig. We zullen er nooit goed achter kunnen komen in hoeverre die juist was. Daaraan liggen meerdere redenen ten grondslag. Allereerst kunnen de afzonderlijke partijen maatregelen hebben getroffen om de risico's te beheersen, waardoor de situatie er anders uit komt te zien. Maar er zijn ook andere redenen. Het empirische beeld van criminaliteit is beperkt. Criminelen doen hun best om niet op te vallen. Slachtoffers doen lang niet altijd aangifte. De politie besteedt niet aan alle vormen van criminaliteit evenveel aandacht. Zij registreert gegevens niet eenduidig en in uiteenlopende bestanden. Verder gelden strikte privacyeisen voor gegevensvastlegging, waardoor de politie lang niet alle soorten gegevens mag vastleggen of lange tijd mag behouden. Informatie die niet direct bijdraagt aan de strafrechtelijke

bewijsvoering, legt de politie niet vast. Contextuele informatie, van belang voor preventie of beleidsevaluatie, is daardoor schaars.[30] Als er al gegevens beschikbaar zijn die wijzen op een verandering, is de oorzaak daarvan niet eenduidig te bepalen. Daders, slachtoffers, de wetgever en opsporingsinstanties passen zich aan aan het gedrag van elkaar. Soms zijn ogenschijnlijke veranderingen slechts te wijten aan registratie-effecten. De politie heeft dan bijvoorbeeld een ander informatiesysteem in gebruik genomen of hanteert een andere classificatie. Het verklaren van waargenomen veranderingen in criminaliteit vereist daardoor een zorgvuldige interpretatie, terwijl een expliciet interpretatiekader ontbreekt. Bovendien hebben alle onderzoeksmethoden hun beperkingen.[31]

De conclusie dringt zich op dat een wetenschappelijk onderbouwde analyse van de trits 'ontwikkeling(en) - (waarschijnlijkheid van) veranderingen in criminaliteit - ongewenste effecten' moeilijk is. Dit geldt overigens ook voor analyses op andere beleidsterreinen. Criminaliteit doet wat dat betreft niet onder voor de andere problemen waarvoor de overheid zich ziet gesteld.[32] Desondanks moet de overheid op deze problemen een antwoord zien te vinden of besluiten niets te doen. Een analyse kan bijdragen aan het inzichtelijk maken van de problematiek. Het alternatief is onderbuikgevoel. Een analyse kan niet alle onzekerheid wegnemen en op alle vragen antwoord geven. Het is de taak van de besluitvormers om besluiten te nemen ondanks de onzekerheid. Het is de taak van de analist om een complexe materie op verantwoorde wijze inzichtelijk te maken.[33]

1.2.3. Preventie en preparatie

Preventie is een beïnvloedingsmechanisme om te voorkomen dat criminaliteit zich voordoet of om de kans daarop te verkleinen. Er zijn diverse soorten preventie denkbaar. Een *eerste* indeling is die op basis van de aangrijpingspunten voor preventie: de (potentiële) daders, de (potentiële) slachtoffers en (criminogene) situaties.[34] Op basis daarvan onderscheidt men dadergerichte, slachtoffergerichte en situationele preventie.[35, 36] Een *tweede* indeling is gebaseerd op de verschillende tijdstippen om preventieve maatregelen te treffen. Preventie kan starten op het moment dat nog geen sprake is van een verandering, hier verder aangeduid als 'vroegtijdige preventie'. Een ander moment is wanneer er al aanwijzingen zijn dat zich een verandering voordoet, zonder dat die al op grote schaal plaatsvindt. Preventie kan ook beginnen wanneer dat juist wel al het geval is. Een *derde* indeling gaat uit van het niveau waarop men preventieve maatregelen kan treffen: het macro-, meso- of microniveau. Van Dijk e.a. introduceren nog een andere indeling, de *vierde*. Zij combineren het tijdstip en het niveau en onderscheiden zo primaire, secundaire en tertiaire criminaliteitspreventie. Primaire preventie is gericht op het verminderen van de vatbaarheid van de samenleving voor criminaliteit. Het gaat om een algemene vorm van preventie. Secundaire preventie is gericht op het verminderen van

[30] {Bruinsma, 1996}, {Koppenol, 1999}, {Meesters e.a., 1999}, {Kortekaas & Aalbersberg, 1996}, {Kortekaas, 1996}, {Commission of the European Communities, 2001}.
[31] Zie hiervoor bijvoorbeeld {Bruinsma, 1996}.
[32] Bijvoorbeeld {Dunn, 1994, 146}, {Bruinsma, 1996, 86}, {In 't Veld & Van der Knaap, 1994, 133}, {Van Heffen, 1993, 74-75} behandelen het type problemen waar de overheid mee te maken krijgt. Frei werkt de bijdrage uit van de sociale wetenschappen aan het buitenlandse veiligheidsbeleid, een terrein met soortgelijke kenmerken als (georganiseerde) criminaliteit {Frei & Ruloff, 1989}.
[33] {Frei & Ruloff, 1989}.
[34] {Van Dijk e.a., 1996}, {Hauber, 2001, 326}.
[35] {Cohen & Felson, 1979}, {Felson & Rutgers, 2001}, {Mitchell Robinson, 2001}, {Hauber, 2001, 329}.
[36] Men hanteert regelmatig de gelegenheidstheorie als theoretisch kader voor situationele preventie.

risicovolle situaties of het vergroten van de weerbaarheid van specifieke risicogroepen. De eerste symptomen hebben zich al voorgedaan. Tertiaire preventie is gericht op situaties waarin criminaliteit al is voorgekomen en/of op individuen die al dader of slachtoffer zijn (geweest). Het doel is om te voorkomen dat de situatie zich opnieuw voordoet en iemand opnieuw als dader of slachtoffer fungeert.[37] Tot slot is nog een *vijfde* indeling te onderscheiden, namelijk een indeling op basis van de instantie die preventieve maatregelen treft. Voorbeelden daarvan zijn bestuurlijke en politiële preventie.

In sommige gevallen is vroegtijdige preventie (nog) niet mogelijk of wenselijk. Wanneer weinig bekend is over het risico of weinig kennis beschikbaar is hoe te handelen, is de basis voor preventie te smal.[38] Soms zijn preventieve maatregelen onwenselijk, omdat ze andere belangen te veel schaden. Het gebruik van e-mail door criminelen is bijvoorbeeld nauwelijks te voorkomen, tenzij men een ernstige inbreuk wil maken op de privacy.

Indien vroegtijdige preventie (nog) niet mogelijk of wenselijk is, kan men preparatie overwegen. Preparatie behelst de voorbereiding voor het geval de ongewenste situatie zich voordoet. Voorbeelden daarvan zijn het opstellen van draaiboeken, het opleiden van medewerkers, het aanschaffen van materiaal en het creëren van wettelijke bevoegdheden voor opsporingsinstanties. Naar analogie van de soorten preventie, kunnen we ook diverse vormen van preparatie onderscheiden. Soms is zelfs daarvoor het inzicht ontoereikend. In dat geval rest slechts een afwachtende houding of het verder inzichtelijk maken van de problematiek.

Vroegtijdige preventie en preparatie, verder aangeduid als vroegtijdige criminaliteits-beheersing, bestaan niet alleen uit het treffen van maatregelen. Tussen het moment dat men een probleem of risico onderkent en het moment dat men daadwerkelijk maatregelen treft, zit een heel proces (het beleidsproces). Sommige auteurs onderscheiden in dat proces fasen.[39] Hoewel de indeling varieert, gaat het ruwweg om de volgende fasen: agenda-vorming, beleidsvorming, beleidsuitvoering en beleidsevaluatie. Tijdens de agendavorming wegen de belanghebbenden af in hoeverre ze de risico's op de agenda willen plaatsen en beleid willen vormen ter beheersing ervan. Wanneer een risico eenmaal op de agenda is geplaatst, komt de beleidsvorming in beeld. Naast een verdere analyse van de problema-tiek, gaat men nadenken over de opties voor maatregelen, de voor- en nadelen daarvan, wie de maatregelen kan of moet treffen en de tijdsvolgorde daarvan. Uiteindelijk resulteert deze fase in geformuleerd beleid. Dan treedt de derde fase in werking. De gespecificeerde instanties gaan het beleid uitvoeren. In de vierde fase, beleidsevaluatie, bekijkt men in hoeverre het geformuleerde beleid tot de gewenste effecten leidt. De wijze waarop beleid totstandkomt, verloopt in de praktijk niet zo rationeel als is weergegeven. Het voert te ver om daar nader op in te gaan evenals op de afzonderlijke fasen. Wel komen hierna kort enkele aspecten van de agendavorming aan bod.

Met name de agendavorming is van belang voor een risicoanalyse ten behoeve van vroegtijdige criminaliteitsbeheersing. Het gaat immers om de risico's van veranderingen

[37] Vrij naar {Van Dijk e.a., 1996, 142}.

[38] Interpretatie van verschillende strategieën die Wildavsky (1988) heeft benoemd voor de omgang met risico's in {Van Duin, 1994}.

[39] Teisman schetst een theoretisch kader voor de reconstructie van beleidsprocessen. Hij onderscheidt drie modellen: het fasenmodel, het stromenmodel en het rondenmodel {Teisman, 1993,19-24}. De beschrijving hier betreft het fasenmodel, een model dat volgens sommigen (onder andere) het verloop van het beleidsproces te rationeel weergeeft.

die zich nog niet voordoen en daarom nog niet op de agenda staan. Voordat belanghebbenden daar daadwerkelijk op willen reageren, moeten de risico's vele hindernissen nemen. Zij komen namelijk niet vanzelfsprekend op de agenda van beleidsmakers, bestuurders, Openbaar Ministerie, politie en anderen. Dat geldt zeker voor risico's die nog niet zijn waargenomen. Er is dan slechts sprake van vermoedens. Sommige risico's negeren ze lange tijd, terwijl ze andere als urgent beschouwen. Sommige risico's definiëren ze weg, terwijl ze andere tot een buitenproportionele omvang opblazen.[40] De belanghebbenden moeten eerst overtuigd raken van de noodzaak van de problematiek. Men wil feiten zien, terwijl dat bij nieuwe risico's nauwelijks mogelijk is.[41] Het gaat om beredeneerde aannames. Verschillende partijen en experts hanteren hierbij andere werkelijkheidsdefinities en zij bekritiseren de visies en aannames van elkaar. Wanneer de politie andere instanties bijvoorbeeld wijst op betrokkenheid bij criminaliteit, kan een defensieve houding ontstaan. Zo ontkenden de banken begin jaren '90 dat ze (ongewild) betrokken waren bij witwasoperaties. Na enkele schandalen bij bankfilialen, konden de banken er niet langer omheen.[42] In een analyse kunnen zaken aan de orde komen die men soms liever niet hoort. Een (niet-verwijtbare) betrokkenheid van banken bij georganiseerde criminaliteit komt het imago van banken niet ten goede. Betrokkenheid van allochtonen bij criminaliteit was lange tijd niet bespreekbaar. Omgekeerd kan een risicoanalyse vermeende problemen juist weerspreken. Maar, niet iedereen heeft belang bij nuancering van een problematiek. Een voorbeeld daarvan was de kwestie omtrent de dioxinekippen in 1999. De staatssecretaris van Landbouw werd toen heftig bekritiseerd voor het bagatelliseren van de kwestie. De politiek heeft verder de neiging om de aandacht te concentreren op problemen die nu actie vereisen in plaats van op veranderingen die zich in de toekomst zouden kunnen voordoen. Volgens Hogwood en Gunn, en Shubik bestaat er voor een ambtenaar of een politicus geen prikkeling om zich bezig te houden met de toekomst. Niets doen is vaak een wijs politiek besluit.[43] Daarnaast hebben media een belangrijke rol om risico's op de agenda te plaatsen. Deze hebben echter meer belangstelling voor incidenten, zoals een terroristische aanslag, dan voor permanente risico's zoals roken of criminaliteit.[44]

Tijdens de agendavorming wegen de belanghebbenden af in welke mate de risico's acceptabel zijn. Uiteraard speelt daarbij een rol welke maatregelen zij kunnen nemen en ten koste van wat. De risico's zelf omvatten immers ongewenste effecten, maar ook de te treffen maatregelen. Deze kosten geld en menskracht en kunnen zelf ongewenste effecten met zich mee brengen, zoals een inbreuk op de privacy. De risicoanalyse reikt rationele argumenten aan om de afweging te maken. Uiteindelijke spelen daarnaast (vooral) normen, waarden, belangen en opportuniteit een rol.[45] De politie beoordeelt bijvoorbeeld de risico's van het internet anders dan de providers, de hardwareleveranciers en de privacykamer. In de uiteindelijke afweging spelen ook cognitieve beperkingen van de mens een rol. Men plaatst bijvoorbeeld de bevindingen in eigen referentiekaders, waardoor vertekening kan optreden. Men hoort wat men wil horen. Men gelooft wat men wil en kan geloven.[46] Een risicoanalyse is dus geen garantie dat belanghebbenden maatregelen gaan treffen.

[40] {De Vries, 1998}, {Shubik, 1991A}. De Vries heeft het overigens niet over risico's, maar over problemen.
[41] Meyer wijst bijvoorbeeld op de beperkte waarde van informatiesystemen voor de agendavorming {Meyer, 1994}.
[42] Eigen waarneming.
[43] {Hogwood & Gunn, 1988, 69}, {Shubik, 1991A, 10,14}.
[44] {Shubik, 1991B}.
[45] Zie hiervoor bijvoorbeeld {Huigen, 1993}, {Rosenthal e.a., 1996}, {Van Swaaningen, 2001} en {Williams & Godson, 2002, 314}.
[46] Zie hiervoor {March, 1994}, {Simon, 1997}, {Hughes-Wilson, 1999} en {Shubik, 1991B}.

Dunn en Hogwood maken onderscheid tussen het analyseproces ten dienste van het beleidsproces (beleidsanalyse) en het beleidsproces zelf. Beleidsanalyse is een vorm van probleemgericht, multidisciplinair en toegepast wetenschappelijk onderzoek. Het is in de kern een conceptueel en intellectueel proces binnen de politieke context van het beleidsproces. De fase van het beleidsproces bepaalt welk type beleidsanalyse nodig is. In de eerste fase ligt het accent op het doorgronden en benoemen van de problematiek, in dit geval de risico's van veranderingen in criminaliteit. In de laatste fase gaat het vooral om de evaluatie van bestaand beleid.[47] In plaats van over beleidsanalyse is het internationaal gebruikelijk om bij opsporingsinstanties te spreken over intelligence, of criminaliteits- of misdaadanalyse. Dit is binnen de defensiewereld en bij opsporingsinstanties een afzonderlijke onderzoeksdiscipline.[48]

Dit proefschrift hanteert eveneens een onderscheid tussen het analyseproces en het beleidsproces. Een risicoanalyse wordt beschouwd als een bijzondere vorm van inlichtingen, criminaliteitsanalyse en beleidsanalyse. De uitgangspunten, methoden en technieken daarvan zijn tevens bruikbaar voor risicoanalyse. Preventie, preparatie en risicobeheersing zijn een bijzondere vorm van beleid en de wijze van totstandkoming, de besluitvorming en de uitvoering een bijzondere vorm van een beleidsproces.

1.2.4. Georganiseerde criminaliteit

Gekozen is om het risicoanalyse-instrumentarium toe te spitsen op georganiseerde criminaliteit (zie paragraaf 1.1). Dit is echter geen eenduidig begrip. Er bestaan vele definities, zowel binnen Nederland als daarbuiten. Onderzoekers hebben het vanuit verschillende theoretische invalshoeken en voor uiteenlopende doeleinden bestudeerd. Er valt een bont palet van delicten onder, hoewel drugshandel de boventoon voert.[49] In Nederland gebruiken wetenschappers, politiemedewerkers en de politiedepartementen vooral de definitie van de onderzoeksgroep Fijnaut.[50] Toch ligt ook deze definitie onder vuur. Zelfs Bovenkerk, één van de leden van die onderzoeksgroep, heeft zijn twijfels. Hij vraagt zich in 2001 af of de definitie niet te veel is aangepast om haar voor Nederland kloppend te maken. Hij geeft een nieuwe betekenis aan het begrip. Op basis daarvan stelt hij dat het niet eenvoudig is om in Nederland goede voorbeelden te vinden van georganiseerde criminaliteit. Verder noemt hij dat een inhoudelijk leeg, maar politiek veelzeggend begrip. Het is leeg omdat georganiseerd geen onderscheidend vermogen heeft. Het is politiek veelzeggend omdat de term het signaal afgeeft dat een situatie heel ernstig is en ingrijpende maatregelen nodig zijn.[51] Vooral Van Duyne verzet zich overigens al jaren tegen de veronderstelling dat georganiseerde criminaliteit (het meest) erg is. Het wil er bij hem niet in dat bijvoorbeeld de drugshandel ernstiger is dan de illegale activiteiten van het Van der Valk-concern in de jaren '90.[52] Klerks stelt vraagtekens bij de bruikbaarheid van het begrip voor wetenschappelijke analyses. Het begrip omvat volgens hem een zodanige

[47] {Hogwood & Gunn, 1988}, {Dunn, 1994}.
[48] Zie bijvoorbeeld {McDowell, 1998}.
[49] Zie bijvoorbeeld {Enquêtecommissie, 1996B}, {Ruggiero, 1996}, {Maltz, 1990}, {Klerks, 2000}, {Van Duyne e.a., 1990}, {Paoli, 2002, 53-63}, {Van Duyne e.a., 2001, 50-51}, {Bovenkerk, 2001}.
[50] Zie bijvoorbeeld {Kleemans e.a., 1999}, {Kernteam Noord- en Oost-Nederland, 2001}, {Criminaliteitsbeheersing, 2001, 31}.
[51] {Bovenkerk, 2001}.
[52] {Van Duyne e.a., 1990}, {Van Duyne, 1995}, {Van Duyne, 1996}.

variatie aan verschijnselen en activiteiten dat het gebruik ervan eerder verwarrend dan verhelderend werkt.[53]

Ondanks genoemde kanttekeningen is toch gekozen voor georganiseerde criminaliteit.[54] Die keuze houdt geen oordeel in over de ernst of belangrijkheid ten opzichte van andere vormen van criminaliteit. De keuze houdt evenmin een oordeel in over gedrag dat niet strafbaar is gesteld, maar wellicht even schadelijk kan zijn. Er is wel gekozen voor een eigen conceptualisering van het begrip.[55]

1.3. Doel, probleemstelling en afbakening

De vorige paragraaf schetst enkele probleemvelden en plaatst kanttekeningen bij het risicoanalyse-instrumentarium ten behoeve van vroegtijdige criminaliteitsbeheersing en het begrip georganiseerde criminaliteit. Daarom is een uitwerking van het instrumentarium voor die toepassing wenselijk. Het eerste doel van dit proefschrift is de ontwikkeling daarvan. De identificatie, selectie en de analyse van de toekomst van de ontwikkelingen vallen daar buiten. De uitwerking van een instrumentarium hiervoor is immers al een proefschrift op zich waard. De mate waarin een risicoanalyse daadwerkelijk leidt tot vroegtijdige criminaliteitsbeheersing en de maatregelen die men kan treffen, komen evenmin aan bod. Ook dat is een proefschrift op zich waard.

Het tweede doel van dit proefschrift is de toepassing van het instrumentarium op een specifieke maatschappelijke ontwikkeling. Hierdoor ontstaat inzicht in de bruikbaarheid ervan. Het product dat zo totstandkomt, heeft ook een zelfstandige waarde. De analyse brengt immers risico's in kaart die nog niet op de agenda staan. Gekozen is voor een cluster van ontwikkelingen, namelijk de ICT-ontwikkelingen. De analyse moet primair bijdragen aan vroegtijdige criminaliteitsbeheersing en dus aan de beleidsfase *agenda-vorming*. Hierdoor heeft de analyse vooral een verkennend karakter en richt zich op de Nederlandse samenleving als geheel (macroniveau). Meer specifiek gaat het dan om georganiseerde criminaliteit die in of vanuit Nederland plaatsvindt, of Nederlandse belangen aantast. Op basis van de analyse kan in een later stadium een verdieping plaatsvinden naar specifieke regio's of sectoren (mesoniveau) of zelfs individuele organisaties en personen (microniveau). De risicoanalyse richt zich verder op de inhoudelijke kant van de problematiek en niet op denkbare maatregelen. Omdat het analyseobject 'toekomstige veranderingen' betreft, is gekozen voor een kwalitatieve en strategische risicoanalyse.[56] De wijze waarop de ICT-ontwikkelingen zich de komende jaren voortzetten, valt buiten de analyse. De vertaling van een ontwikkeling naar de toekomst, maakt immers geen onderdeel uit van het te ontwikkelen instrumentarium. Het vroegtijdige karakter van de analyse schuilt in de vertaling van de huidige ICT-ontwikkelingen naar toekomstige veranderingen in georganiseerde criminaliteit. De tijdshorizon van de analyse is daardoor beperkt.

[53] {Klerks, 2000, 177-178}.
[54] Zie paragraaf 1.1 voor de redenen van deze keuze.
[55] Zie hoofdstuk 3 voor de argumenten hiervoor en het concept.
[56] Paragraaf 2.3 gaat nader in op deze begrippen en paragraaf 2.5 onderbouwt deze keuze.

Als afgeleide van de genoemde doelen luidt de probleemstelling:

1 Op welke wijze kan men de risico's analyseren van veranderingen in georganiseerde criminaliteit die het gevolg zijn van ontwikkelingen in de samenleving?
2 Wat zijn de risico's van veranderingen in georganiseerde criminaliteit die voortkomen uit de ICT-ontwikkelingen?

1.4. Opzet en verantwoording proefschrift

Dit proefschrift bestaat in de kern uit twee componenten. De eerste component, de hoofdstukken 2 tot en met 4, beschrijft het risicoanalyse-instrumentarium. Deze hoofdstukken beantwoorden de eerste vraag uit de probleemstelling en dienen het eerste doel. De tweede component, de hoofdstukken 5 en 6, brengt de risico's van veranderingen in georganiseerde criminaliteit als gevolg van de ICT-ontwikkelingen in kaart. Deze hoofdstukken beantwoorden de tweede vraag uit de probleemstelling en dragen bij aan het tweede doel. Tevens heeft de analyse een zelfstandige gebruikswaarde voor de agendavorming.

Het risicoanalyse-instrumentarium zelf bestaat uit drie onderdelen. Het *eerste onderdeel*, hoofdstuk 2, betreft een uitwerking van risicoanalyse voor vroegtijdige criminaliteitsbeheersing. Daarbij is vooral gekeken naar literatuur op het terrein van criminaliteit en veiligheidsstudies. Het *tweede onderdeel*, hoofdstuk 3, beschrijft een nieuw concept voor georganiseerde criminaliteit, namelijk als een stelsel van illegale groothandelsondernemingen. Dit concept is vooral geënt op een theoretische hoofdstroom die georganiseerde criminaliteit beschouwt als een stelsel van (misdaad)ondernemingen. Deze hoofdstroom sluit aan bij de gelegenheidstheorie.[57] Het *derde onderdeel*, hoofdstuk 4, werkt het analysekader uit om inzicht te krijgen in de trits 'ontwikkeling(en) – veranderingen in criminaliteit – ongewenste effecten' en in de waarschijnlijkheid van die veranderingen. Dit kader vindt mede haar basis in de gelegenheidstheorie die is geïnterpreteerd voor georganiseerde criminaliteit.

Component		Onderdeel	
1	Risicoanalyse-instrumentarium	1.1	Risicoanalyse voor vroegtijdige criminaliteitsbeheersing (H. 2)
		1.2	Conceptueel model georganiseerde criminaliteit (H. 3)
		1.3	Analysekader georganiseerde criminaliteit (H. 4)
2	Risicoanalyse veranderingen georganiseerde criminaliteit als gevolg van ICT-ontwikkelingen	2.1	Analyse van ICT-ontwikkelingen (H. 5)
		2.2	Geïdentificeerde dreigingen en beoordeling ervan (H. 6)

Figuur 1.3 Opzet proefschrift

[57] Zie paragraaf 3.5 voor de onderbouwing.

De uitgevoerde risicoanalyse omvat een analyse van de ICT-ontwikkelingen, die is gebaseerd op literatuur en beleidsstukken (hoofdstuk 5). De risicoanalyse omvat verder de geïdentificeerde dreigingen en een beoordeling van de waarschijnlijkheid en ongewenste effecten daarvan (hoofdstuk 6). De hoofdstukken 4 en 5 vormen daarvoor de basis. Daarbij is primair van buiten (ICT-ontwikkelingen) naar binnen (georganiseerde criminaliteit) gekeken.

De identificatie van dreigingen en de beoordeling van de waarschijnlijkheid en ongewenste effecten ervan, zijn *niet* gebaseerd op een empirisch onderzoek. Hieraan liggen enkele redenen ten grondslag. Een eerste reden, en tevens de belangrijkste, houdt verband met de aard van de analyse. De analyse is bedoeld om maatregelen te overwegen *voordat* de dreigingen zich daadwerkelijk manifesteren. Wanneer empirische gegevens beschikbaar zouden zijn over de risico's, is feitelijk geen sprake van vroegtijdige, maar van reactieve preventie en preparatie.[58] Men loopt dan al achter de feiten aan. Een tweede reden is dat, als er al gegevens beschikbaar zouden zijn, deze selectief van aard zijn en een interpretatie-kader ontbreekt om de gegevens te beoordelen.[59] Als we al veranderingen kunnen signaleren op basis van de gegevens, dan is lang niet altijd duidelijk wat de oorzaak ervan is en of het de voorbode is van meer onheil. Indien we bijvoorbeeld één website vinden waar men drugs te koop aanbiedt, is dat dan het topje van de ijsberg, de voorbode van een grote toename daarin of een uitzondering? En wanneer we geen website vinden, hoeven we dat dan in de toekomst ook niet te verwachten? Een derde reden, die samenhangt met de tweede, is de onbekendheid met de mogelijkheden van de ICT-ontwikkelingen. De belanghebbenden zijn nog relatief onbekend hiermee en hebben nog geen compleet beeld. De plegers van georganiseerde criminaliteit zijn zich evenmin hiervan bewust. Zij zullen de mogelijkheden nog niet volledig benutten.

Desondanks is wel gebruikgemaakt van enige literatuur. De ICT-ontwikkelingen zijn per slot van rekening al enige jaren aan de gang. Diverse auteurs hebben reeds onderzoek verricht naar (nieuwe vormen van) criminaliteit als gevolg van aspecten daarvan.[60] In aanvulling op de bestudeerde literatuur zijn vier interviews gehouden (zie bijlage 4). Tijdens die interviews is niet alleen gevraagd naar bekende vormen van criminaliteit, maar ook naar toekomstverwachtingen.[61] Uit zowel de bestudeerde onderzoeken als de interviews komen diverse mogelijkheden naar voren die plegers van georganiseerde criminaliteit (zouden kunnen) gebruiken. Deze zijn meegenomen bij de beschrijving en beoordeling van de geïdentificeerde dreigingen. Bij de beoordeling van de dreigingen zijn geen experts of anderen betrokken geweest. Allereerst is het niet het primaire doel om de risico's diepgaand te analyseren. Het gaat om een nevenproduct van de toepassing van het instrumentarium. In een later stadium kan de analyse worden verdiept met behulp van een raadpleging van experts.[62]

[58] Zie subparagraaf 1.2.3.
[59] Zie subparagraaf 1.2.2.
[60] {Boni & Kovacich, 1999}, {Galeotti, 2000B}, {Hoogenboom, 2001}, {NCIS, 1999}, {O'Brien, 2000}, {Power, 2000A}, {Power, 2000B}, {Robinson, 2000}, {Stol e.a., 1999A}, {Stol e.a., 1999B}, {Vriesde e.a., 1999}, {Williams, 1999}
[61] Hoewel gedateerd, zijn de interviews nog steeds relevant voor de analyses.
[62] Analisten spreken in dat kader van het T-model: van onderzoek in de breedte (het horizontale deel van de T), naar onderzoek in de diepte (het verticale deel). Zie hiervoor paragraaf 2.3.

Het proefschrift eindigt met een nabeschouwing over de ervaringen met het instrumentarium (hoofdstuk 7). Bovendien staat dit hoofdstuk nog stil bij de (moeizame) relatie tussen strategische risicoanalyses en criminaliteitsbeheersing.

Het literatuuronderzoek dat ten grondslag ligt aan dit proefschrift is begin 2003 beëindigd, maar is vooral uitgevoerd in 2001. Door omstandigheden is het manuscript pas in juli 2004 afgerond. Sinds 2003 zijn diverse publicaties verschenen over georganiseerde criminaliteit, de ICT-ontwikkelingen en risicoanalyse. Hiervan is geen gebruik meer gemaakt. Twee uitzonderingen daarop vormen de studie van Svensson en Zouridis en het 'Nationaal Dreigingsbeeld zware of georganiseerde criminaliteit' van de Dienst Nationale Recherche Informatie van het Korps Landelijke Politiediensten.[63] De eerste studie is gebruikt om vooral paragraaf 5.6 over sociale controle beter te onderbouwen. De tweede studie, hoewel breder bruikbaar voor dit proefschrift, is uitsluitend benut om de oorspronkelijke analyses in hoofdstuk 6 te toetsen en te onderbouwen met recent uitgevoerd onderzoek. Eén van de onderwerpen waaraan het dreigingsbeeld expliciet aandacht besteedt, is namelijk het gebruik van ICT door zware of georganiseerde criminaliteit. Tevens zijn, naar analogie van het dreigingsbeeld, de (impliciete) deeldreigingen expliciet benoemd. Deze wijzigingen zijn aangebracht in januari 2005.

[63] {Svensson & Zouridis, 2004}, {DNRI, 2004}.

2. Risicoanalyse

2.1. Inleiding

Het risicoanalyse-instrumentarium bestaat uit drie onderdelen. Dit hoofdstuk beschrijft het eerste onderdeel, namelijk een uitwerking van risicoanalyse voor vroegtijdige criminaliteitsbeheersing. Paragraaf 2.2 gaat nader in op het begrip risico, de componenten ervan en aanverwante begrippen. Paragraaf 2.3 werkt het begrip risicoanalyse uit en schetst enkele toepassingsdoeleinden. Paragraaf 2.4 beschrijft de stappen waarin een risicoanalyse totstandkomt. Paragraaf 2.5 tot slot behandelt de specifieke uitgangspunten voor vroegtijdige criminaliteitsbeheersing.

2.2. Risico, de componenten en aanverwante begrippen

Een analyse van risico's begint uiteraard met de vraag wat nu precies een risico is. Woordenboeken wijzen vooral op het verzekeringswezen als oorsprong van het begrip. Van Duin refereert aan een studie waarin maar liefst eenentwintig definities zijn opgesomd.[1] Hij geeft aan dat de definities hun oorsprong vinden in de technisch-wetenschappelijke, de sociaal-psychologische en de bestuurlijk-culturele literatuur.[2] Een zoekvraag in de bestanden van de universiteitsbibliotheken maakt duidelijk dat ook in de medische wetenschap het begrip veelvuldig voorkomt. Binnen het domein van veiligheidsstudies en criminaliteit hanteert men diverse definities.[3] Ondanks de verschillen in de definities en toepassingsdomeinen is de rode draad dat het begrip is opgebouwd uit drie componenten.

De *eerste* component betreft 'iets' wat onwenselijk is. Sommigen spreken van (be)dreiging. Anderen hebben het over een gevaar, scenario, (ongunstige) gebeurtenis, situatie, proces of cluster van gebeurtenissen of situaties.[4] De auteurs maken geen onderscheid tussen bedreiging en dreiging. Het uitgangspunt in dit proefschrift is dat sprake is van een bedreiging wanneer iemand uitspreekt of door zijn gedrag kenbaar maakt iets of iemand te bedreigen. Er is bijvoorbeeld pas sprake van een bedreiging van fysiek geweld als iemand vertelt of daadwerkelijk aanstalten maakt om geweld te gebruiken. Een dreiging is daarentegen breder. Het is daarbij niet van belang of iemand daadwerkelijk een ander bedreigt. Een argeloze voorbijganger kan zomaar slachtoffer worden van geweld, zonder dat sprake was van een bedreiging. De verzameling van bedreigingen is dus een deelverzameling van de verzameling van dreigingen. Om niet op voorhand een beperking aan te brengen, is hier gekozen voor het begrip dreiging. De achterliggende vraag bij deze component is: wat zou er kunnen gebeuren?

De *tweede* component van een risico gaat over de waarschijnlijkheid of kans dat iets zich voordoet. Ericson en Haggerty geven aan dat het gaat om de beste schatting van de

[1] Het gaat om een studie van Vlek uit 1991 {Van Duin, 1994}.
[2] {Van Duin, 1994, 57}.
[3] {Black e.a., 2000}, {Wardlaw, 1999}, {Ericson & Haggerty, 1997}, {Starr & Whipple, 1991}, {Koning e.a.}, {Frei & Ruloff, 1989}, {Ten Brink & van der Leest, 2002}.
[4] Idem.

waarschijnlijkheid. Bij Starr en Whipple is deze component impliciet meegenomen. Zij spreken namelijk over de potentiële blootstelling aan een verlies.[5] De waarschijnlijkheid kan betrekking hebben op de dreiging, bijvoorbeeld de waarschijnlijkheid van de dreiging van een woninginbraak. De waarschijnlijkheid kan ook betrekking hebben op de ongewenste effecten, bijvoorbeeld psychische schade als gevolg van een woninginbraak. Deze tweede vorm is niet alleen afhankelijk van de waarschijnlijkheid van de dreiging (de woninginbraak), maar ook van andere factoren. Voorbeelden daarvan zijn de mate waarin de daders geweld gebruiken en de leeftijd van het slachtoffer. De waarschijnlijkheid is mede afhankelijk van de maatregelen die partijen reeds hebben getroffen tegen de dreiging. Zo is de waarschijnlijkheid dat iemand in Nederland besmet raakt met polio klein als gevolg van het inentingsprogramma. In dit proefschrift is als naam voor de tweede component gekozen voor 'waarschijnlijkheid'. De achterliggende vraag is: hoe waarschijnlijk is het dat de dreiging zich manifesteert?

De *derde* component van een risico duidt op de effecten van de dreiging. Andere benamingen zijn: invloed op belangen, schade, gevolgen of verlies. Sommigen nemen zowel de positieve als negatieve effecten mee.[6] Anderen richten de aandacht specifiek op de negatieve effecten.[7] Ook al doet de dreiging zich nog niet voor, er kan toch al sprake zijn van ongewenste effecten. De dreiging van een woninginbraak kan er toe leiden dat mensen 's avonds niet meer de deur uitgaan, geld uitgeven aan beveiliging en zich niet veilig voelen. Wanneer de dreiging zich daadwerkelijk manifesteert, ontstaan eveneens (ongewenste) effecten. Als zich bij iemand feitelijk een inbraak voordoet, kunnen geld en dierbare herinneringen verdwijnen of kan het slachtoffer psychische schade ondervinden. In het risicobegrip gaat het om het tweede type effecten: de effecten wanneer de dreiging zich feitelijk voordoet. In dit proefschrift is de derde component verder aangeduid als 'ongewenste effecten'. Bij criminaliteitsbeheersing is de aandacht immers vooral gericht op het ongewenste. Verder is nog een onderscheid te maken tussen de aard van de ongewenste effecten en de omvang of frequentie ervan. Omdat de omvang en frequentie mede afhankelijk zijn van de waarschijnlijkheid van de dreiging, wordt dit uit oogpunt van complexiteitsreductie niet meegenomen in de analyse. Er is dan immers sprake van een dubbele onzekerheid: die van de waarschijnlijkheid van de dreiging en die van de relatie tussen de dreiging en de mate van voorkomen van de ongewenste effecten. De achterliggende vraag bij deze component is dus: wat zijn de ongewenste effecten als de dreiging zich manifesteert?

Met de benoeming van de componenten van een risico hebben we nog geen definitie. Het accent daarin kan zowel liggen op de waarschijnlijkheid, de dreiging als de ongewenste effecten. Wat betekent bijvoorbeeld 'het risico van woninginbraak'? Gaat het dan om de waarschijnlijkheid van een woninginbraak, de ongewenste effecten en/of de woninginbraak zelf? Alle genoemde varianten zijn terug te vinden in de aangetroffen definities.

Wanneer we drie componenten onderscheiden bij een risico, ligt het voor de hand deze mee te nemen in de definitie. Duidelijk moet zijn dat de waarschijnlijkheid betrekking heeft op de dreiging en dat het gaat om de ongewenste effecten wanneer de dreiging zich manifesteert. Wel is het zo dat de componenten dreiging en ongewenste effecten elkaar

[5] Idem.
[6] {Black e.a., 2000}, {Wardlaw, 1999} en {Koning e.a.}.
[7] {Ericson & Haggerty, 1997}, {Starr & Whipple, 1991}, {Bruning, 1994}.

overlappen. Een dreiging omvat immers taalkundig iets ongewenst. De zinsnede 'dreiging met ongewenste effecten' is als een ronde cirkel. Dat zou ervoor pleiten om één van beide weg te laten. Wanneer dreiging ontbreekt, lijkt het dat de waarschijnlijkheid betrekking heeft op de ongewenste effecten. Dit is niet juist. Wanneer de component ongewenste effecten ontbreekt, ligt het accent te veel op de waarschijnlijkheid. Ook dit is niet juist. Daarom komen toch beide voor in de definitie.

Op basis van bovenstaande argumentatie luidt de definitie:

> *Een risico is de combinatie van de waarschijnlijkheid dat een dreiging zich manifesteert en de ongewenste effecten daarvan.*

Bij het gebruik van de begrippen risico en dreiging moet wel duidelijk zijn wat het analyseobject is. In een risicoanalyse voor vroegtijdige criminaliteitsbeheersing is het object: verandering in (georganiseerde) criminaliteit als gevolg van (een) ontwikkeling(en) in de samenleving. Ogenschijnlijk zijn een dreiging en een risico synoniem. Toch is dat niet het geval. Een dreiging is een (analytische) component van een risico. Een risico heeft dan wel dezelfde naam als de component dreiging, maar daarvoor is beoordeeld wat de waarschijnlijkheid en de ongewenste effecten zijn. De methodische meetlat voor een risico ligt daarom hoger dan voor een dreiging.

De dreiging kan zich manifesteren gedurende een bepaalde periode in de toekomst.[8] De waarschijnlijkheid, de dreiging en de ongewenste effecten kunnen veranderen in de loop der tijd. Bovendien treffen belanghebbenden maatregelen tegen het risico. Deze beïnvloeden op enig moment de waarschijnlijkheid, de dreiging en de ongewenste effecten. Daarom is het noodzakelijk om in (de voorbereiding op) een risicoanalyse de periode te specificeren waarop de analyse betrekking heeft.

Bovenstaand geldt ook voor (een groep van) belanghebbenden. De dreiging, de waarschijnlijkheid en de ongewenste effecten kunnen namelijk variëren per soort belanghebbende. Voor een fietsenhandelaar is bijvoorbeeld geen sprake van een dreiging van 'betrokkenheid bij georganiseerde criminaliteit'. Voor vrijeberoepsbeoefenaren (notaris en dergelijke) echter speelt die dreiging wel.[9] Een bank heeft vaker van doen met een overval dan een ziekenhuis en dus is de waarschijnlijkheid groter. Bovendien kan een overval op een bank tot andere ongewenste effecten leiden als een overval op een ziekenhuis. In sommige gevallen is de dreiging juist gericht tegen een specifieke groep van belanghebbenden, zoals politici. De (groep van) belanghebbenden kunnen we op uiteenlopende abstractieniveaus bestuderen: de Nederlandse samenleving, Nederlandse politici, politici van een specifieke partij of een individuele politicus.

Een risico krijgt pas betekenis wanneer het in een bepaalde context is geplaatst.[10] Voorbeelden daarvan zijn: de invoering van de euro in januari 2002 (gebeurtenis), de ICT-ontwikkelingen en de uitvoering van fiscale wetten door de Belastingdienst (taakstelling). Die context speelt bijvoorbeeld een rol bij het onderscheid naar eenmalige of permanente risico's. De dreiging van een overval op een geldtransport is altijd aanwezig. Vanwege de

[8] Zie {Ten Brink & van der Leest, 2002} en {Albanese, 2002}.
[9] Zie subparagraaf 4.3.3.
[10] {Albrecht & Kilchling, 2002, 29-30}, {Ten Brink & van der Leest, 2002}.

invoering van de euro, een eenmalige gebeurtenis, lag de waarschijnlijkheid tijdelijk hoger. De waarschijnlijkheid kunnen we in dat geval uitdrukken ten opzichte van de situatie zonder de invoering. Daarom is het noodzakelijk om in (de voorbereiding op) een risicoanalyse de context te specificeren waarin de analyse plaatsvindt.

Veelal voorziet men een risico van een bijvoeglijk naamwoord zoals groot of klein, hoog of laag of ernstig of niet ernstig. Op voorhand is niet duidelijk wat de betekenis daarvan is. Er zijn immers vele combinaties denkbaar van waarschijnlijkheid en ongewenste effecten. Voorbeelden daarvan zijn de combinatie van 1) een kleine waarschijnlijkheid en ernstige effecten en 2) een grote waarschijnlijkheid met niet-ernstige effecten. Soms spreekt men van een potentieel risico. Omdat een risico per definitie onzekerheid inhoudt, is het bijvoeglijk naamwoord potentieel overbodig.

We treffen ook het begrip risicofactor aan. Een risicofactor is van invloed op de waarschijnlijkheid van de dreiging. Er bestaan verschillende soorten risicofactoren. Ondeugdelijke elektriciteit kan de oorzaak zijn van een ‘brand in een woning’ en vormt daardoor een oorzakelijke risicofactor. Een rieten dak op een woning vat niet vanzelf vlam, maar is wel extra kwetsbaar voor brand en kan tot meer schade leiden wanneer een brand uitbreekt. Een soortgelijke redenering geldt voor het wonen naast een vuurwerkfabriek. Omdat een vuurwerkfabriek gevoeliger is voor brand dan een normaal pand, verhoogt dit de waarschijnlijkheid van een brand. We bevinden ons hier wel op een glijdende schaal in de analyse. In de formele logica hanteert men een onderscheid naar noodzakelijke en voldoende voorwaarden. Voor brand is in elk geval een vonk noodzakelijk, bijvoorbeeld door blikseminslag of kortsluiting. Een vonk leidt niet altijd tot brand, bijvoorbeeld vanwege het gebruik van brandwerend materiaal. De vonk is dan wel een noodzakelijke voorwaarde, maar geen voldoende voorwaarde. Een rieten dak, of het wonen naast een vuurwerkfabriek zijn noch voldoende noch noodzakelijke voorwaarden. De mate waarin wel of niet bepaalde risicofactoren meegewogen moeten worden, is afhankelijk van het doel en het abstractieniveau van de analyse evenals van de beschikbare kennis en informatie.

De mate waarin risicofactoren kunnen worden vastgesteld, hangt samen met de mate waarin informatie en kennis over het risico bekend zijn. Over de oorzaken van een brand en de omstandigheden daarvan is bijvoorbeeld veel bekend. Daardoor bestaat een goede basis om risicofactoren te benoemen. Voor andere dreigingen, zoals een terroristische aanslag, is dat veel minder het geval. Daardoor is het veel minder eenvoudig om risicofactoren vast te stellen.

Een ander gehanteerd begrip is risico-indicator. Een risico-indicator is een operationalisatie van een risicofactor. Een risicofactor is niet meetbaar en een risico-indicator wel.[11] Ondeugdelijke elektriciteit is niet meetbaar en daardoor een risicofactor. Het aantal jaren dat de kabels in de woning aanwezig zijn en het regelmatig doorslaan van de stoppen, twee risico-indicatoren, zijn wel meetbaar. Bovendien kan een risico-indicator fungeren als een signaal dat een dreiging zich kan gaan manifesteren. In die betekenis is een risico-indicator een soort waarschuwingslampje op een dashboard van een auto. Het regelmatig doorslaan van de stoppen in huis kan een indicatie zijn van ondeugdelijke elektriciteit en dus een

[11] Geïnspireerd door {Frei & Ruloff, 1989, 48-51}.

voorbode zijn van brand. Een verdere verbijzondering is dan nog mogelijk door te werken met aanvullende criteria. Empirisch zou kunnen blijken dat bij overschrijding van een bepaalde waarde de waarschijnlijkheid van een dreiging substantieel toeneemt. Per afzonderlijk criterium kan met behulp van een gewicht worden aangegeven in welke mate het criterium een voorspellend vermogen heeft. Daartoe is wel een validatie nodig van het voorspellende vermogen ervan voor de manifestatie van de dreiging.

Dreiging (risico)	Risicofactor	Risico-indicator	Criterium
Brand in woning	Ondeugdelijke elektriciteit	Aantal jaren dat bekabeling aanwezig is Het doorslaan van stoppen	Doorslaan vaker dan 1 keer per dag
Groei van drugshandel	Toename export van drugs	Groei van het aantal in beslag genomen kilo's drugs in het buitenland afkomstig uit Nederland	Stijging met 20% gedurende één jaar
Fraude met werknemers-verzekeringen door werkgever[12]	Gelegenheid werkgever Motivatie werkgever	Betalingsgedrag werkgever Tijdig aanmelden van werknemers door werkgever Bestaansduur bedrijf	Korter dan twee jaar Tussen twee en vijf jaar Langer dan vijf jaar
Creditcardfraude[13]	Specifieke karakteristie-ken van een transactie Afwijkend koopgedrag kaarthouder	Land van de transactie Type aankoop Afwijkend tijdstip van transactie	

Figuur 2.1 Voorbeelduitwerking dreiging, risicofactor, risico-indicator en criterium

Tot slot treffen we ook wel het begrip risicoprofiel of risicomodel aan.[14] Een risicoprofiel/ -model fungeert als een selectiemechanisme om riskante daders, situaties, goederen (et cetera) te identificeren. Gekozen is voor het begrip risicoprofiel. Dat profiel is de som van de risico-indicatoren. Een risicoprofiel kan men bijvoorbeeld gebruiken om jeugdige criminelen op het spoor te komen op basis van risico-indicatoren zoals: 'aantal verzuim-dagen op school van een kind' en 'afkomstig uit eenoudergezin'. De achterliggende gedachte is dan dat deze twee indicatoren een selecterende werking hebben voor jongeren die extra aandacht behoeven.

2.3. Risicoanalyse nader uitgewerkt

Niet alleen van het begrip risico treffen we vele varianten aan, ook van risicoanalyse.[15] Wardlaw noemt risicoanalyse als de eerste van drie stappen van risicomanagement. De andere stappen zijn risicobeoordeling en het volgen van het risico. Het feitelijk treffen van maatregelen lijkt bij hem niet te vallen onder het begrip risicomanagement.[16] Black e.a.

[12] Uitwerking is ontleend aan {Lyre, 2000}.
[13] Onleend aan {Luijks, 2000}.
[14] Zie bijvoorbeeld {Lyre, 2000} en {Luijks, 2000}.
[15] Zie bijvoorbeeld {Black e.a., 2000} voor een globale literatuurstudie op dit terrein.
[16] {Wardlaw, 1999}.

stellen op basis van een literatuurstudie dat risicoanalyse onderdeel uitmaakt van risicobeoordeling, naast risico-identificatie en -evaluatie. Daarnaast onderkennen zij in de literatuur risicomanagement, dat bestaat uit risicoacceptatie, -beheersing en -monitoring.[17] Zelf werken ze een methodologie uit voor risicobeoordeling die bestaat uit vijf fasen: 1) verkenning van de omgeving, 2) beoordeling van de primaire elementen van de analyse (bijvoorbeeld bekende criminele samenwerkingsverbanden), 3) beschrijving van de bevindingen van 1 en 2 tezamen, 4) formulering van voorstellen voor de omgang met de risico's en 5) evaluatie van de uitvoering van maatregelen en ontwikkeling van de risico's.[18] Starr en Whipple beschouwen risicobeoordeling en risicomanagement daarentegen als onderdeel van risicoanalyse.[19]

Welke van de varianten heeft de voorkeur? Eerder is een onderscheid aangebracht tussen het analyseproces en het beleidsproces. Naar analogie daarvan is ervoor gekozen om het begrip risicoanalyse te reserveren voor de analysekant en risicobeheersing voor de beleidskant.[20] Het begrip risicomanagement is verder niet gehanteerd, omdat beheersing beter aansluit bij criminaliteitsbeheersing dan management. Op basis van deze scheiding beschrijft paragraaf 2.4 de stappen van een risicoanalyse. Preventie en preparatie zijn op hun beurt specifieke vormen van risicobeheersing.

Men kan het risicoanalyse-instrumentarium voor uiteenlopende doelen inzetten. Eerder is al aangegeven dat de fase van het beleidsproces bepaalt aan welk type risicoanalyse behoefte bestaat. Er zijn vier fasen benoemd, namelijk: 1) agendavorming, 2) beleidsvorming, 3) beleidsuitvoering en 4) beleidsevaluatie. De fase van het beleidsproces zegt impliciet iets over: a) de mate van politieke onenigheid over het risico, b) de mate van onzekerheid, c) het soort benodigde informatie en d) de mate waarin informatie beschikbaar is. Wanneer we het hebben over een risicoanalyse ten behoeve van vroegtijdige criminaliteitsbeheersing is vooral de fase van agendavorming van belang.[21] Er is nog weinig of geen informatie beschikbaar en kennis is eveneens schaars of ontbreekt. Er bestaat bijvoorbeeld nog weinig informatie en kennis over het gebruik van biotechnologie door criminelen en de risico's die daaruit voort kunnen komen. Voor de agendavorming is daarom vooral behoefte aan verkennende risicoanalyses.

Wardlaw en Black e.a. gebruiken het instrumentarium ook voor het volgen van risico's (monitoren). Tijdens een verkennende risicoanalyse ontstaat immers slechts een momentopname. Door de ontwikkelingsrichting van de risico-indicatoren (toename of afname) en de snelheid daarvan te volgen, ontstaat een beeld hoe het risico zich ontwikkelt in de tijd. Op basis daarvan is een afweging mogelijk of en in welke mate het risico alsnog op de agenda moet worden geplaatst en/of aanvullende maatregelen noodzakelijk zijn. Het volgen van de risico-indicatoren kan ook een functie hebben om meer kennis en informatie te vergaren over het risico. Variatie kan worden aangebracht in de mate van volgen (actief of passief), de hoeveelheid te volgen indicatoren en de in te zetten capaciteit. Het volgen van risico's kan aan de ene kant bijdragen aan de fase van agendavorming voor risico's die de

[17] {Black e.a., 2000, 33-38}.
[18] {Black e.a., 2000, 37-72}. De terminologie is niet altijd uniform en consistent gehanteerd.
[19] {Starr & Whipple, 1991, 53}.
[20] Zie subparagraaf 1.2.3.
[21] Zie subparagraaf 1.2.3.

agenda niet hebben gehaald. Aan de andere kant kan het bijdragen aan de fase van beleidsevaluatie.

Sommigen gebruiken het risicoanalyse-instrumentarium voor detectie van riskante gebeurtenissen, plaatsen, processen, gedrag, situaties (et cetera).[22] Deze vorm van risicoanalyse is vooral gericht op de fase van beleidsuitvoering. De resultaten van een 'detectie risicoanalyse' kan men gebruiken om gerichte maatregelen te treffen. Op basis van een risicoprofiel probeert het GAK bijvoorbeeld uitkeringsgerechtigden en werkgevers te selecteren die onjuiste of onvolledige informatie verstrekken.[23] Eigenlijk is hier al sprake van een manifestatie van de dreiging. Er is daarom eerder sprake van detectie van fraude, dan van het risico van fraude. Een risico is immers gericht op een dreiging die zich in de toekomst kan manifesteren, in plaats van een dreiging die zich heeft gemanifesteerd. De inzet van het risicoanalyse-instrumentarium voor detectie veronderstelt wel een risicoprofiel. Kennis van de risicofactoren en -indicatoren is daarvoor randvoorwaardelijk.

Het risicoanalyse-instrumentarium kan verder worden gebruikt voor zowel strategische als tactische sturing. Bij *strategische* sturing gaat het om het maken van de keuzen die richting geven aan de criminaliteitsbeheersing. Dit wordt ook wel criminele politiek genoemd. Strategische sturing vindt plaats binnen de fasen agendavorming, beleidsvorming en beleidsevaluatie. *Tactische* sturing richt zich, binnen de kaders van de strategische sturing, op de te bereiken effecten van criminaliteitsbeheersing. Tactische sturing richt zich op problemen waarvoor een operationele aanpak noodzakelijk is. Het gaat daarbij om problemen die op korte termijn spelen, zoals locaties waar zich vaak problemen voordoen, daders, dadergroepen en series van delicten. Tactische sturing komt vooral voor in de fase beleidsuitvoering.[24] Daarvan afgeleid kunnen we strategische en tactisch analyses onderscheiden. Een strategische risicoanalyse draagt er toe bij dat bijvoorbeeld inzicht ontstaat in veranderingen in criminaliteit op basis waarvan prioriteiten en beleidsmaat-regelen kunnen worden vastgesteld. Een tactische risicoanalyse richt zich daarentegen op *specifieke* situaties, beroepsgroepen, processen, criminaliteits- of fraudevormen, locaties et cetera. De jeugdzorg kan bijvoorbeeld met behulp van een risicoanalyse specifieke groepen jongeren identificeren die in aanmerking komen voor gericht toezicht.

Een risicoanalyse is te onderscheiden naar het product en het proces. Het product risicoanalyse is het resultaat van het proces dat doorlopen is. Dit hoofdstuk beschrijft vooral de proceskant. Hoofdstuk 6 beschrijft een risicoanalyseproduct.

Verder onderscheidt men een kwantitatieve en een kwalitatieve risicoanalyse, een onderscheid dat we ook aantreffen bij wetenschappelijk onderzoek.[25] Bij een kwantitatieve analyse ligt het accent op (statistische) berekeningen van de waarschijnlijkheid en ongewenste effecten.[26] Bij een kwalitatieve risicoanalyse ligt het accent op de redenering en de argumenten in plaats van berekeningen. Starr en Whipple definiëren dit als "[….] revealed judgment and common sense applied to the formulation of a risk structure". Zij

[22] Zie bijvoorbeeld {Luijks, 2000} en {Lyre, 2000}.
[23] {Lyre, 2000}.
[24] Deze vormen van sturing worden onder andere genoemd in {NCIS, 2000A} en {Stuurgroep Informatie gestuurde opsporing, 2001A}, {McDowell, 1996}, {McDowell, 1998}, {Wardlaw, 1999, 2}, {Meesters e.a., 1999}. De omschrijving betreft een eigen interpretatie.
[25] Zie bijvoorbeeld {Baarda e.a, 1997} voor het onderscheid in kwalitatief en kwantitatief onderzoek.
[26] Zie bijvoorbeeld {Bruning, 1994} voor een kwantitatieve risicoanalyse.

stellen dat een kwalitatieve risicoanalyse het meest bruikbaar is "[….] when fears, emotions, prejudices, and fixed mindsets all tend to drive policy discussions in separate directions, rather than leading to a consensus".[27] Een combinatie van een kwantitatieve en kwalitatieve analyse is ook mogelijk. Deskundigen kunnen bijvoorbeeld argumenten wegen en/of een cijfermatige waardering toekennen aan de waarschijnlijkheid en ongewenste effecten. Op basis van deze wegingen en waarderingen kan de analist een kwantitatieve onderbouwing presenteren.[28] De berekening richt zich dan niet op de feitelijke gegevens, maar op de oordelen van deskundigen.

2.4. Stappen risicoanalyse

2.4.1. Overzicht stappen

Alvorens in te gaan op de stappen waarin een risicoanalyse totstandkomt, is het goed om de tot nu toe geformuleerde uitgangspunten samen te vatten. Risicoanalyse is te bezien als een proces en als een product. Een risicoanalyse kan kwalitatief of kwantitatief van aard zijn en een strategisch of tactisch doel hebben. De risicoanalyse moet zijn afgestemd op de fase waarin het beleidsproces zich bevindt. Het is een bijzondere vorm van beleidsanalyse, criminaliteitsanalyse of inlichtingenstudies en een specifieke vorm van toegepast wetenschappelijk onderzoek. Daar gehanteerde methoden en technieken zijn (groten)deels ook bruikbaar voor risicoanalyse.

De primaire stappen van een risicoanalyse zijn het identificeren en beoordelen van dreigingen. Daaraan vooraf gaat wel een goede voorbereiding, de eerste stap. Verder is vooraf inzicht nodig in het domein van de analyse, bijvoorbeeld socialewerknemersverzekeringen of georganiseerde criminaliteit. Het beschrijven en operationaliseren van het domein van de analyse is verder aangeduid als het ontwikkelen van een conceptueel model: de tweede stap. De derde stap richt zich op het identificeren van dreigingen binnen de kaders zoals deze zijn geformuleerd tijdens de voorafgaande stappen. De vierde stap, het beoordelen van dreigingen, onderbouwt de waarschijnlijkheid en de ongewenste effecten. Tijdens de vijfde stap komt het risicoanalyseproduct tot stand. Een risicoanalyse omvat dus de volgende stappen:

1. voorbereiden risicoanalyse;
2. ontwikkelen conceptueel model domein(en) van analyse;
3. identificeren dreigingen;
4. beoordelen dreigingen;
5. schrijven eindrapportage.

In de volgende subparagrafen zijn de stappen verder uitgewerkt.

2.4.2. Voorbereiden risicoanalyse

Verschuren bepleit dat ieder type onderzoek, en dus ook een risicoanalyse, start met het maken van een gedegen onderzoeksplan. "Een onderzoeksplan geeft een duidelijk en realistisch antwoord op de vraag waarom, wat, waar, hoe, hoeveel en wanneer onderzocht

[27] {Starr & Whipple, 1991, 52-53}.
[28] Zie voor dat laatste bijvoorbeeld {Wardlaw, 1999} en {Ten Brink & Van der Leest, 2002}.

gaat worden".[29] Met andere woorden, het onderzoeksplan geeft een uitwerking van het doel, de probleemstelling, het analyseobject, de te hanteren onderzoeksmethoden, de afbakening, de benodigde menskracht en middelen en een planning.

Duidelijk moet zijn voor welke fase van het beleidsproces de analyse is bedoeld. Ook moet helderheid bestaan over het analyseobject en het gewenste abstractieniveau. Een dreiging en risico zijn immers nader onder te verdelen in deeldreigingen en -risico's. Het risico van brand kan bijvoorbeeld worden verbijzonderd naar het type brand (uitslaande brand), de oorzaak (brand door blikseminslag), het type object (brand in woning) of de gevolgen (brand met dodelijke slachtoffers). Met andere woorden, de verzameling van branden is op uiteenlopende wijzen onder te verdelen naar deelverzamelingen. De onderscheiden deel-risico's kunnen overigens onderling overlappen. De deelrisico's van 'uitslaande brand', 'brand door blikseminslag' en 'brand in woning' sluiten elkaar niet uit. Verder is een specificatie nodig van de periode waarop de analyse zich richt, de belanghebbenden en de context.[30] De waarschijnlijkheid van een terroristische aanslag (dreiging) in de Verenigde Staten (gebied) door Al Qa'ida (dader) tegen regeringsgebouwen (doelwit) op 11 september (tijdstip) is naar we mogen aannemen groter dan in Nederland. Tijdens een oorlog met een moslimland (context) is die waarschijnlijkheid nog groter. Verder moet overeenstemming bestaan of de analyse kwalitatief of kwantitatief moet zijn. Specifiek voor georganiseerde criminaliteit geldt nog eens dat het internationale karakter ervan tot analytische migraine kan leiden. Vooraf moeten daarom keuzen worden gemaakt tot hoe ver de analyse reikt (zie paragraaf 4.5).

In praktijkgerichte omgevingen start een risicoanalyse vaak met een opdracht van een opdrachtgever. McDowell bepleit daarom dat de voorbereiding van een (strategische) analyse start met een verkenning van de opdracht. Het doel daarvan is het krijgen van inzicht in de opdracht, het te onderzoeken probleem en de belangen van de opdrachtgever. Op basis daarvan kan het team gericht met de opdrachtgever overleggen. Tijdens die communicatie over en weer krijgen beide partijen meer greep op de materie en kunnen zij de verwachtingen op elkaar afstemmen. McDowell spreekt hier over het (her)definiëren van de taak.[31] Eigenlijk ontstaat zo het door Verschuren genoemde onderzoeksplan en de definitieve opdracht.

2.4.3. Ontwikkelen conceptueel model domein(en) van analyse

Om dreigingen te kunnen identificeren en de waarschijnlijkheid en ongewenste effecten te onderbouwen, is aanvullend inzicht nodig in het domein van de analyse. Zonder dat zijn de drie vragen waarop een risicoanalyse antwoord moet geven niet op systematische en toetsbare wijze te beantwoorden.[32] Tevens behoeft het analyseobject een verdere uitwerking. Het analistenteam moet daartoe het domein holistisch en vanuit verschillende perspectieven beschouwen.[33]

---

[29] {Verschuren, 1996}.
[30] Zie paragraaf 2.2.
[31] {McDowell, 1998} {McDowell, 1996} en eigen ervaring. Dat ook het maken van een onderzoeksplan voorbereiding vergt, benadrukt ook Verschuren {Verschuren, 1996}.
[32] Het betreft de vragen: wat zou er kunnen gebeuren, hoe waarschijnlijk is het dat de dreiging zich manifesteert en wat zijn de ongewenste effecten als de dreiging zich manifesteert?
[33] Dit laatste bepleiten Dunn en Black e.a. {Dunn, 1994, 416-417}, {Black e.a., 2000}.

Het inzicht in het domein van de analyse vindt zijn neerslag in een conceptueel model. Dit is een mentaal plaatje van een complexe en onoverzichtelijke materie.[34] "Doordat ingewikkelde (relatie)patronen in beeld worden gebracht, ontstaan overzicht van en inzicht in mogelijke beschrijvings- en verklaringscategorieën".[35] De ontwikkeling van een conceptueel model biedt een goede gelegenheid om kennis en informatie te vergaren, te structureren en aannames af te leiden. Een conceptueel model scheidt belangrijke zaken van onbelangrijke. Conceptuele modellen bewijzen niets en een kwalificatie in termen van waar of niet-waar is niet aan de orde. Toch kan de bruikbaarheid sterk verschillen. De bruikbaarheid is afhankelijk van de mate waarin het kan bijdragen aan het doel.[36]

Een conceptueel model is richtinggevend voor de overige stappen van de risicoanalyse. Dit heeft een schaduwzijde. Het model bepaalt vanuit welke invalshoek(en) het analistenteam naar dreigingen, risicofactoren (en dergelijke) op zoek gaat. De kwaliteit en bruikbaarheid van het model bepalen daardoor tevens de kwaliteit van het eindproduct. Bovendien kan een conceptueel model in de loop van de tijd verstarrend werken. Hierdoor kunnen analisten nieuwe dreigingen niet altijd opmerken. Tijdens de totstandkoming zijn daarom creativiteit en het wisselen van invalshoeken van groot belang.[37]

Voorbeeld van een opdracht	**Aspecten waarin (onder andere) inzicht nodig is**	**Object van analyse**
Analyseer de risico's van fraude met werknemersverzekeringen opdat de wetgever lacunes in de wetgeving kan repareren	Domein werknemersverzekeringen • Kenmerken van de werknemersverzekeringen • Soorten fraude die uitkeringsgerechtigden en werkgevers kunnen plegen • Motivatie en kenmerken van fraudeurs • Controlemogelijkheden en -bevoegdheden[38]	Vormen van onjuiste of onvolledige informatieverstrekking door uitkeringsgerechtigde of werkgever
Analyseer de risico's van veranderingen in georganiseerde criminaliteit als gevolg van de ICT-ontwikkelingen ten behoeve van vroegtijdige criminaliteitsbeheersing	Domein georganiseerde criminaliteit • Kenmerken • Afbakening • Gelegenheidsfactoren • Domein ICT-ontwikkelingen • Kenmerken • Effecten op het legale bedrijfsleven	(Toekomstige) veranderingen in georganiseerde criminaliteit
Analyseer de risico's van criminaliteit die een succesvolle invoering van de euro in de weg staan in de periode december 2001 tot en met januari 2002	Domein invoering euro • Factoren die bepalend zijn voor een succesvolle invoering • Kritische momenten tijdens de invoering • Domein criminaliteit • Kansen voor criminelen om te profiteren van de invoering	Criminaliteitsvormen die succesvolle invoering in de weg staan

Figuur 2.2 Voorbeelden van opdrachten voor risicoanalyse en aspecten waarin inzicht nodig is

[34] {McDowell, 1998}.
[35] {Verschuren, 1996, 148}.
[36] {McDowell, 1998}, {Verschuren, 1996, 142-153}, {Dunn, 1994, 137-188}, {Van Heffen, 1993, 72-75}.
[37] {Hoogenboom, 2000, 21}, {March, 1994, 236-240}, {Cachet & Sluis, 2000, 174} en {Dunn, 1994, 149}.
[38] Zie {Lyre, 2000} voor een uitwerking.

In sommige gevallen is inzicht nodig in meer dan één domein, zoals voor een risicoanalyse van georganiseerde criminaliteit als gevolg van de ICT-ontwikkelingen. Het primaire domein is dan georganiseerde criminaliteit. Het secundaire domein betreft de context waarin of de ontwikkeling van waaruit gekeken moet worden naar risico's (zie figuur 2.2). Wanneer de verwachting is dat een risicoanalyse ook voor andere domeinen moet worden herhaald, dan verdient het aanbeveling om een specifiek analysekader te ontwikkelen. In dit proefschrift is voor georganiseerde criminaliteit een specifiek kader ontwikkeld van soorten veranderingen, risicofactoren en ongewenste effecten. Dit kader kan ook voor andere ontwikkelingen, specifieke gebeurtenissen en dergelijke worden benut.

2.4.4. Identificeren dreigingen

Tijdens deze stap staat de vraag centraal: wat zou er kunnen gebeuren? In principe kan deze vraag tot vele antwoorden leiden en is in beginsel ongericht. Denkbaar is om open bronnen te bestuderen op zoek naar door anderen reeds genoemde dreigingen. Een andere mogelijkheid is om experts te benaderen en hen te vragen naar dreigingen.

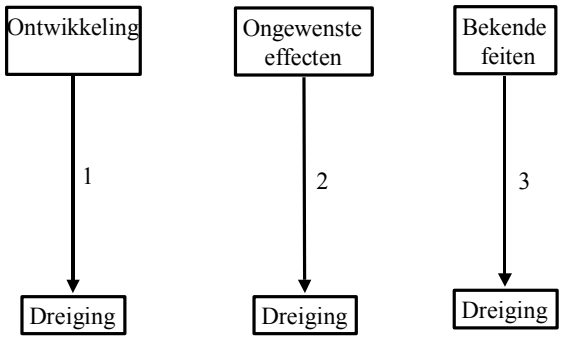
Met behulp van een conceptueel model is een meer gestructureerde werkwijze mogelijk. Dreigingen zijn dan op drie manieren te identificeren (zie figuur 2.3). Een *eerste* manier is om dreigingen te identificeren vanuit een specifieke ontwikkeling. 't Hart noemt dit vooruit-redeneren.[39] Het internet biedt voor legale ondernemingen vele mogelijkheden voor e-commerce. Een crimineel kan die benutten om bijvoorbeeld drugs via het internet aan te bieden. Een *tweede* manier is om dreigingen te beredeneren vanuit specifieke ongewenste effecten. 't Hart noemt dit achteruit-redeneren.[40] Vertrouwen in e-commerce door zowel consumenten als leveranciers is van groot belang om e-commerce verder te laten groeien en daardoor een economisch belang. Het vertrouwen in e-commerce neemt af wanneer criminelen fraude plegen met bijvoorbeeld creditcardbetalingen. Fraude met creditcardbetalingen is dus te beschouwen als dreiging. Een *derde* manier is om dreigingen te identificeren vanuit reeds bekende feiten. Naast andere vormen van creditcardfraude, is fraude als gevolg van diefstal van creditcardgegevens via het internet in opmars. Deze relatief nieuwe vorm van fraude, de dreiging, kan men ontdekken op basis van de fraudebestanden van creditcardmaatschappijen. Tot slot zijn mengvormen mogelijk.

Vooral het doel van de analyse en de opdracht bepalen welke van die manieren het meest geëigend is. De eerste manier is gehanteerd in hoofdstuk 6. De tweede manier is bruikbaar om de risico's van de invoering van de euro te beoordelen. De derde manier is geschikt voor de opdracht om risico's van fraude in werknemersverzekeringen te analyseren (zie figuur 2.2 in combinatie met figuur 2.3).

Tijdens deze stap kan men gebruikmaken van standaard onderzoeks- en analysetechnieken. Voorbeelden daarvan zijn: het uitvoeren van een literatuurstudie, het interviewen en brainstormen. Het voert te ver om in het kader van dit proefschrift de technieken te behandelen.[41]

---

[39] {'t Hart, 1998}.
[40] Idem.
[41] Zie voor deze technieken {Hogwood & Gunn, 1988}, {Bryson, 1995}, {McDowell, 1996}, {McDowell, 1998}, {Dunn, 1994}, en {Baarda e.a, 1997}.



Figuur 2.3 Manieren om dreigingen te identificeren

2.4.5. Beoordelen dreigingen

Tijdens deze stap moet een antwoord komen op de vraag hoe waarschijnlijk het is dat de dreiging zich manifesteert en wat de ongewenste effecten daarvan zijn. Het eerder ontwikkelde conceptuele model speelt hierbij een belangrijke ondersteunende rol. Per dreiging kan men in het model op zoek gaan naar de risicofactoren. Ook kan het model behulpzaam zijn bij de benoeming van ongewenste effecten. In sommige gevallen heeft een conceptueel model het karakter van een uitgewerkt analysekader. In dat geval zijn de risicofactoren en ongewenste effecten al benoemd (zie hoofdstuk 4). Dat kader dient dan als basis voor deze stap.

Het analistenteam kan aanvullend deskundigen vragen naar hun oordeel over de waarschijnlijkheid en de ongewenste effecten. Zij kunnen daarbij gebruikmaken van bestaande technieken, zoals interviewen, enquêteren en brainstormen. Tevens kan men op zoek gaan naar vergelijkbare dreigingen in het verleden en de mate van voorkomen en de ongewenste effecten daarvan onderzoeken. De invoering van de euro had bijvoorbeeld zijn historische gelijkenis met de invoering van de mark in het voormalige Oost-Duitsland.

Uiteindelijk is een totaaloordeel nodig. Voor de waarschijnlijkheid luidt dit oordeel in termen van 1) hoog of laag of 2) waarschijnlijk of niet-waarschijnlijk. Het oordeel voor de ongewenste effecten luidt in termen van ernstig of niet-ernstig. Wardlaw laat de analisten eerst ieder afzonderlijk de waarschijnlijkheid en de ongewenste effecten beoordelen. Vervolgens bespreken zij de afzonderlijke beoordelingen en ontstaat het totaaloordeel.[42] Een andere aanpak is om juist experts het oordeel te laten vellen. Op basis van het totaaloordeel over de waarschijnlijkheid en de ongewenste effecten kan men de risico's ordenen. Een denkbare ordening is de volgende:

1. Ongewenste effecten van ernstig, middel ernstig naar niet ernstig, waarbij als eerste voor de categorie ernstig de waarschijnlijkheid wordt geordend, vervolgens voor de categorie middel ernstig en daarna voor de categorie niet ernstig.
2. Waarschijnlijkheid van hoog naar laag.

[42] {Wardlaw, 1999}.

2.4.6. Schrijven eindrapportage

In dit stadium van de risicoanalyse zijn de analyses uitgevoerd en zijn de resultaten bekend. Het analistenteam kan nu het eindrapport schrijven. Dit eindproduct moet aansluiten bij de referentiekaders, de context en de cultuur van de belanghebbenden.[43] Naast de schriftelijke verwoording, is het ook belangrijk om presentaties te houden voor de verschillende doelgroepen van het risicoanalyseproduct.

Een onderdeel van de eindrapportage zou kunnen zijn het inventariseren en beoordelen van de mogelijk te treffen maatregelen. Ook een analyse van de kosten en de baten van de verschillende opties zou er onder kunnen vallen. De analist gaat daarmee wel op de stoel van de beleidsmakers zitten, iets wat Wardlaw afraadt.[44] Dunn, Hogwood en Gunn benoemen afzonderlijke producten voor een analyse van de problematiek, in dit geval een risicoanalyse, beleidsvoorstellen, evaluatie van bestaand beleid en dergelijke.[45] De mate waarin het formuleren van maatregelen en kosten-batenanalyses mogelijk en zinvol zijn, is mede afhankelijk van de fase waarin het beleidsproces zich bevindt. In de fase van beleidsvorming ligt dat bijvoorbeeld meer voor de hand dan in de fase van agendavorming. Tijdens de agendavorming zouden de analisten kunnen volstaan met algemene aanbevelingen op basis van de ordening van risico's (zie figuur 2.4).

Waarschijnlijkheid:	**Ongewenste effecten:**	
	Niet ernstig	*Ernstig*
Laag	Analytisch volgen van de ontwikkeling	Analytisch volgen van de ontwikkeling en voorbereidende maatregelen treffen
Hoog	Analytisch volgen van de ontwikkeling en voorbereidende maatregelen treffen	Preventieve en voorbereidende maatregelen treffen

Figuur 2.4 Mogelijke reacties op risico's[46]

2.5. Risicoanalyse voor vroegtijdige criminaliteitsbeheersing

Een risicoanalyse ten behoeve van vroegtijdige criminaliteitsbeheersing moet primair bijdragen aan de *agendavorming*. Daarom heeft de analyse vooral een verkennend karakter. Specifieke aspecten kunnen in een later stadium worden verdiept. In dat kader spreken analisten wel van het zogenaamde 'T-model'. Algemene analyses (de horizontale as van de T) vormen in die benadering de basis voor gerichte analyses (de verticale as).[47] De risicoanalyse richt zich verder op de inhoudelijke kant van de problematiek en niet op de oplossingen. Deze splitsing van probleemanalyse en oplossingen past bij een gefaseerde analyseaanpak voor de afzonderlijke fasen van het beleidsproces. Tevens wordt zo vermeden dat de analist op de stoel van de beleidsmaker gaat zitten.[48]

Een *kwalitatieve risicoanalyse* ligt meer voor de hand dan een kwantitatieve. Juist voor nieuwe risico's bestaan namelijk weinig informatie en kennis. Berekeningen zijn dus

[43] {Dunn, 1994, 416-417}, {Wardlaw, 1999}.
[44] {Wardlaw, 1999}.
[45] {Dunn, 1994}, {Hogwood & Gunn, 1988}.
[46] Deze indeling is deels gebaseerd op {Wardlaw, 1999}.
[47] {Klerks & Versteegh, 2000}.
[48] Zie subparagraaf 2.4.6.

nauwelijks mogelijk. Beredeneerde aannames en argumenten zijn daarentegen wel mogelijk. Bij voorkeur zijn daarom de belanghebbenden betrokken bij de analyse. Er bestaan immers veel onzekerheden over de ontwikkelingen, de daaruit voortkomende veranderingen en de ongewenste effecten. De afzonderlijke belanghebbenden beschikken ieder over andere deskundigheid, informatie, en kennis en hebben andere rollen en belangen. Hierdoor variëren de percepties van de situatie. Door communicatie over en weer zullen nieuwe of aangepaste percepties zich ontwikkelen en vervlecht raken. Tevens kunnen de belanghebbenden het gezamenlijke belang ontdekken en de gezamenlijke doelen. Zo ontstaat een beter draagvlak voor het eindproduct en een betere basis voor risicobeheersing. Een risicoanalyse is immers ook een instrument in een bewustwordings- en beïnvloedingsproces.[49]

Het karakter van de risicoanalyse is *strategisch* van aard. Vroegtijdige criminaliteitsbeheersing richt zich immers op het overwegen en treffen van maatregelen voordat de dreigingen zich daadwerkelijk manifesteren. In dit stadium doen de dreigingen zich in principe nog niet voor, waardoor een tactische risicoanalyse geen functie heeft. De inzichten vanuit de strategische risicoanalyse kunnen wel worden gebruikt om in een later stadium tactische analyses van af te leiden. Het niveau van de analyse is het *macroniveau* vanwege het verkennende en strategische karakter. In een later stadium kan de analyse worden verdiept naar specifieke sectoren, regio's en dergelijke (mesoniveau).

[49] Klijn en Termeer gaan in op de interactie tussen belanghebbenden en het voordeel daarvan {Klijn, 1993, 66}, {Termeer, 1993, 114}.

3. Georganiseerde criminaliteit

3.1. Inleiding

Dit hoofdstuk beschrijft het tweede onderdeel van het risicoanalyse-instrumentarium, namelijk een conceptualisering van georganiseerde criminaliteit. Georganiseerde criminaliteit is immers geen eenduidig begrip en er bestaan vele definities en theoretische invalshoeken. Paragraaf 3.2 gaat in op enkele theoretische hoofdstromen. In paragraaf 3.3 komt in algemene zin de definitiekwestie aan de orde. Vervolgens behandelt paragraaf 3.4 de definitie van de onderzoeksgroep Fijnaut die gezaghebbend is in Nederland. Op basis van de beoordeling daarvan volgt een verantwoording van de aannames in dit proefschrift en een eigen definitie (paragraaf 3.5). Afzonderlijke paragrafen besteden vervolgens aandacht aan de sleutelbegrippen in die definitie, namelijk: misdaadmarkt, illegale groothandelsonderneming en illegale groothandelsactiviteiten (paragraaf 3.6 tot en met 3.8). Tot slot beschrijft paragraaf 3.9 de afbakening met de omgeving.

3.2. Theoretische hoofdstromen

Er bestaan vele definities van georganiseerde criminaliteit en er zijn verschillende invalshoeken gehanteerd voor de theorievorming.[1] Het begrip vindt zijn oorsprong in de Verenigde Staten en is een vertaling van 'organized crime'. Vooral daar bestaat een rijke onderzoekstraditie op dit terrein. Vele inzichten zijn daarvandaan overgewaaid naar Nederland.[2]

Klerks benoemt drie hoofdstromen in de theorievorming in de Verenigde Staten. De hoofdstromen zijn:

> *"Het traditionele beeld, populair bij wetshandhavers en de pers, dat georganiseerde misdaad als een hiërarchisch gestructureerde samenzwering van etnisch onderscheiden groepen voorstelt (aanvankelijk met name Italianen), waarbij criminaliteit als een dreiging van buitenaf wordt gezien voor een op zichzelf stabiele maatschappij.*
>
> *De structureel-functionalistische stroming, voortkomend uit met name etnografisch veldonderzoek, die criminele groepen heeft beschreven als een samenstel van veelal etnische netwerken opgebouwd uit wederzijdse afhankelijkheidsrelaties, en gekenmerkt door tijdelijke gelegenheidscoalities van opportunisten die deels in een symbiotische relatie staan met de reguliere samenleving.*
>
> *De visie dat georganiseerde criminaliteit niets anders is dan een stelsel van ondernemingen. Zakendoen dus, maar aan de andere kant van het legaliteitsspectrum."*[3]

[1] Zie bijvoorbeeld {Enquêtecommissie, 1996B}, {Ruggiero, 1996}, {Maltz, 1990}, {Klerks, 2000}, {Van Duyne e.a., 1990}, {Bovenkerk, 2001}, {Paoli, 2002, 53-63}, {Van Duyne e.a., 2001, 50-51}.
[2] {Klerks, 2000, 15}, {Bovenkerk, 2001}, {Enquêtecommissie, 1996B}.
[3] {Klerks, 2000, 36}.

Klerks noemt hoofdstroom één 'etnische samenzwering', hoofdstroom twee de 'structureel-functionalistische benadering' en hoofdstroom drie het 'enterprisemodel', ook wel aangeduid als de bedrijfsmatige benadering.[4]

Kleemans e.a. identificeren eveneens drie stromingen, die zij aanduiden als oerbeelden. Zij onderscheiden binnen georganiseerde criminaliteit: 1) een centraal geleide samenzwering van buitenstaanders die de samenleving bedreigt, 2) een bureaucratische organisatievorm en 3) illegaal ondernemerschap. Zij splitsen dus de eerste hoofdstroom van Klerks in twee afzonderlijke oerbeelden. Met een bureaucratische organisatievorm bedoelen zij een piramidale organisatie met een strenge hiërarchie, een duidelijke taakverdeling, een gedragscode en een intern sanctiesysteem.[5] De onderzoekers zelf kiezen een ander perspectief, namelijk die van in netwerken samenwerkende criminelen. Deze benadering maakt onderdeel uit van hoofdstroom twee van Klerks, de structureel-functionalistische benadering.

Geen van de drie hoofdstromen of oerbeelden – verder aangeduid als hoofdstromen – beschrijft exclusief de waarheid. De onderzoekers kijken vanuit verschillende invalshoeken naar dezelfde werkelijkheid, hebben een selectieve waarneming en gebruiken uiteenlopende instrumentaria. De hoofdstromen zijn de laatste jaren naar elkaar toe gegroeid en er bestaat een overlapping daartussen.[6]

Er is een analogie te zien tussen de Amerikaanse en de Nederlandse ideeënontwikkeling. In Nederland is lange tijd naar georganiseerde criminaliteit gekeken vanuit de optiek van min of meer stabiele en hiërarchische organisaties, ook wel aangeduid als 'het maffiamodel'. Dit past binnen hoofdstroom één van Klerks en oerbeeld twee van Kleemans e.a. De bedrijfsmatige invalshoek is in Nederland toegepast door onderzoekers van het WODC, vooral door Van Duyne. Met het verschijnen van de rapportage van de onderzoeksgroep Fijnaut is in Nederland de invalshoek van in netwerken opererende criminelen, onderdeel van de tweede hoofdstroom, in zwang geraakt. Deze invalshoek is ook gekozen in de WODC-rapportages uit 1999 en 2002.[7]

3.3. Definitie van georganiseerde criminaliteit: algemeen

Er is een voortdurende strijd (gevoerd) over de definitie, niet alleen binnen Nederland, maar ook daarbuiten.[8] Het verschil tussen georganiseerde en andere vormen van criminaliteit ligt (ogenschijnlijk) besloten in het woord georganiseerd. Toch is niet op voorhand duidelijk waarop dat betrekking heeft. Het ligt voor de hand om het onderscheid te zoeken in de kenmerken van de groep die criminaliteit pleegt of in de criminele activiteit. Variaties daarop vormen de kenmerken van het proces, de pleegwijze of de functie.[9] Overeenstemming daarover bestaat niet en dat zien we terug in de definities.

[4] Idem.
[5] {Kleemans e.a., 1999, 32}.
[6] {Klerks, 2000, 36, 84-94}, {Kleemans e.a., 1999, 32}.
[7] {Klerks, 2000, 94-95}, {Kleemans e.a., 1999, 34-35}, {Kleemans e.a., 2002}.
[8] Zie bijvoorbeeld {Enquêtecommissie, 1996B, 12-22}, {Ruggiero, 1996, 26-30}, {Maltz, 1990, 121}, {Paoli, 2002, 53-63}, {Klerks, 2000, 35-167}, {Bovenkerk, 2001}, {Van Duyne e.a., 2001, 50-51}.
[9] {Halstead, 1998, 1, 10, 22-23}, {Adamoli e.a., 1998 e.a., 1998, 4}, {Enquêtecommissie, 1996B, 23-24}, {Paoli, 2002, 55}.

Uiteraard bepaalt de hoofdstroom waartoe men zich rekent voor een belangrijk deel de definitie. Daarin komen allerlei kenmerken voor, die niet (altijd) overeenkomen. Een piramidale organisatie en het gebruik van corruptie en geweld zijn discriminerende kenmerken voor auteurs die vallen onder hoofdstroom één van Klerks en oerbeelden één en twee van Kleemans e.a. In de andere hoofdstromen zijn dit daarentegen geen discriminerende kenmerken en komen ze veelal niet voor. Verder zien we variatie in de vormgeving. Sommigen, waaronder de onderzoeksgroep Fijnaut[10], kiezen voor een definitie in de vorm van een formule. Anderen kiezen juist voor een opsomming van kenmerken.[11] Een voorbeeld van de tweede soort is de EU-definitie (zie figuur 3.1).

De volgende vier criteria moeten altijd aanwezig zijn wil sprake zijn van georganiseerde criminaliteit:

1. Een samenwerkingsverband van meer dan twee personen.
2. Een samenwerkingsverband voor een langdurige of onbepaalde duur.
3. Een samenwerkingsverband dat wordt verdacht van ernstige strafbare feiten.
4. Een samenwerkingsverband dat is gericht op streven naar winst.

Op de volgende vragen moet het antwoord minstens twee keer ja luiden wil sprake zijn van georganiseerde criminaliteit:

5. Een samenwerkingsverband waarbij sprake is van een specifieke taakverdeling tussen de leden van het samenwerkingsverband.
6. Een samenwerkingsverband waarbij sprake is van disciplinering.
7. Een samenwerkingsverband dat internationaal actief is.
8. Een samenwerkingsverband dat gebruikmaakt van geweld of andere intimidatiemiddelen.
9. Een samenwerkingsverband dat gebruikmaakt van commerciële en zakelijke activiteiten.
10. Een samenwerkingsverband waarbij sprake is van witwassen van criminele inkomsten.
11. Een samenwerkingsverband dat invloed op politiek, media, openbaar bestuur, justitie of economie heeft.[12]

Figuur 3.1 EU-criteria voor georganiseerde criminaliteit

Naast definities voor wetenschappelijke doeleinden, treffen we ook definities aan voor operationeel gebruik. Zo gebruikte de politie in Nederland voor 1996 een lijst met kenmerken waaraan een criminele groep moet voldoen. Een andere operationele definitie is die van het Duitse Bundeskriminalamt.[13] Dergelijke definities bepalen voor een deel de afbakening tussen organisatieonderdelen. In Nederland richten de Nationale Recherche[14] en de divisies (zware en) georganiseerde criminaliteit van de regionale korpsen zich op georganiseerde criminaliteit. De districten houden zich daarentegen met andere vormen van criminaliteit bezig. Ook de bovenregionale rechercheteams richten zich niet op georganiseerde criminaliteit. Als gevolg van de taakafbakening hebben die organisaties belang bij een bepaalde definitie. Het bepaalt immers hun werkterrein. Achter een definitie schuilt verder een beeld van de werkelijkheid, evenals een weerspiegeling van de belangen. Brancheorganisaties van banken, creditcardmaatschappijen en dergelijke trekken wel heel

[10] Zie paragraaf 3.4 voor de definitie van de onderzoeksgroep Fijnaut.
[11] {Van Duyne e.a., 2001}.
[12] {De Vette e.a., 1999}
[13] Zie bijvoorbeeld {Klerks, 2000, 135}.
[14] De voormalige kernteams zijn per 1 juli 2003 opgegaan in de Dienst Nationale Recherche van het Korps Landelijke Politiediensten (KLPD).

snel de criminaliteit waarmee zij te maken hebben in het kamp van georganiseerde criminaliteit.[15] Zij hopen daarmee dat de politie actie onderneemt. Hoewel de wetgever niet expliciet georganiseerde criminaliteit in het Wetboek van Strafrecht heeft opgenomen, heeft de politie voor de bestrijding daarvan wel extra bevoegdheden. De definitie is daardoor (impliciet) medebepalend voor het bevoegdhedenrepertoire.

Empirisch gezien bestaat dé georganiseerde criminaliteit niet omdat het verschilt tussen landen. Het neemt de kleur aan van de economie, cultuur en de demografische en bestuurlijke context waarin het zich manifesteert. Zo verklaart het specifieke politieke systeem in de Verenigde Staten enkele verschillen ten opzichte van andere landen. Voor bijvoorbeeld corruptie maakt het nogal uit met welke ambtelijke en politieke cultuur georganiseerde criminaliteit te maken heeft.[16] Nederland is in tegenstelling tot Schotland een doorvoerland, waardoor de handel zich richt op grotere partijen. Een partij drugs waar men in Nederland niet van onder de indruk is, kan in Schotland de vangst van de eeuw zijn. Deze verschillen beïnvloeden de definities en de literatuur over georganiseerde criminaliteit van landen. Definities en empirische bevindingen uit andere landen zijn daarom niet zonder meer bruikbaar voor Nederland. Ook binnen Nederland bestaat empirisch gezien dé georganiseerde criminaliteit niet. Zo wijst de onderzoeksgroep Fijnaut op verschillen tussen Amsterdam, Nijmegen, Arnhem en Enschede.[17]

De vraag is dus überhaupt of er ooit één allesomvattende definitie mogelijk is. In elk geval zal een dergelijke definitie op enigerwijze bruikbaar moeten zijn voor de afzonderlijke doelen en rekening moeten houden met de uiteenlopende belangen. Het bereiken van overeenstemming over een definitie heeft daarom veel weg van compromisvorming.

3.4. Definitie onderzoeksgroep Fijnaut

De definitie van de onderzoeksgroep Fijnaut is gezaghebbend in Nederland. Zowel wetenschappers, politiemedewerkers als beleidsambtenaren gebruiken deze.[18] Daarom komt deze definitie hier uitgebreid aan bod. Deze verhandeling vormt de opmaat voor de conceptualisering in dit proefschrift (zie paragraaf 3.5).

Zoals eerder is aangegeven, is niet op voorhand duidelijk waarop georganiseerd betrekking heeft en wat kenmerkend is ten opzichte van andere vormen van criminaliteit. De onderzoeksgroep kiest er voor om de daders centraal te stellen in de definitie. “Georganiseerde criminaliteit onderscheidt zich van andere vormen van criminaliteit in de opstelling van de plegers. Zij zijn in een aantal opzichten bereid en in staat «verder» te gaan dan andere misdrijfplegers”. De onderzoeksgroep doelt dan op het verdedigen van de positie met verregaande middelen, waaronder het gebruik van geweld.[19]

De onderzoeksgroep heeft een eigen definitie van georganiseerde criminaliteit ontwikkeld. Zij heeft bewust *niet* gekozen voor een enge definitie waardoor er alleen maffia-achtige

[15] Eigen indruk.
[16] {Fijnaut, 1996B, 24}, {Van Duyne e.a., 1990, 17}, {Kleemans e.a., 1999, 63}, {Wiebrens & Röell, 1988, 75}.
[17] {Enquêtecommissie, 1996B}.
[18] Zie bijvoorbeeld {Kleemans e.a., 1999}, {Kleemans e.a., 2002}, {Kernteam Noord- en Oost-Nederland, 2001}, {Criminaliteitsbeheersing, 2001, 31}.
[19] {Enquêtecommissie, 1996B, 24}.

organisaties onder zouden vallen. Zij heeft ook *niet* gekozen voor een ruime definitie die een te grote verscheidenheid aan criminaliteit onder het begrip plaatst.[20] In latere artikelen lichten leden van de onderzoeksgroep die keuze nog eens toe. "Het belangrijkste beleidsprobleem was niet zozeer de verontrusting over de omvang, maar over de aard van de problematiek, namelijk de verweving van georganiseerde criminaliteit met de legale sectoren van de samenleving".[21] Volgens Fijnaut was de belangrijke achterliggende vraag de proportionaliteit van het probleem van georganiseerde criminaliteit enerzijds en het arsenaal aan noodzakelijke en aanvaardbare opsporingsmethoden anderzijds. Een ruimere definitie vond de onderzoeksgroep minder gepast. "Zij zou al vlug hebben geleid tot een artificiële vergroting, vermeerdering, opwaardering van het probleem en zodoende zijn uitgelopen op disproportionele ideeën over verdergaande uitbreiding van het arsenaal aan bijzondere opsporingsmethodes en over de schaalvergroting van de feitelijke toepassing".[22] Dit standpunt is overigens meer normatief dan wetenschappelijk van aard.

De definitie van de onderzoeksgroep luidt:

> *"Er is sprake van georganiseerde criminaliteit indien groepen, die primair gericht zijn op illegaal gewin, systematisch misdaden plegen met ernstige gevolgen voor de samenleving en in staat zijn deze misdaden op betrekkelijk effectieve wijze af te schermen, in het bijzonder door de bereidheid te tonen fysiek geweld te gebruiken of personen door middel van corruptie uit te schakelen."*[23]

De definitie bestaat uit drie onderdelen: a) groepen die primair gericht zijn op illegaal gewin, b) systematisch misdaden plegen met ernstige gevolgen voor de samenleving en c) in staat zijn zich op betrekkelijk effectieve wijze af te schermen. Deze drie onderdelen zijn onlosmakelijk met elkaar verbonden en moeten gelijktijdig aanwezig zijn.[24]

Het *eerste onderdeel* heeft betrekking op groepen die primair zijn gericht op illegaal gewin. De onderzoeksgroep stelt weinig eisen aan de omvang of de aard van de groepen. Zo hoeft er geen sprake te zijn van een hiërarchische structuur en/of een uitgebalanceerde taakverdeling. Het kunnen ook knooppunten in sociale netwerken zijn waartussen een rudimentaire taakverdeling bestaat. Het onderdeel 'primair gericht op illegaal gewin' vormt een belangrijke inperking. Hierdoor zijn politiek geïnspireerde misdrijven of misdrijven die uitsluitend worden begaan om politieke macht te verwerven, uitgesloten. Bovendien is organisatiecriminaliteit uitgesloten.[25]

Er bestaat kritiek op dit onderdeel van de definitie. Het element 'primair gericht op illegaal gewin' is niet eenduidig. Verder is niet duidelijk of er een ondergrens geldt voor het gewin. Het element groep is niet geoperationaliseerd. Klerks neemt aan dat hiermee een ondergrens van drie personen wordt verondersteld.[26] Het onderscheid tussen georganiseerde en organisatiecriminaliteit deelt niet iedereen. Ruggiero vindt het niet correct dat in feite niet de (mis)daad of de gehanteerde werkwijze bepalend is voor het onderscheid,

[20] {Enquêtecommissie, 1996B, 23}.
[21] {Bovenkerk e.a., 1997, 58}.
[22] {Fijnaut, 1996A, 81}.
[23] {Enquêtecommissie, 1996B, 24-25}.
[24] {Enquêtecommissie, 1996B, 24-25, 27}.
[25] {Enquêtecommissie, 1996B, 25-26}
[26] {Van Duyne, 1996, 49-57}, {Klerks, 2000, 151}.

maar de dader. Hij stelt dat het achterliggende mensbeeld is gebaseerd op 'zij die aan de algemene norm voldoen en de normlozen. Degenen met een hoog aanzien en/of een hoog inkomen plegen organisatiecriminaliteit. Personen met een lage sociale status en/of een laag inkomen houden zich bezig met georganiseerde criminaliteit. Het type criminaliteit verschilt daarentegen in essentie niet en gewone ondernemers werken ook samen met plegers van georganiseerde criminaliteit. En ook de intentie verschilt niet veel. Zowel een ondernemer die misdaden pleegt als een ondernemende misdadiger, wil zich verrijken.[27] Het onderscheid is bovendien lastig hanteerbaar in de praktijk omdat allerlei tussenvormen voorkomen. Klerks is evenmin overtuigd dat er een wezenlijk verschil bestaat tussen een criminele ondernemer en een ondernemende crimineel. Bovendien is het in sommige gevallen arbitrair of in de beschrijvingen van de onderzoeksgroep niet toch sprake is van organisatiecriminaliteit.[28] In een artikel dat na de afronding van het onderzoek tot stand is gekomen, blijft de onderzoeksgroep van mening dat er voldoende redenen zijn voor het aanbrengen van een analytisch onderscheid tussen georganiseerde en organisatiecriminaliteit.[29] Die redenen specificeert de onderzoeksgroep niet in dat artikel.

Van Dijk e.a. vinden het een nadeel dat politiek gemotiveerde criminaliteit buiten wordt gesloten. Zij wijzen bijvoorbeeld op de bindingen tussen criminele groepen met het Koerdisch verzet of de IRA. Ook noemen zij de betrokkenheid van de Surinaamse legerleiding bij de cocaïnehandel. De voormalige legertop is niet primair gericht op de drugshandel en valt dus niet onder georganiseerde criminaliteit. Ondanks het buitensluiten van politiek gemotiveerde criminaliteit, constateert Klerks dat de activiteiten van de PKK volop aandacht krijgen in de rapportage van de onderzoeksgroep.[30] De onderzoeksgroep heeft zich in een later artikel verdedigd tegen deze kritiek. Het op één hoop vegen van criminaliteit die wel of niet politiek is georiënteerd, werkt eerder verwarrend dan verhelderend. Dit betekent volgens de onderzoeksgroep niet dat de genoemde groepen buiten de analyse van de problematiek vallen.[31] Hoe dit valt te rijmen, is niet helder.

Het *tweede onderdeel* in de definitie heeft betrekking op het systematisch misdrijven plegen met ernstige gevolgen voor de samenleving.

> *"Ernstige misdrijven hebben niet zonder meer ernstige gevolgen voor de samenleving. Dit geldt evenzo voor systematisch gepleegde misdrijven. Een incidentele ontvoering, het exploiteren van een kleine hasjlijn of systematisch gepleegde fietsendiefstallen worden, met andere woorden, niet tot de georganiseerde criminaliteit gerekend. Uiteraard is deze afgrenzing arbitrair en subjectief; wanneer kan van 'ernstige' gevolgen worden gesproken? Wij hebben er vanaf gezien om deze ondergrens te specificeren. Met dit onderdeel van de definitie wordt alleen onderstreept dat georganiseerde criminaliteit zich niet slechts tegen personen keert, maar ook floreert ten koste van markten of de samenleving als geheel".*[32]

Er bestaat veel kritiek op dit onderdeel van de definitie. Van Duyne heeft als bezwaar dat het twee ongelijksoortige delen bevat: stelselmatigheid en de ernst van de gevolgen.

[27] {Ruggiero, 1996, 155}.
[28] {Klerks, 2000, 151}, {Van Dijk e.a., 1996, 252-253}, {Van Duyne, 1996, 57-59}.
[29] {Bovenkerk e.a., 1997, 58-59}.
[30] {Klerks, 2000, 151}, {Van Dijk e.a., 1996, 252-253},
[31] {Bovenkerk e.a., 1997, 59}.
[32] {Enquêtecommissie, 1996B, 26}.

Volgens hem is niet helder of de misdaden op zichzelf ernstige gevolgen moeten hebben of dat het gaat om de gevolgen van de stelselmatigheid of van beide. Overigens blijkt uit de toelichting van de onderzoeksgroep dat het om beide gaat. Stelselmatigheid wijst op een regelmaat of reeks van handelingen, maar bevat ook een tijdsbestanddeel. Klerks onderkent twee andere betekenissen van stelselmatigheid. Het kan de betekenis krijgen van 'meer dan incidenteel'. Het kan echter ook duiden op de wijze van acteren: gepland, volgens afspraken en procedures. Hij neemt aan dat met misdaden wordt bedoeld de categorie misdrijven waarvoor voorlopige hechtenis is toegelaten. Verder is niet duidelijk of "[….] het om verdenkingen, aanwijzingen of welke andere graad van zekerheid dan ook moet gaan, en evenmin is duidelijk of ook voorbereiding, deelneming, poging et cetera in relatie tot de 'misdaden' er onder vallen".[33]

De critici vinden het element 'ernstige gevolgen voor de maatschappij' subjectief en dus wetenschappelijk onbruikbaar, tenzij het nader wordt geoperationaliseerd. Van Duyne vindt dat de aard van de afscherming, het derde onderdeel van de definitie, als versterker van de ergheid fungeert. Immers de afscherming is ook een noodzakelijk onderdeel indien die afscherming gepaard gaat met geweld of corruptie. Hij stelt dat deze overlapping niet mag in een definitie.[34] Overigens gaat hij er dan van uit dat dit kenmerk van de groep behoort tot 'ernstige gevolgen voor de samenleving'. In paragraaf 4.8 wordt betoogd dat dit niet het geval is. In een verweer op de kritiek stelt de onderzoeksgroep dat bij een descriptief breed opgezet onderzoek de keuze voor een open karakter van 'ernstige gevolgen' verstandig is.[35]

Het *derde onderdeel* in de definitie heeft betrekking op het in staat zijn zich op betrekkelijk effectieve wijze af te schermen.

> *"Sommige van deze methoden richten zich tegen de eigen leden, andere richten zich meer rechtstreeks tegen de overheid. In het scala van deze methoden (voortaan 'contrastrategieën') moet onderscheid gemaakt worden tussen defensieve en offensieve contrastrategieën. Defensieve contrastrategieën hebben betrekking op de wijzen waarop groepen hun illegale optreden proberen te verheimelijken tegenover concurrenten en de overheid. [….] Kenmerkend voor de georganiseerde criminaliteit is de bereidheid (en het vermogen) om offensieve contrastrategieën tegen de overheid te gebruiken. Het gaat er hier niet langer om het eigen optreden te verheimelijken tegenover de overheid, maar om het overheidsoptreden zelf actief te bestrijden".*[36]

Dit onderdeel bevat vaagheden in de formulering. Vaag zijn de elementen 'in staat zijn', 'op betrekkelijk effectieve wijze', 'in het bijzonder', 'door de bereidheid te tonen fysiek geweld te gebruiken' en 'uit te schakelen'. Van Duyne vindt het een doodzonde dat er een open lijst van afschermingsmiddelen wordt gegeven. Ook is het begrip corruptie niet geoperationaliseerd. Gaat het om een strafrechtelijke omschrijving?[37]

[33] {Van Duyne, 1996, 49-57}, {Klerks, 2000, 151-152}.
[34] {Van Duyne, 1996, 49-57}, {Van Dijk e.a., 1996, 252-253}, {Van Dijk, 1996, 78}.
[35] {Bovenkerk e.a., 1997, 59-60}.
[36] {Enquêtecommissie, 1996B, 27-28}.
[37] {Klerks, 2000, 152-153}, {Van Duyne, 1996, 49-57}.

Inhoudelijk bestaat eveneens kritiek. Klerks stelt dat het element afscherming doorgaans niet in definities wordt opgenomen en dus nieuw is. Kleemans e.a. (1999 en 2002), Van Duyne en Klerks stellen dat offensieve contrastrategieën, geweld en corruptie geen noodzakelijke instrumenten vormen en dat het gebruik ervan lang niet altijd verstandig is. Van Dijk (e.a.) vinden het een gemis dat de onderzoeksgroep innesteling in de legale economie niet als afzonderlijk kenmerk beschouwt. Zij vinden innesteling een wezenlijker kenmerk dan afscherming.[38] In een later artikel geeft de onderzoeksgroep toe dat zij het begrip afscherming beter had moeten uitwerken. De onderzoeksgroep verstaat onder afscherming niet alleen corruptie en geweld tegen politie en justitie, maar ook meer geavanceerde vormen van afscherming. Voorbeelden daarvan zijn de afscherming van illegaal verworven winsten en het geleidelijk veroveren van een machtspositie in de legale economie door het opkopen van legale bedrijven. Dit laatste vindt zij één van de meest gevaarlijke vormen van afscherming.[39]

Van Duyne is van mening dat de definitie van de onderzoeksgroep niet voldoet aan de technische eisen. Bovendien is volgens hem de ergheidsdiscussie tijdens de Parlementaire Enquêtecommissie onvoldoende gevoerd. De definitie stoelt te veel op het beeld van Boris Boef en Dagobert Duck.[40] Impliciet stelt hij daarmee dat te veel is geredeneerd vanuit de onderwereld naar de bovenwereld en niet omgekeerd.

Bovenkerk, één van de leden van de onderzoeksgroep, vraagt zich in 2001 af of de definitie niet te veel is aangepast om haar voor Nederland kloppend te maken. Hij is van mening dat de essentie van georganiseerde criminaliteit is opgesloten in de Amerikaanse definitie. “Ondernemers beheersen de handel in illegale goederen en diensten en zij oefenen macht uit om hun markt te ordenen met behulp van (de dreiging van) privaat geweld”. Private ondernemers nemen in die optiek de twee belangrijkste monopolies van de overheid over, namelijk het gebruik van geweld en het recht om belasting te heffen. Zij vormen als het ware een alternatieve overheid. Bovenkerk ontleent daaraan de gevolgtrekking dat hij geen georganiseerde criminaliteit kan identificeren in Nederland.[41] Een misdaadanalist van het korps Amsterdam Amstelland stelde daarentegen in 1998 dat volgens de definitie van de onderzoeksgroep er geen georganiseerde criminaliteit voorkwam in Amsterdam.[42]

De definitie van de onderzoeksgroep Fijnaut heeft dus geen consensus kunnen brengen. Dit geldt voor de inhoudelijke keuzen, voor de formulering en de gehanteerde begrippen. Onduidelijk en/of arbitrair blijft de kern van georganiseerde criminaliteit. Dit speelt vooral bij de afbakening van georganiseerde criminaliteit ten opzichte van andere vormen van criminaliteit en andere daders. Bovendien sluit de insteek van de onderzoeksgroep voor de daders niet aan bij de gelegenheidstheorie die juist uitgaat van de criminele gebeurtenis.

[38] {Kleemans e.a., 1999, 117-118}, {Kleemans e.a., 2002, 91-96}, {Van Duyne, 1995}, {Van Duyne, 1996}, {Klerks, 2000, 152-159}, {Van Dijk e.a., 1996, 252-253}, {Van Dijk, 1996, 78}.
[39] {Bovenkerk e.a., 1997, 59-60}.
[40] {Van Duyne, 1996}.
[41] {Bovenkerk, 2001, 13, 21, 30-32}
[42] Eigen waarneming.

3.5. Georganiseerde criminaliteit als stelsel van illegale groothandelsondernemingen

Ondanks de uiteenlopende hoofdstromen en definities bestaat unanimiteit over de belangrijkste drijfveer van de plegers. Zij streven naar financieel gewin door strafbare feiten te plegen.[43] Door dit kenmerk vallen vele soorten daders en criminaliteit af. Terroristen streven bijvoorbeeld niet naar financieel gewin, maar naar realisatie van politieke idealen. Geld is daarvoor instrumenteel. Hooligans plegen geen strafbare feiten om geld te verdienen, maar voor de opwinding. Pedofielen plegen criminaliteit vanwege hun seksuele geaardheid. De activiteiten van terroristen, hooligans en pedofielen vallen dus buiten het begrip georganiseerde criminaliteit.

Er bestaan enkele mogelijkheden om op illegale wijze geld te verdienen. Eén mogelijkheid is de handel in illegale goederen en diensten. Deze kunnen verboden of streng gereguleerd zijn, zoals drugs- of mensensmokkel. Er bestaan ook vele andere mogelijkheden om op illegale wijze geld te verdienen zonder dat sprake is van handel. Voorbeelden zijn het plegen van een overval, een ontvoering, creditcardfraude en oplichting van een bank. Volgens Paoli komt in vele definities op enige wijze naar voren dat georganiseerde criminaliteit zich bezighoudt met de levering van of handel in illegale goederen en diensten. Volgens Bovenkerk bestaat zelfs eenstemmigheid over het feit dat georganiseerde criminaliteit zich richt op de handel in illegale goederen en diensten.[44] Anderen rekenen ook vormen van criminaliteit waarbij geen sprake is van handel tot georganiseerde criminaliteit, zoals bankovervallen.[45]

In dit proefschrift geldt als uitgangspunt dat georganiseerde criminaliteit zich bezighoudt met de handel in illegale goederen en diensten. Daar vloeit uit voort dat sprake moet zijn van een vragende en een aanbiedende partij en dat een transactie tussen hen vrijwillig totstandkomt. Afpersing, veel genoemd als activiteit van georganiseerde criminaliteit, valt daar níét onder. Wanneer we afpersing zouden beschouwen als illegale dienst, dan zou de afperser de aanbieder moeten zijn en het afgeperste individu de vragende partij. Daarbij is sprake van gedwongen winkelnering omdat de afperser de vraag opdringt. Bovendien is geen sprake van een vrijwillige transactie. Bij een bankoverval kunnen we evenmin spreken van een vrijwillige transactie tussen een vragende en een aanbiedende partij.

Het onderscheid tussen een goed of dienst is veelal gradueel, variërend ergens tussen 100% fysieke goederen en 100% dienstverlening. Cocaïne is een illegaal goed en, mensensmokkel is een illegale dienst. Hoewel cocaïne een goed is, speelt daarbij ook een zekere mate van dienstverlening een rol, zoals levering op het afgesproken moment en plaats. Bij mensensmokkel spelen ook goederen een rol, zoals vervalste papieren en vervoermiddelen. Een goed en een dienst noemt men gezamenlijk een product.

Legale handel vindt plaats in markten tussen vragende en aanbiedende partijen die op vrijwillige basis een transactie met elkaar aangaan. In markten opereren verschillende partijen met elk hun eigen activiteiten. Voordat een product bij een consument terecht-

[43] {Van Duyne e.a., 1990}, {Van Duyne, 1995}, {Chang, 1998, 23}, {Halstead, 1998, 9}, {Lupsha, 1996, 34}, {Adamoli e.a., 1998}, {Reuter, 1984}, {Enquêtecommissie, 1996B, 24-25}, {Williams & Godson, 2002}, {NCIS, 2002, 6}.
[44] {Bovenkerk, 2001, 21} en {Paoli, 2002}. Bovenkerk stelt dat ook overeenstemming bestaat over afpersing als activiteit van georganiseerde criminaliteit. Deze benadering wordt hier niet overgenomen. Zie verderop in deze paragraaf.
[45] Zie bijvoorbeeld de onderzoeksgroep Fijnaut {Enquêtecommissie, 1996B, 46}.

komt, is een geheel proces doorlopen. Zo is een stuk vlees op het bord in een restaurant voorafgegaan door activiteiten van de veevoederproducent, de boer, de transporteur, de slachter, de slager, de kok en de ober. In een markt kunnen we dus uiteenlopende rollen onderscheiden. Een product vindt zijn weg naar de consument via distributiekanalen. McCarthy maakt daarbij een onderscheid tussen producent, detailhandel en groothandel.[46] In theorie zou een restaurant zelf vee kunnen houden en slachten. Toch zien we dat restaurants overwegend vlees inkopen bij de groothandel of de detailhandel. Een boer die vlees levert aan velen, kan op veel grotere schaal vee houden. Dit brengt allerlei voordelen met zich mee. De inspanning voor bijvoorbeeld de inkoop van veevoer voor één koe is niet veel groter dan de inkoop voor honderd koeien. Een slachterij kan zich toeleggen op de slacht en daardoor eveneens schaalgroottevoordelen realiseren. Doordat ondernemingen zich toeleggen op een specifieke rol, dalen de kosten. In theorie zou het dan nog steeds mogelijk zijn dat een restaurant het vlees inkoopt bij een boer en naar de slachterij brengt. Toch is het goedkoper wanneer anderen deze rollen van het restaurant overnemen. Ook zij kunnen schaalgroottevoordelen realiseren. Elke partij in een markt profiteert in principe van de specialisatie en schaalgroottevoordelen van de afzonderlijke marktpartijen.[47]

Toch hebben specialisatie en schaalgrootte niet alleen voordelen. Nadelen zijn namelijk dat er een grotere professionaliteit en meer organisatie, kennis, vaardigheden en kapitaal zijn vereist. Als gevolg daarvan zijn niet alle ondernemingen in staat om de potentiële schaalgroottevoordelen te benutten en de specialistische rol op zich te nemen. Dat is slechts voor enkelen weggelegd. Er zijn nog andere nadelen. Als gevolg van specialisatie zijn vele partijen betrokken bij een product en iedereen wil daarvan een graantje meepikken. Bovendien stijgen de transactiekosten. Eenvoudig gezegd zijn dit de kosten die samenhangen met de handel tussen partijen.[48] Wanneer één van de marktpartijen de rol van anderen overneemt, kan hij die winst opstrijken en zich de transactiekosten besparen. Het Van der Valk-concern heeft bijvoorbeeld eigen boerderijen, slachterijen en eigen transporteurs. Zij gaan zelfs zover dat ze ook een eigen bouwonderneming hebben opgezet. Op enig moment kan het dus voordeliger zijn om de rollen van anderen over te nemen. Toch hebben ook grote ondernemingen weer hun nadelen. Het in eigen beheer uitvoeren van activiteiten gaat op enig moment juist leiden tot meer in plaats van minder kosten. De kosten van coördinatie en dergelijke, de interne transactiekosten, overstijgen dan de oorspronkelijke kostenvoordelen. Er is dus een balans nodig tussen enerzijds specialisatie en generalisatie van activiteiten en anderzijds de schaalgroottevoordelen en de -nadelen.[49]

Naar analogie van de legale handel kunnen we stellen dat de illegale handel plaatsvindt in misdaadmarkten met daarin misdaadondernemingen.[50] Ook in misdaadmarkten opereren ondernemingen van uiteenlopende grootte en vanuit diverse rollen. In de cocaïnemarkt zijn zowel boeren in Colombia, laboratoria, transportondernemingen, smokkelaars, groothandelaren en straatdealers te onderscheiden.[51] In potentie kan een boer uit Colombia in een

[46] {McCarthy, 1981, 337-406}.
[47] Deze alinea is mede gebaseerd op {Naylor, 1997}, {Halstead, 1998} en {Wiebrens & Röell, 1988}.
[48] "Transaction costs are the costs arising from finding someone with whom to do business, of reaching an agreement about the price and other aspects of the exchange, and of ensuring that the terms of the agreement are fulfilled. Transaction costs are additional to, and do not include, the costs of production" {Halstead, 1998, 12}.
[49] Deze alinea is mede gebaseerd op {Naylor, 1997}, {Halstead, 1998} en {Wiebrens & Röell, 1988}.
[50] Zie bijvoorbeeld {Arlacchi, 1998}, {Van Duyne e.a., 1990}, {Van Duyne, 1995}, {Naylor, 1997, 10-13}, {Wiebrens & Röell, 1988} en {Reuter, 1984} voor deze benadering.
[51] Naylor werkt de cocaïnemarkt gedetailleerder uit {Naylor, 1997, 20}.

eigen laboratorium cocaïne produceren en verkopen aan verslaafden in Nederland. Omgekeerd kan een verslaafde bij een laboratorium in Colombia zijn cocaïne betrekken. Toch ligt dat om een aantal redenen niet voor de hand. Om de drugs van een boer uit Colombia bij de drugsverslaafden in Nederland te krijgen, zijn immers vele stappen nodig. De transactiekosten zijn daardoor hoog vanwege onder andere het leggen van contacten, de reiskosten en reistijd. Bij enige omvang is het afsluiten van transacties op individuele basis onbeheersbaar en leidt tot hoge transactiekosten. Bovendien is de onzekerheid groot. Zo weet de verslaafde niet welke kwaliteit hij krijgt en of hij niet tegen de lamp loopt. De boer in Colombia weet niet of de verslaafde te vertrouwen is. De combinatie van de hoge transactiekosten voor individuen en de onzekerheid maakt het verklaarbaar dat er behoefte bestaat aan misdaadondernemingen die zich bezighouden met de handel. Zij stroomlijnen transacties en creëren zekerheid, maken de transacties goedkoper en verkleinen de risico's voor de afzonderlijke marktpartijen.[52]

De rol van groothandel in misdaadmarkten is een aantrekkelijke. Aan de vraagzijde van de markt staat die rol ver af van de eindconsument, bijvoorbeeld de verslaafde op straat. Daar is de zichtbaarheid het grootst. Een straatdealer, die wel dicht opereert bij de verslaafde, doet zaken met vele verslaafden en is tevens lokaal gebonden. Daardoor is hij veel zichtbaarder voor de opsporingsinstanties. Bovendien liggen de drempels om straatdealer te worden niet hoog en daardoor is de concurrentie groot. Een groothandelaar doet daarentegen met minder partijen zaken en de drempels liggen hoger. Net zomin als alle legale ondernemingen in staat zijn om de potentiële schaalgroottevoordelen te benutten, geldt dat voor misdaadondernemingen. Dat is slechts voor enkelen weggelegd.[53] Aan de aanbodzijde staat de rol van groothandel ook ver af van de veelal minder aantrekkelijke en soms riskante productie. De drempel om als boer cocaïneplanten te verbouwen of voor autodieven is laag en de winstmarge daardoor gering. De handel in de uiteindelijke cocaïne of gestolen auto's is vele malen winstgevender en de drempels zijn hoger. Aan zowel de vraagzijde als aan de aanbodzijde in misdaadmarkten ontstaat als het ware een vernauwing van het aantal partijen, door sommigen aangeduid als criminaliteitspiramide (zie paragraaf 3.8). In die vernauwing is ruimte om te opereren als groothandel. Het uitgangspunt in dit proefschrift is dat georganiseerde criminaliteit die rol vervult.[54]

Op basis van genoemde redenering kunnen we de kern van georganiseerde criminaliteit preciseren. De kern is dat de plegers streven naar illegaal gewin door in één of meer misdaadmarkten op te treden als groothandel in illegale producten. Zij voeren illegale groothandelsactiviteiten uit met behulp van hun illegale groothandelsonderneming. Daarmee zijn zowel de invalshoeken van de daders, van de criminaliteit als de functie uitgewerkt.

Vanuit het vertrekpunt van de winstgerichtheid via illegale handel, misdaadmarkt en misdaadonderneming zijn we terechtgekomen bij de bedrijfsmatige benadering.[55] Deze

[52] {Halstead, 1998, 12-14}.
[53] Zie subparagraaf 4.3.3 voor een verdere onderbouwing van deze stelling.
[54] Van Duyne e.a. lijken ook uit te gaan van het uitgangspunt dat georganiseerde criminaliteit zich richt op handel op grote schaal. Vanuit financieel rechercheren komen zij uit bij bewegingen van goederen en geld op grote schaal in misdaadmarkten. Vervolgens behandelen zij georganiseerde criminaliteit in hetzelfde hoofdstuk. Waarom zij uitgaan van schaalgrootte en de relatie met georganiseerde criminaliteit maken de auteurs niet expliciet {Van Duyne e.a., 2001, 21-70}.
[55] Zie paragraaf 3.2.

hoofdstroom leent zich voor een primair economische benadering. De fundamentele aanname daarin is dat criminelen rationele actoren zijn die streven naar winstmaximalisatie. Andere aannames zijn dat er een continuüm is van legale en illegale ondernemingen en dat vele economische en bedrijfsmatige principes ook van toepassing zijn voor misdaadmarkten. De economische benadering is bruikbaar op het niveau van een individuele transactie, de onderneming, de industrie en de markt. Zij is tevens toepasbaar voor lokale en mondiale markten.[56] Binnen de economische benadering maakt men weer onderscheid tussen de invalshoek van misdaadmarkten en misdaadondernemingen.[57]

De economische benadering past op haar beurt binnen een bredere benadering waarin criminaliteit wordt bestudeerd vanuit de gedachte dat criminelen rationeel te werk gaan. Een aspect van rationeel gedrag is dat criminelen inspelen op gelegenheden (kansen) die er bestaan om criminaliteit te plegen.[58] De economische benadering van georganiseerde criminaliteit sluit daarmee aan bij de gelegenheidstheorie,[59] die eerder is geformuleerd als basis om veranderingen te identificeren. In de gelegenheidstheorie staat de criminele gebeurtenis centraal.[60] In de gekozen conceptualisering van georganiseerde criminaliteit vormen illegale groothandelsactiviteiten de criminele gebeurtenis.

De economische en bedrijfsmatige benadering hebben voor- en nadelen. Als *voordeel* geldt de rationele inslag en de bruikbare methodieken voor analyse. De nuchterheid en feitelijkheid spreken de beleidsmakers en uitvoerders doorgaans sterk aan. De benadering is breed toepasbaar en ook andere benaderingen zijn daarin onder te brengen.[61] Een ander voordeel is dat beschikbare kennis over legale organisaties kan worden gebruikt voor het bestuderen van misdaadondernemingen. Zo heeft Williams de drugshandel beschreven met behulp van een model voor industriële analyse van Porter.[62] Een *nadeel* is dat sociale relaties onvoldoende aandacht kunnen krijgen. Met name sociale relaties zijn vanwege het illegale karakter van belang.[63] Een ander nadeel is dat de verschillen tussen legale en illegale ondernemingen onder kunnen sneeuwen. Aan zowel de betekenis van sociale relaties als de verschillen tussen legale en illegale ondernemingen wordt in het vervolg van dit hoofdstuk nog de nodige aandacht besteed.

Een kritiekpunt op de bedrijfsmatige benadering is dat te veel criminele groepen/ misdaadondernemingen onder het begrip georganiseerde criminaliteit komen te vallen. Vanwege de geladenheid van dit begrip vinden sommigen dat ongewenst.[64] Deze kritiek is in dit proefschrift ondervangen door alleen misdaadondernemingen die de rol van groothandel op zich nemen te rekenen tot georganiseerde criminaliteit.[65] Die rol stelt relatief hoge eisen aan de misdaadonderneming en lang niet allen kunnen of willen daaraan voldoen (zie paragraaf 4.3). Bovendien is niet in alle misdaadmarkten op basis van de aard

[56] {Halstead, 1998, 9-10}. In {Smith, 1994} zijn diverse economische benaderingen toegepast op georganiseerde criminaliteit. Wiebrens en Röell gaan eveneens in op de economische en bedrijfsmatige benadering {Wiebrens & Röell, 1988}.
[57] Zie bijvoorbeeld {Williams & Godson, 2002, 322-328}.
[58] {Van Dijk e.a., 1996}.
[59] {Clarke & Felson, 1993}
[60] Zie paragraaf 1.2.2.
[61] {Klerks, 2000, 83}, {Smith, 1994, 130-131}.
[62] {Williams, 1995}.
[63] {Klerks, 2000, 83}, {Kleemans e.a., 1999, 34}.
[64] Dat is bijvoorbeeld het standpunt geweest van de onderzoeksgroep Fijnaut (zie paragraaf 3.4).
[65] Zie paragraaf 3.7 voor een definitie van een illegale groothandelsonderneming en van de rol van de groothandel.

van de producten ruimte voor illegale groothandelsactiviteiten (zie paragraaf 4.2). Daardoor is ook het aantal misdaadmarkten waarin georganiseerde criminaliteit voorkomt, begrensd.

Er is kritiek op illegale handel als kernelement van georganiseerde criminaliteit. Paoli is van mening dat de illegale handel eerder ongeorganiseerd dan georganiseerd verloopt en dat het daarom niet past bij het begrip georganiseerde criminaliteit.[66] Ten opzichte van de legale handel heeft ze gelijk voor wat betreft het ongeorganiseerde karakter. Haar betoog is echter gebaseerd op de impliciete aanname dat georganiseerd inhoudt dat er grote misdaadondernemingen bestaan. Ten opzichte van legale markten kenmerken misdaadmarkten zich eerder door vele en relatief kleine partijen (zie subparagraaf 3.6.4). Dit laat onverlet dat binnen misdaadmarkten niet alle partijen een gelijke omvang hebben en beschikken over dezelfde bekwaamheden en middelen.

Verder stelt Paoli dat juist de organisaties die traditioneel worden gerekend tot georganiseerde criminaliteit, de maffia-achtige organisaties, zich *niet alleen* met de handel bezighouden. Zij verrichten bijvoorbeeld soms ook politieke functies. Zij gaat, net als Bovenkerk, in op de regulerende rol van de maffia en de overname van enkele functies van de overheid. Het gebruik van rituelen om trouw af te dwingen en de (dreiging met) geweld zijn daarbij essentieel. Dit heeft grote voordelen voor het opereren in misdaadmarkten. Toch geeft zij aan dat de maffia-achtige organisaties zijn ontstaan los van de dynamiek van misdaadmarkten. Deze organisaties bestonden al ruim voordat bijvoorbeeld de drugsmarkt opkwam. Toch hebben zij in de relatief nieuwe misdaadmarkten van de wapenhandel en mensensmokkel deels de boot gemist. Verder merkt zij op dat soms ook legale organisaties zich bezighouden met de handel in illegale producten. Bovendien slagen misdaadondernemingen die zich richten op de handel in illegale producten er nauwelijks in om uit te groeien tot organisaties die kunnen profiteren van schaalgrootte. Omgekeerd houden de misdaadondernemingen die wel een zekere schaalgrootte hebben gerealiseerd, zich niet alleen bezig met de handel. Ze vervullen namelijk ook andere functies en ze bestonden al voordat de moderne misdaadmarkten opkwamen. Zij concludeert daarom dat de concepten van illegale handel en georganiseerde criminaliteit apart moeten worden gehouden.[67]

Ondanks deze kritiek van Paoli wordt toch uitgegaan van illegale groothandelsactiviteiten als kern van georganiseerde criminaliteit. Op basis van bovenstaande keuzen is grotendeels al kleur bekend in de hoofdstromen zoals Klerks die heeft geïdentificeerd. Het accent ligt op de bedrijfsmatige benadering. Toch is er op grond van de beperkingen van de illegaliteit eigenlijk maar één mogelijkheid om handel te bedrijven, namelijk in netwerken (zie subparagraaf 3.6.4 en 4.3.3). De inzichten vanuit de structureel-functionalistische benadering worden dus zeker meegenomen. Het accent ligt echter daarbij niet op de netwerken op zich, maar op de functie die ze vervullen voor illegale groothandelsondernemingen en in misdaadmarkten.

Laten we vanuit bovenstaande beschouwingen nog eens kijken naar de definitie van de onderzoeksgroep Fijnaut, alvorens te komen met een eigen definitie. Het eerste onderdeel in de definitie van de onderzoeksgroep heeft betrekking op groepen die primair zijn gericht op illegaal gewin. Dit is hier verbijzonderd tot illegale groothandelsondernemingen.

[66] {Paoli, 2002}.
[67] {Paoli, 2002}.

Tussen deze vindt handel plaats, samenwerking om handel te kunnen drijven, maar soms ook concurrentie en strijd. Net als de onderzoeksgroep zijn politiek geïnspireerde misdrijven en organisatiecriminaliteit uitgesloten (zie verder paragraaf 3.7). Niet iedereen beschikt over de bekwaamheden en middelen om illegale groothandelsactiviteiten uit te voeren. De misdaadondernemer moet in staat zijn een bedrijfsvoering op te zetten en handel te drijven in een misdaadmarkt. Dit stelt eisen aan de persoonlijke bekwaamheden van de misdaadondernemer. Bovendien moeten de noodzakelijke financiële, materiële en personele middelen beschikbaar zijn.[68] Volgens de onderzoeksgroep Fijnaut moeten de plegers bereid en in staat zijn verder te gaan dan andere misdrijfplegers als het gaat om het verdedigen van de positie.[69] In dit proefschrift is een ander accent gelegd. Zij moeten de intentie hebben om winst te maken en zij moeten kunnen beschikken over de bekwaamheden en middelen om te opereren als groothandel.

Het tweede onderdeel in de definitie van de onderzoeksgroep heeft betrekking op groepen die systematisch misdrijven plegen met ernstige gevolgen voor de samenleving. Met het concept misdaadonderneming en de rol van groothandel is het element 'systematisch misdrijven plegen' afgedekt (zie paragraaf 3.8). Beide omvatten immers een zekere regelmaat in activiteiten en planmatig opereren. Ten opzichte van de definitie van de onderzoeksgroep geldt wel als beperking dat het moet gaan om de handel in illegale producten. Ontvoeringen en bankovervallen vallen hierdoor, in tegenstelling tot bij de onderzoeksgroep, niet onder georganiseerde criminaliteit. De illegale groothandelsactiviteiten resulteren in uiteenlopende ernstige gevolgen voor de samenleving. Het aspect 'ernstige gevolgen voor de samenleving' ligt dus besloten in de rol van de groothandel. Het hoeft daarom niet expliciet te worden benoemd in de definitie. Wat dan die ernstige gevolgen zijn, verder aangeduid als ongewenste effecten, komt aan bod in paragraaf 4.8.

Het derde onderdeel van de definitie van de onderzoeksgroep betreft de afscherming van de groep en activiteiten. Dit onderdeel vloeit logisch voort uit de keuze van de onderzoeksgroep dat de opstelling van de plegers onderscheidend is voor georganiseerde criminaliteit. In dit proefschrift ligt daarentegen, in de lijn van de gelegenheidstheorie, het accent op de criminele gebeurtenis: illegale groothandelsactiviteiten. Zoals eerder is aangegeven, is het omstreden in hoeverre afscherming een discriminerend kenmerk is van georganiseerde criminaliteit. Bepaalde vormen van afscherming, zoals het gebruik van codetaal, zijn in elk geval randvoorwaardelijk voor de illegale handel, ongeacht of het nu wel of niet gaat om georganiseerde criminaliteit. Als gevolg van de illegaliteit opereren misdaadondernemingen in een vijandige omgeving. Bovendien is een misdaadmarkt niet gereguleerd door de overheid, door wet- en regelgeving en rechters (zie subparagraaf 3.6.4). Voorzichtigheid is dus geboden in een dergelijke omgeving en doordat overeenkomsten geen juridische basis hebben, kan (de dreiging met) geweld onontkoombaar zijn. Zonder een zekere mate van afscherming, waaronder de dreiging met geweld, kan daarom geen enkele crimineel. Haller merkt op dat iemand met een gewelddadige reputatie daarentegen minder kans maakt om deel te nemen aan criminele samenwerkingsverbanden. De geweldsreputatie staat dat in de weg.[70] Deze defensieve vormen van afscherming zijn dus wel een noodzakelijke, maar geen voldoende voorwaarde om te kunnen spreken van georganiseerde criminaliteit en zijn ook niet uniek daarvoor. Het gebruik van de door

[68] Zie bijvoorbeeld {Bovenkerk, 2001, 41-79}, {NCIS, 2002} en subparagraaf 4.3.3.
[69] {Enquêtecommissie, 1996B, 23-24}.
[70] {Van Duyne e.a., 1990}, {Klerks, 2000}, {Haller, 1990, 222}.

sommigen specifiek geachte vormen van afscherming, offensieve contrastrategieën en corruptie, is evenmin altijd noodzakelijk of uniek. Het gebruik ervan is noch een noodzakelijke, noch een voldoende voorwaarde om te kunnen spreken van georganiseerde criminaliteit. Dat desondanks corruptie en geweld vaak worden genoemd als discriminerende kenmerken, heeft te maken met afpersing of machtsuitoefening in een geografisch afgeschermd gebied. Hiervoor is corruptie wel nodig omdat de reputatie van de afperser of machtsbeoefenaar bekend moet zijn en daarvoor extra afscherming onontkoombaar is. Afpersing en de uitoefening van macht zijn in dit proefschrift níét beschouwd als een vorm van illegale handel en vallen daardoor buiten het begrip.

De onderzoeksgroep Fijnaut heeft later aangegeven dat zij verweving van legale en illegale activiteiten, ook wel aangeduid als innesteling, rekent onder afscherming. Verweving is veelal instrumenteel voor een illegale groothandelsonderneming. Bijvoorbeeld smokkelaars van grote volumineuze partijen drugs kunnen eigenlijk niet buiten een legale transportonderneming wanneer zij grensoverschrijdende bewegingen maken. Zonder dat neemt het risico om bij de grens tegengehouden te worden toe. Verweving is dus veelal wel een noodzakelijke voorwaarde. Maar, is het ook een voldoende voorwaarde voor georganiseerde criminaliteit? Het is in elk geval kenmerkend ten opzichte van bepaalde andere vormen van criminaliteit, zoals overvallen, ontvoeringen en dergelijke. Toch is verweving niet uniek. Voor een eenmalige oplichting en organisatiecriminaliteit is dat eveneens onontkoombaar. Verweving is dus geen voldoende voorwaarde en maakt daarom geen onderdeel uit van de definitie. Het is veelal wel een noodzakelijk instrument voor illegale groothandelsactiviteiten (zie paragraaf 3.8 en 4.3.3).

Continuïteit van de misdaadonderneming en van de bedrijfsvoering komen niet voor in de definitie van de onderzoeksgroep Fijnaut, maar verdient wel de aandacht. De drijfveer achter georganiseerde criminaliteit is dan wel het streven naar illegale winst, maar dit moet wel in verhouding staan tot de risico's.[71] Dat zoeken van een balans tussen winst en risico heeft te maken met het streven naar continuïteit. Hierin schuilt natuurlijk ook een persoonlijk belang voor de misdaadondernemer. Hij wil immers niet in de gevangenis belanden en hij wil niet dat de overheid zijn vermogen afneemt. Toch houden ook andere criminelen rekening met risico's. Voor een groothandel komt er nog wel een element bij. In tegenstelling tot een groep criminelen die zo af en toe een overval pleegt, is continuïteit nodig. De misdaadonderneming moet het verdiende geld bijvoorbeeld deels investeren in handelswaar, transportmiddelen, rechtspersonen en dergelijke. Zij moet voortdurend werken aan het beheer van de criminele relaties door goede waar te leveren. Het belang van continuïteit neemt weliswaar toe naarmate de handel in omvang toeneemt, maar geldt überhaupt voor handel. Het streven naar continuïteit is dus wel een noodzakelijke, maar geen voldoende voorwaarde om te kunnen spreken van georganiseerde criminaliteit. Daarom is continuïteit niet opgenomen in de definitie. Bovendien is dit ingesloten in de begrippen illegale groothandelsactiviteiten en illegale groothandelsonderneming.

Op basis van bovenstaand betoog luidt de definitie:

> *Georganiseerde criminaliteit is het uitvoeren van illegale groothandelsactiviteiten in één of meer misdaadmarkten door een illegale groothandelsonderneming.*

[71] Zie subparagraaf 4.3.2.

De volgende paragrafen werken de sleutelbegrippen misdaadmarkt, illegale groothandelsonderneming en illegale groothandelsactiviteiten uit.

3.6. Misdaadmarkt

3.6.1. Inleiding

Als eerste komt het begrip misdaadmarkt aan bod. Vervolgens vindt een uitwerking plaats van producten waarvoor een misdaadmarkt bestaat en daarmee van soorten misdaadmarkten. Tot slot gaat deze paragraaf ook in op enkele kenmerken van die markten.

3.6.2. Begrip misdaadmarkt

In een markt komen voortdurend vraag naar en aanbod van producten bij elkaar. De aanbiedende en vragende partijen onderhandelen over de prijs en voorwaarden waaronder de uitwisseling van producten kan plaatsvinden. Nadat de transactie is gesloten, wisselen de goederen van eigenaar of levert de aanbieder de afgesproken diensten. In sommige gevallen is een markt plaatsgebonden. Een voorbeeld daarvan is de veemarkt in Utrecht, waar handelaren en vee samenkomen en het vee van eigenaar verwisselt. Dit duidt men ook wel aan met het begrip 'marktplaats'. Overigens is niet aannemelijk dat de goederen op dezelfde locatie fysiek van eigenaar wisselen in het geval van een groothandel. In andere gevallen is sprake van een ruimere en niet plaatsgebonden betekenis van een markt. Een voorbeeld daarvan is de markt voor pc's. De producenten bieden de pc's aan via uiteenlopende distributiekanalen. De producenten en consumenten komen niet fysiek samen en de koop kan niet alleen worden beklonken in winkels, maar ook via de telefoon of het internet. Markten zijn op uiteenlopende wijzen te typeren en te ordenen. Veelal is duidelijk om welk product het gaat, zoals vee of pc's. Soms onderscheidt men geografisch afgebakende markten, zoals de Nederlandse, Europese of mondiale markt. In andere gevallen verbijzondert men markten naar doelgroepen, zoals de jongerenmarkt of de ouderenmarkt.[72]

Wanneer sprake is van illegale producten dan spreken we van een misdaadmarkt. Hoewel de toevoeging illegaal eenduidig lijkt, is toch een verbijzondering nodig. De toevoeging is duidelijk wanneer de wetgever het product zelf verboden of strikt gereguleerd heeft. Dit is het geval bij bijvoorbeeld kinderporno-afbeeldingen en drugs. Zowel de productie, verkoop als het bezit zijn strafbaar. Arlacchi spreekt alleen bij deze producten over een misdaadmarkt: "Illegal markets may be defined as those places within which goods and services are exchanged whose production, sale and consumption are forbidden or strictly regulated by the majority of national states and/ or by international legislation".[73] Als gevolg van de laatste toevoeging ontstaat onduidelijkheid. Zijn bijvoorbeeld vuurwapens en kinderporno strafbaar gesteld of streng gereguleerd in de meerderheid van staten of via internationale wetgeving? Een nader onderzoek is nodig om hierover uitsluitsel te kunnen geven. Daarom is dit onderdeel van zijn definitie problematisch.

[72] Zie bijvoorbeeld {Lipsey & Steiner, 1981, 950} en {McCarthy, 1981, 746} voor een verdere toelichting.
[73] {Arlacchi, 1998, 203}. Williams hanteert deze definitie met een kleine wijziging {Williams & Godson, 2002, 322}.

Lastiger is het wanneer het product zelf legaal is, maar onderdelen van het productieproces illegaal zijn. Productieproces moet in dit kader overigens ruim worden opgevat. Voorbeelden daarvan zijn diefstal van auto's, illegaal kopiëren van cd's, oplichting, ontduiking van accijnzen voor sigaretten, het vetmesten van koeien met groeihormonen en illegale dumping van chemisch afval. Bij dergelijke producten speelt de vraag of wel sprake is van een *misdaad*markt. Het gaat immers om legale producten, waarvoor een legale markt bestaat. Deze handel valt in elk geval niet onder het begrip misdaadmarkt van Arlacchi. Hij geeft immers als beperking aan dat de productie, verkoop en consumptie verboden of gereguleerd moeten zijn. Dat is bij legale producten zoals hierboven genoemd niet (volledig) het geval. Anderen rekenen deze handel wel degelijk onder het begrip misdaadmarkt, hoewel voor die producten ook legale markten bestaan.[74] Dit proefschrift hanteert eveneens die benadering en beschouwt ook dit type producten als een illegaal product.

Op basis van bovenstaande argumenten luidt de definitie van een misdaadmarkt:

> *Een misdaadmarkt is een ruimte waarin voortdurend vraag naar en aanbod van illegale producten bij elkaar komen.*

Diverse auteurs hanteren (impliciet) uiteenlopende indelingen voor illegale producten en misdaadmarkten in relatie tot georganiseerde criminaliteit. Kleemans e.a. stellen dat georganiseerde criminaliteit een product levert die bonafide bedrijven in het geheel niet of tegen hogere kosten produceren of leveren.[75] De reden dat bonafide bedrijven die producten niet produceren of leveren is dat het product op zich zelf en/of onderdelen van het productieproces strafbaar of strikt gereguleerd zijn. Het kan ook gaan om producten die de misdaadonderneming tegen dezelfde prijs levert als bonafide bedrijven. In dat geval maakt zij minder kosten of meer winst door de wet- en regelgeving te overtreden of anderen op te lichten. De definitie van een illegaal product luidt derhalve:

> *Een illegaal product is een product dat bonafide bedrijven in het geheel niet, tegen hogere kosten of lagere winstmarge produceren of leveren doordat het product op zich zelf en/of onderdelen van het productieproces a) strafbaar zijn of b) strikt gereguleerd zijn en er sprake is van overtreding van die regulerende wet- of regelgeving.*

3.6.3. Soorten misdaadmarkten

Een misdaadonderneming kan verdienen aan producten die bonafide bedrijven in het geheel niet leveren, maar waar wel vraag naar bestaat. Het gaat daarbij in de *eerste* plaats om producten die op zich zelf zijn verboden, zoals drugs en kinderporno-afbeeldingen. Een *tweede* variant zijn streng gereguleerde producten die niet voor iedere behoeftige op legale wijze toegankelijk zijn. Voorbeelden zijn vuurwapens en specifieke medicijnen. Een *derde* vorm betreft goederen die uniek of zeer schaars zijn waardoor niet iedere behoeftige er op legale wijze aan kan komen. Door diefstal kan een misdaadonderneming een dergelijk goed aanbieden. Een voorbeeld daarvan is een schilderij van Rembrandt. Een *vierde* variant betreft falsificaten, zoals van identiteitsdocumenten of bankbiljetten. Een *vijfde* optie is ondersteunende dienstverlening door criminelen aan misdaadondernemingen, zoals

[74] {Van Duyne e.a., 2001}, {Williams & Godson, 2002, 322}.
[75] {Kleemans e.a., 2002, 66}. Zij werken dit onderscheid overigens niet verder uit.

het uitvoeren van een liquidatie of het vervalsen van paspoorten. Deze dienstverlening heeft veelal het karakter van het uitvoeren van klussen. De activiteiten die direct gerelateerd zijn aan de handel, vallen daarentegen onder de (primaire) misdaadmarkten. De diefstal van auto's en de levering ervan aan de heler hebben direct te maken met de handel in gestolen auto's. Daardoor maken ze onderdeel uit van de primaire misdaadmarkt, in dit geval de markt van gestolen goederen. Een *zesde* vorm betreft dienstverlening door legale bedrijven aan een misdaadonderneming. Daarbij moet op zijn minst sprake zijn van bewuste betrokkenheid (zie subparagraaf 4.3.3). Voorbeelden daarvan zijn ondersteuning voor het witwassen en het vervoer van smokkelwaar door een legale transportonderneming. Het gaat hier om legale dienstverlening door legale ondernemingen voor illegale doeleinden waarbij de dienstverlener op de hoogte is van zijn rol.[76]

Andere producten kunnen bonafide bedrijven wel degelijk produceren of leveren, maar dan wel tegen een hogere prijs of een kleinere winstmarge. Het gaat om legale producten die op zichzelf niet zijn verboden. Een *eerste* variant zijn producten waar de crimineel tijdens het productieproces marktregulerende wet- en regelgeving overtreedt. In de kern gaat het hier om fraude met fiscale en sociale wetgeving, overtreding van milieuwetgeving of misbruik van subsidieregelingen. Voorbeelden zijn sigarettensmokkel of illegale lozing van chemisch afval. Een *tweede* variant om goedkoper producten te leveren, is het (laten) stelen ervan. Een voorbeeld zijn auto's. Een *derde* variant is het leveren van valse of vervalste producten of producten van mindere kwaliteit. In sommige gevallen weet de afnemer dat het gaat om een vervalsing, bijvoorbeeld bij een illegaal gekopieerde cd. In andere gevallen weet de afnemer dat niet, bijvoorbeeld bij merkenpiraterij van kleding of vlees van met hormonen behandelde koeien. Een *vierde* variant is het inspelen op hebzucht. Een voorbeeld daarvan is het verkopen van land op de maan aan mensen die daarvan rijk denken te worden. Tot slot is het ook mogelijk om te suggereren dat goederen worden geleverd tegen een lagere prijs, maar deze worden feitelijk nooit geleverd. Dit is een vorm van oplichting.

De soorten producten overlappen elkaar gedeeltelijk. Toch verschillen zij op enkele belangrijke kenmerken ten aanzien van de vraag, het aanbod, de aard, de bijbehorende criminele activiteiten, de winstverwachting, het risico, de benodigde bedrijfsvoering en de mate van verweving tussen illegale en legale activiteiten. Zo kunnen de vuurwapenhandelaren de vuurwapens betrekken van zowel dieven en helers als van de legale wapenhandelaren. In het laatste geval moet de misdaadonderneming de bovenwereld betreden, hetgeen extra risico's met zich meebrengt.

In figuur 3.2 zijn de afzonderlijke producten gecategoriseerd en zijn de hoofdsoorten misdaadmarkten van een naam voorzien. De daarin genoemde illegale producten zijn primair afgeleid van de typen criminaliteit die men rekent tot georganiseerde criminaliteit.[77] De genoemde typen zijn, voorzover van toepassing, vertaald naar één van de hiervoor genoemde soorten illegale producten. De lijst is niet limitatief. Paragraaf 4.2 formuleert factoren die van invloed zijn op de mate van aantrekkelijkheid van een product voor de illegale groothandel.

[76] Van Duyne e.a. spreken bij de vijfde en zesde variant over de Criminele dienstenmarkt. Deze misdaadmarkt splitsen zij in de 'eigen dienstenmarkt' en de 'dienstverleningsmarkt van de bovenwereld'{Van Duyne e.a., 1990, 15-18}.

[77] Gebaseerd op {Van Duyne e.a., 1990, 80}, {Van Duyne, 1995, 98, 132}, {Van Duyne e.a., 2001}, {De Vette e.a., 1999}, {Kleemans e.a., 2002} en {Enquêtecommissie, 1999B}.

Categorieën illegale producten/ misdaadmarkten	Subcategorieën
1. Verboden producten (misdaadmarkt van verboden producten)	1A Drugs: 1) cannabis, 2) heroïne, 3) cocaïne en 4) synthetische drugs 1B Kinderpornomateriaal 1C Mensenhandel 1D Uitheemse dieren en planten, waaronder eieren van zeldzame vogels, of daarvan afgeleide medicijnen
2. Streng gereguleerde producten (misdaadmarkt van gereguleerde producten)	2A Wapens, waaronder vuurwapens, oorlogsmateriaal en nucleair materiaal 2B Illegaal vuurwerk 2C Illegaal gokken 2D Mensensmokkel 2E Uitheemse dieren en planten, waaronder eieren van zeldzame vogels, of daarvan afgeleide medicijnen
3. Unieke en schaarse producten (misdaadmarkt van unieke en schaarse producten)	3A Specifieke kunstvoorwerpen 3B Menselijke organen
4. Falsificaten (misdaadmarkt van falsificaten)	Voorbeelden zijn valse identiteitsdocumenten en betaalmiddelen
5. Dienstverlening aan criminelen door criminelen (criminele dienstenmarkt)[78]	Vele mogelijkheden, waaronder uitvoeren liquidaties en geld wisselen
6. Dienstverlening aan criminelen door (medewerkers van) legale bedrijven (criminele dienstverleningsmarkt van de bovenwereld)[79]	Voorbeelden zijn het helpen bij witwassen of juridische constructies
7. Producten waarbij marktregulerende wet- en regelgeving is overtreden (misdaadmarkt van marktreguleringfraude)	7A Goederen met een (fiscale) prijswig (bijvoorbeeld vlees of sigaretten, consumentenelektronica en minerale olie) 7B Afval (illegale afvalmarkt)
8. Gestolen goederen (misdaadmarkt van gestolen goederen)	Voorbeelden zijn wapens, (vracht)auto's of creditcards
9. Vervalste of gemanipuleerde goederen (misdaadmarkt van vervalste goederen)	9A Vervalste goederen waarbij inbreuk is gemaakt op intellectuele eigendomsrechten of het merkrecht (bijvoorbeeld illegale cd's, merkenpiraterij) 9B Gemanipuleerde goederen, zoals vlees afkomstig van koeien met groeihormonen
10. Hebzuchtproducten (hebzuchtmarkt)	Er bestaan vele mogelijkheden, zoals het verkopen van land op de maan, niet-bestaande landerijen of beleggingsvormen
11. Overige producten waarbij sprake is van oplichting (oplichtingsmarkt)	Er bestaan daarvoor vele mogelijkheden, zoals het niet-leveren van betaalde goederen

Figuur 3.2 Soorten misdaadmarkten en illegale producten (niet limitatief)

3.6.4. Kenmerken misdaadmarkten

Tussen legale en misdaadmarkten bestaan belangrijke overeenkomsten. Zo zijn er vragende en aanbiedende partijen. Deze partijen moeten elkaar weten te vinden en er komt een prijs tot stand. Er bestaan ook belangrijke verschillen. Het belangrijkste verschil is

[78] Naam is ontleend aan {Van Duyne e.a., 1990, 15-18}.
[79] Idem.

uiteraard het illegale karakter (van de wijze van totstandkoming) van de aangeboden producten.

Als gevolg van het illegale karakter is de omgeving voor een misdaadonderneming vijandig. Een belangrijke vijand vormt de overheid. Overheidsingrijpen kan immers leiden tot: ontneming van het gewin, vrijheidsstraf, inbeslagname van goederen en verstoring van de bedrijfsvoering. Maar er zijn meer vijanden. Medewerkers van legale bedrijven waarop de misdaadonderneming een beroep moet doen, bijvoorbeeld een notaris of een bankemployee, kunnen aangifte doen bij de politie. Ook collega-criminelen kunnen een vijandige houding aannemen. Meningsverschillen of fouten kunnen resulteren in geweld tegen de misdaadondernemer en zijn geliefden. Collega-criminelen kunnen overgaan tot beroving van de handelswaar of verraad plegen. Vanwege die vijandigheid zijn geheimhouding en vermijding van bewijssporen cruciaal. Geheimhouding is nodig om de overheid, de samenleving en de collega-criminelen in het ongewisse te laten over de criminele activiteiten. Zo moeten bij smokkel de illegale goederen onopgemerkt blijven en moeten zo weinig mogelijk mensen ervan op de hoogte zijn. Doordat de criminele activiteiten lang niet altijd geheim (kunnen) blijven, moet de misdaadonderneming in elk geval strafrechtelijke en fiscale bewijssporen vermijden. Dit betekent dat de relatie tussen het delict en de misdaadondernemer, de werknemers en de partners niet te bewijzen moet zijn. Toch doet iedere illegale transactie afbreuk aan de noodzakelijke geheimhouding en kan resulteren in bewijssporen en daardoor het einde betekenen van de misdaadonderneming. De leveranciers, de afnemers, de medewerkers en andere betrokkenen zijn immers op de hoogte van de transactie. Zij kunnen dit doorgeven aan opsporingsinstanties.[80]

Een ander gevolg van het illegale karakter is dat misdaadmarkten zich kenmerken door ongereguleerdheid. Wet- en regelgeving ontbreekt. Er is geen formele instantie die zorgt voor marktregulering en zekerheid kan bieden over de naleving van overeenkomsten. Bij geschillen met de eigen medewerkers, klanten of leveranciers kan de misdaadonderneming geen beroep doen op de rechter. Er bestaat geen instantie die marktgegevens bijhoudt of waar bekend is wie zich waarmee bezighoudt. Er zijn evenmin gegevens bekend over consumenten. Prijsvergelijking is niet mogelijk. Er ontbreekt een overzicht van vraag en aanbod. De misdaadondernemingen verstrekken bij voorkeur geen informatie en adverteren is er niet bij. Misdaadmarkten zijn dus niet transparant. Er kunnen bovendien sterke fluctuaties optreden in de kwaliteit van de geleverde waar en in de beschikbaarheid. Marktpartijen kunnen van de ene op de andere dag verdwijnen. Er is dus geen sprake van een perfecte marktwerking.[81]

Vertrouwen speelt in misdaadmarkten een sleutelrol. Dit als gevolg van het vijandige en het ongereguleerde karakter. Het uitvoeren van klussen of het zakendoen met onbekenden ligt daarom niet voor de hand. Verraad, bedrog of geweldsgebruik kan het gevolg zijn. De misdaadonderneming valt daarom veelal terug op de familie- of sociale relaties om de risico's te beperken (zie verderop). Desondanks zijn opportunisme of meningsverschillen zeer wel mogelijk en kunnen bedrijfsongevallen zoals de inbeslagname van een grote partij drugs, het vertrouwen weer tenietdoen. Er kan dan geen beroep op een formele instantie worden gedaan. De dreiging met geweld vormt dan een voor de hand liggende sanctie-

[80] Ontleend aan {Van Duyne e.a., 1990}, {Klerks, 2000}, {Arlacchi, 1998}, {Reuter, 1984}, {Mastrofski & Potter, 1987}, {Paoli, 2002}, {Naylor, 1997}, {Wiebrens & Röell, 1988}.
[81] Idem.

mogelijkheid of instrument voor geschillenbeslechting.[82] Geweld is echter een inefficiënt middel. Het trekt de aandacht van de overheid of leidt tot haat en nijd waardoor het gevaar van verraad op de loer ligt. De aanwezigheid van geweld is daarom een teken van problemen in de misdaadmarkt en/of van een slechte bedrijfsvoering.[83]

Kortom, het vijandige en ongereguleerde karakter van misdaadmarkten leidt tot spanningsvelden. Bij elke illegale transactie bestaat een spanningsveld tussen enerzijds het zakendoen en anderzijds het zorgen voor geheimhouding en het vermijden van bewijssporen. Verder is in iedere illegale transactie een spanningsveld aanwezig tussen vertrouwen en geweld.[84] De misdaadonderneming moet verder zowel zonder als tegen de overheid opereren.[85]

De genoemde spanningsvelden hebben enkele effecten. Allereerst ontstaan er drie knelpunten. Betrouwbaar personeel, beheersing van informatie en geldbeheer zijn van groot belang, maar veel lastiger in te vullen dan bij legale ondernemingen (zie verder subparagraaf 4.3.3).[86] Een ander effect is dat de kosten hoger zijn dan bij vergelijkbare legale ondernemingen. Zo zijn de transactiekosten hoger, omdat de misdaadonderneming niet met iedereen zaken kan doen en de partners zorgvuldig moet uitkiezen. Ook de bedrijfsvoering brengt extra kosten met zich mee door bijvoorbeeld het omkopen van personen en het inhuren van lijfwachten. Daarbovenop zijn extra kosten nodig als een vorm van risicopremie. Het opereren in de illegaliteit brengt immers risico's met zich mee van arrestatie, inbeslagname van geld en goederen door de overheid en diefstal of bedrog door andere criminelen. Ondanks extra kosten en risico's behalen plegers van georganiseerde criminaliteit volgens de meeste onderzoekers grote winsten.[87] Van Duyne en Naylor betwijfelen echter of zij inderdaad wel zoveel geld verdienen. Tussen de winstberekeningen die dienen als bewijsvoering voor het ontnemen van crimineel verdiende gelden en de feitelijk getraceerde gelden, komen grote verschillen voor. Bovendien blijkt regelmatig dat een misdaadondernemer in de financiële problemen komt bij een tegenslag zoals de inbeslagname van een partij drugs.[88]

Het vijandige en ongereguleerde karakter van misdaadmarkten resulteert ook in beperkingen voor de consument. Hij heeft eveneens te maken met een vijandige omgeving. In principe moeten zowel de overheid, opsporingsinstanties als de samenleving in het ongewisse blijven van de koop van illegale producten. De mate van illegaliteit, gedogen en sociale acceptatie kunnen overigens sterk verschillen. Het bezit en de aanschaf van kinderporno-afbeeldingen zijn strafbaar. De overheid gedoogt kinderporno-afbeeldingen niet en het bezit ervan is bovendien niet sociaal geaccepteerd. Een consument moet daarom zeer voorzichtig opereren. Dit in tegenstelling tot het bezit en de aanschaf van bijvoorbeeld een illegaal gekopieerde muziek-cd. Misdaadondernemingen maken geen reclame voor hun producten. Er bestaan geen winkels waar de consumenten terechtkunnen. Prijsvergelijking is niet mogelijk. Er kunnen sterke fluctuaties optreden in de kwaliteit van de

[82] {Van Duyne e.a., 1990}, {Klerks, 2000}, {Arlacchi, 1998, 207-212}, {Halstead, 1998, 19-20}, {Reuter, 1984}.
[83] {Van Duyne e.a., 1990}, {Van Duyne, 1995}, {Arlacchi, 1998}, {Reuter, 1984, 130}.
[84] {Arlacchi, 1998, 207-212}.
[85] {Paoli, 2002, 64-67}.
[86] De eerste twee van de genoemde knelpunten zijn gebaseerd op {Van Duyne, 1995}.
[87] {Enquêtecommissie, 1996B, 123}, {Kleemans e.a., 2002}. Arlacchi bespreekt het aspect van de hogere transactiekosten {Arlacchi, 1998}.
[88] {Van Duyne, 1995, 166-171}, {Enquêtecommissie, 1996C}, {Naylor, 1997}.

geleverde waar en in de beschikbaarheid. De leverancier kan van de ene op de andere dag verdwijnen. Misdaadmarkten zijn dus ook voor consumenten niet transparant en de macht van consumenten is daardoor beperkt.[89] Ook tussen consument en misdaadonderneming moet een basis van vertrouwen bestaan. Het overeenkomstenrecht is niet van toepassing en bij een geschil kan men geen rechter of consumentenbond inschakelen.

De genoemde spanningsvelden, knelpunten en andere kenmerken van misdaadmarkten vormen samen een hindernis voor het uitvoeren van activiteiten in de eigen misdaadonderneming en dus voor schaalgrootte. Net als bij legale ondernemingen wegen de voordelen op enig moment niet meer op tegen de nadelen. Dat moment is eerder bereikt dan bij legale ondernemingen. Bij een grote omvang gaan de beperkingen van de illegaliteit steeds meer knellen en neemt bovendien het risico van ontdekking toe. Zo vormen veel medewerkers, afnemers en leveranciers een risicofactor, niet alleen voor de misdaadonderneming zelf, maar ook voor de zakenpartners en de medewerkers. Bovendien leidt het zakendoen met vele partijen tot extra complexiteit waarbij de genoemde knelpunten extra naar voren komen. De illegaliteit beperkt bovendien het zakendoen over grote afstanden. Daardoor daalt het aantal potentiële marktpartijen waarmee de onderneming zaken kan doen. Marketing is niet mogelijk. Expansie van de activiteiten moet komen uit de verdiende gelden, omdat de misdaadondernemer geen beroep kan doen op externe financiers. Wanneer de baas stopt of is gearresteerd, houdt de onderneming veelal op te bestaan. De misdaadonderneming kan niet aan anderen worden verkocht met goodwill. Op latere leeftijd investeren in de onderneming is daarom niet aantrekkelijk. Daardoor zijn misdaadondernemingen minder omvangrijk dan vergelijkbare legale ondernemingen. Daaruit vloeit logischerwijze voort dat misdaadmarkten ten opzichte van legale markten meer marktschijven kennen om een product bij de eindconsument te krijgen (zie ook paragraaf 3.7).[90]

Menig misdaadmarkt, en wellicht zelfs élke misdaadmarkt, heeft een internationaal karakter. Producten zoals cocaïne en heroïne worden slechts in een beperkt aantal landen geproduceerd, terwijl de vraag een mondiaal karakter heeft. Mensenhandel en -smokkel zijn vormen van dienstverlening met een internationaal karakter. De dienstverlening bestaat uit het helpen van veelal arme mensen om naar rijke landen te komen.

Hoe vinden nu de misdaadondernemingen binnen de geschetste context leveranciers en afnemers waarmee ze handel kunnen drijven, alsmede ondersteuners en medewerkers? Eigenlijk is er maar één mogelijkheid, namelijk via netwerken. Volgens Paoli zijn de meest stabiele ondernemingen niet gebaseerd op economische relaties, maar op solidariteitsrelaties, zoals bloedverwantschap. Alleen dan kunnen de beperkingen van de illegaliteit worden geneutraliseerd.[91] Sociale relaties hebben immers een groot voordeel. De deelnemers zijn loyaal aan elkaar en opportunisme maakt minder kansen doordat schending van het vertrouwen in het netwerk snel bekend is. Toch creëren de sociale relaties ook nadelen. Zij beperken bijvoorbeeld het aantal individuen waarmee een misdaadonderneming zaken kan doen of als medewerker kan rekruteren, zowel kwantitatief als

[89] Zie voor dat laatste {Williams, 1995, 168-169}.
[90] {Van Duyne e.a., 1990,22-26}, {Reuter, 1984}, {Mastrofski & Potter, 1987}, {Paoli, 2002, 64-65}, {Wiebrens & Röell, 1988}, {Naylor, 1997}, {Halstead, 1998, 12-14}.
[91] {Paoli, 2002, 84-87}. Ook anderen gaan in op de noodzaak om in netwerken te opereren waaronder {Kleemans e.a., 1999} en {Kleemans e.a., 2002}.

kwalitatief.[92] Eén misdaadmarkt kan bestaan uit meerdere (gescheiden) netwerken. Het lijkt immers niet waarschijnlijk dat alle marktpartijen behoren tot hetzelfde netwerk. Omgekeerd kan één netwerk uiteenlopende misdaadmarkten omspannen.[93]

Uit onderzoek van netwerken van legale ondernemingen blijkt dat deze hoge eisen stellen aan de vaardigheden van het management en aan de processen. Netwerken kennen bovendien een zekere mate van vrijblijvendheid. Het netwerk bestaat bij de gratie van overlappende doelen, maar er bestaan ook spanningsvelden tussen de doelen van de afzonderlijke partners. Netwerken zijn niet afgebakend en er is geen controle op andere netwerken waarin de partners samenwerken. De samenwerkingspartners moeten informatie en kennis delen. Dit biedt weliswaar voordelen, maar ook mogelijkheden voor misbruik. Vanwege de vrijblijvendheid en het aantal partners is planning van en controle op de werkzaamheden ingewikkeld. Hierdoor wordt een deel van de operationele flexibiliteit tenietgedaan. Flexibiliteit op strategisch niveau, bijvoorbeeld bij noodzakelijke veranderingen, is beperkt. Voor veranderingen zijn onderhandelingen nodig met de andere partners en veranderingen kunnen de balans van voor- en nadelen verstoren. Tot slot geldt als nadeel dat verschillen tussen de partners in waarden, normen, cultuur en achtergronden kunnen leiden tot verkeerde interpretaties, irritaties, fouten en een afname van het noodzakelijke vertrouwen in elkaar.[94] De genoemde kenmerken van misdaadmarkten neutraliseren deze nadelen niet en zij zijn daarom in beginsel ook van toepassing voor criminele netwerken.[95]

Misdaadmarkten hebben dus enkele bijzondere kenmerken ten opzichte van legale markten. Een misdaadmarkt vormt in vergelijking met een legale markt een vijandige en ongereguleerde omgeving. Er bestaat een spanningsveld tussen zakendoen en geheimhouding alsmede tussen vertrouwen en geweld. Misdaadondernemingen hebben daardoor te kampen met knelpunten om betrouwbaar en deskundig personeel te krijgen en om informatie en geld te beheersen. Als gevolg van die kenmerken is sprake van een imperfecte marktwerking. Zo zijn misdaadmarkten niet transparant, zijn de transactiekosten hoog en vindt de handel primair plaats in netwerken. Een ander kenmerk is dat er grenzen bestaan voor de omvang van misdaadondernemingen. Daardoor zijn er meer marktschijven dan in vergelijkbare legale markten.

3.7. Illegale groothandelsonderneming

Vooral de organisatievorm van georganiseerde criminaliteit is het onderwerp (geweest) van veel discussie. Onderzoekers hanteren uiteenlopende concepten zoals onderneming, organisatie, crimineel samenwerkingsverband, groep, netwerk of strak geleide hiërarchische organisatie met divisies. In dit proefschrift is gekozen voor het concept van de illegale groothandelsonderneming. Alvorens daarop in te gaan, komt eerst het concept van de (misdaad)onderneming aan bod.

[92] Zie voor andere nadelen paragraaf 4.3.3.
[93] Eigen aanname.
[94] {De Man e.a., 2001}.
[95] Eigen aanname.

Voor de Inkomstenbelasting geldt als uitgangspunt dat "[….] als onderneming wordt beschouwd een organisatie van kapitaal en arbeid die de volgende kenmerken vertoont: 1) zelfstandigheid, 2) duurzaamheid, 3) met een op zichzelf staand winstdoel en 4) met een in beginsel niet beperkte kring van afnemers. De zelfstandigheid houdt in dat pas sprake is van ondernemerschap als men handelt onder eigen naam, voor eigen verantwoordelijkheid en voor eigen risico".[96] Van Duyne e.a. spreken van een misdaadonderneming "[….] wanneer er sprake is van een bestendige marktgerichte onwettige bedrijvigheid, samenwerking en een personele en ruimtelijke organisatie".[97] In deze omschrijving is het element 'personele en ruimtelijke organisatie' vaag en ontbreekt het element van kapitaal en zelfstandigheid ten opzichte van andere marktpartijen. Deze kenmerken zijn van belang om een onderscheid te kunnen maken tussen een misdaadonderneming en andere vormen van criminele samenwerking. Alvorens te komen met een definitie, moeten we eerst nog eens stilstaan bij de mate van samenwerking en de relatie met legale ondernemingen. Dit zijn immers de aspecten die in de definitie van de onderzoeksgroep Fijnaut als problematisch zijn benoemd.

Het begrip onderneming moeten we in het criminele milieu niet al te letterlijk opvatten. Er is immers geen Kamer van Koophandel waar de crimineel zijn organisatie aanmeldt en er zijn geen arbeidscontracten met medewerkers. Een misdaadonderneming is daarom moeilijker af te bakenen dan zijn legale tegenhanger. Van Duyne e.a. spreken van een binnencirkel en van een buitencirkel. De *binnencirkel* bestaat uit naaste medewerkers die nauw betrokken en steeds beschikbaar zijn.[98] Hoewel die medewerkers uiteraard niet op een loonlijst staan, staat het de medewerkers desondanks niet vrij om voor een andere baas te werken of zomaar voor zich zelf te beginnen. De *buitencirkel* bestaat uit de leveranciers, afnemers en ondersteuners in vooral het netwerk. De mate van samenwerking kan variëren van incidenteel tot structureel. Een drugshandelaar kan zijn drugs betrekken van steeds andere handelaren. Hij moet dan maar hopen dat hij kwalitatief goede waar krijgt en dat de ander hem niet bedriegt. Bij structurele samenwerking speelt dat minder, maar neemt de afhankelijkheid van de ander wel toe. Vanwege onder andere de vrijblijvendheid en eventuele arrestaties kan de misdaadonderneming echter niet altijd handelen met dezelfde leveranciers en afnemers.

Een gewone ondernemer maakt een afweging tussen activiteiten binnen de eigen onderneming of inkopen via de markt. Deze afweging geldt ook voor een misdaadondernemer. Wanneer een misdaadonderneming uiteenlopende activiteiten zelf ter hand neemt, duidt men dat wel aan als verticale integratie. Het Van der Valk-concern heeft bijvoorbeeld een eigen slachterij en eigen transporteurs. Een groothandelaar in XTC zou ook zelf een deel van de productie voor zijn rekening kunnen nemen of een deel van de detailhandel. Omgekeerd kan een producent of straatdealer van bijvoorbeeld cocaïne juist de activiteiten uitbreiden naar de groothandel. De spanningsvelden en knelpunten van de illegaliteit vormen echter een barrière om activiteiten binnen de eigen misdaadonderneming uit te voeren. De uitoefening van diverse rollen is bovendien riskant. Zo heeft de misdaadonderneming dan te maken met veel meer betrokkenen, maar ook met grotere financiële risico's.

[96] {Stevens, 1997, 181}. Gekozen is voor het begrip onderneming van de Belastingdienst omdat het hier gaat om een bont pallet van samenwerkingsvormen zonder rechtspersoonlijkheid, zoals een BV of NV. Uiteraard zijn samenwerkingsvormen met rechtspersoonlijkheid niet toepasbaar voor misdaadondernemingen.
[97] {Van Duyne e.a., 1990, 14, 28}.
[98] {Van Duyne e.a., 1990, 3}.

Om dezelfde redenen gaat de misdaadonderneming minder snel over tot diversificatie van producten en activiteiten waarvoor een andere bedrijfsvoering is vereist. De misdaadonderneming beperkt zich daarom bij voorkeur tot producten en activiteiten die aansluiten bij de bestaande bedrijfsvoering.[99] De aanname is daarom dat misdaadondernemingen niet snel overgaan tot verticale integratie van activiteiten en/of diversificatie, zeker niet wanneer daarvoor een andere bedrijfsvoering is vereist.

De misdaadonderneming ontkomt er niet aan om gebruik te maken van de producten van legale ondernemingen. Voorbeelden daarvan zijn telefoonmaatschappijen, vliegmaatschappijen, financiële instellingen of transportondernemingen. Ook hier moet de misdaadondernemer een afweging maken tussen het organiseren van de activiteiten binnen de eigen onderneming of inkopen via de markt, al dan niet via intermediairs. In sommige gevallen zijn die ondernemingen het eigendom van een crimineel. In dat geval maakt de legale onderneming integraal onderdeel uit van de binnencirkel van de misdaadonderneming. Wanneer sprake is van inkopen via de markt, behoort de legale onderneming tot de buitencirkel. Daarmee zijn we terechtgekomen in de discussie over de afbakening tussen georganiseerde en organisatiecriminaliteit.

Wanneer een legale onderneming primair is opgezet om criminaliteit te plegen of te ondersteunen, vormt die een misdaadonderneming op zich of maakt onderdeel uit van een misdaadonderneming. Ditzelfde geldt als een onderneming alleen door de inkomsten uit criminaliteit bestaansrecht heeft. In tegenstelling tot een misdaadonderneming is een onderneming die organisatiecriminaliteit pleegt niet primair gericht op illegaal gewin.[100] Stel dat een bestaand advocatenkantoor meewerkt aan de activiteiten van een misdaadonderneming om de winst van het kantoor wat op te vijzelen. De medewerking van het advocatenkantoor valt op grond van bovenstaande criteria onder organisatiecriminaliteit. Een soortgelijke redenering geldt voor terroristische groepen die in illegale producten handelen om aan het benodigde geld te komen. Het onderdeel van de groep dat handelt in illegale producten met als oogmerk het verdienen van geld, zouden we kunnen beschouwen als misdaadonderneming. Vanuit het bredere perspectief van de politiek georiënteerde groep is echter sprake van een terroristische groep.

Op basis van bovenstaande argumentatie geldt de volgende definitie:

Een misdaadonderneming is een organisatie van kapitaal en arbeid die de volgende kenmerken vertoont:

- *zelfstandigheid (handelt onder eigen naam, voor eigen verantwoordelijkheid en voor eigen risico);*
- *gericht op een duurzame marktgerichte onwettige bedrijvigheid;*
- *met een opzichzelfstaand illegaal winstoogmerk;*
- *voor haar bestaan afhankelijk van inkomsten uit criminaliteit;*
- *met een in beginsel niet beperkte kring van afnemers.*

[99] Zie hiervoor bijvoorbeeld {Reuter, 1984, 129}, {Adamoli e.a., 1998, 16-17}, {Paoli, 2002, 64-67}, {Wiebrens & Röell, 1988}, {Naylor, 1997} en {Kleemans e.a., 2002}.

[100] Zie voor het vraagstuk van georganiseerde criminaliteit en organisatiecriminaliteit onder andere {Enquêtecommissie, 1996B, 26}, {Enquêtecommissie, 1996C}, {Huisman & Niemeijer, 1998}, {Ruggiero, 1996}.

Niet elke misdaadonderneming houdt zich bezig met georganiseerde criminaliteit. Daarvoor geldt als aanvullend criterium dat de onderneming de rol van groothandel moet vervullen. Wat is nu een illegale groothandelsonderneming?

Zoals eerder is aangegeven, vindt een product zijn weg naar de consument via distributiekanalen nader te verbijzonderen naar producent, detailhandel en groothandel. Binnen de categorie consumenten valt een onderscheid te maken tussen een eindconsument en een tussenconsument. Een tussenconsument neemt producten af en verkoopt die weer of gebruikt ze voor de productie van andere producten.[101] De straatdealer in drugs is bijvoorbeeld een tussenconsument van de drugsgroothandelaar. Hij vervult daarbij tevens de rol van de detailhandel voor verslaafden.

Volgens McCarthy is een groothandel een onderneming waarvan de belangrijkste functie is het leveren van groothandelsactiviteiten. Groothandel is "[….] concerned with the activities of those persons or establishments (wholesalers) which sell to retailers and other wholesalers, and/or to industrial, institutional, and commercial users -but who do not sell in large amounts to final consumers". De groothandelsfuncties of groothandelsactiviteiten zijn variaties op de basisfuncties kopen, verkopen, sorteren, opslaan, transporteren, financieren, het nemen van risico's en marktinformatie vergaren. Deze basisfuncties kan een groothandel voor zowel de afnemers, producenten als leveranciers voor zijn rekening nemen. De groothandel kan bijvoorbeeld al goederen inkopen terwijl de klanten er nog niet om vragen. Hierdoor neemt hij het financiële risico voor zijn rekening. Dat is niet alleen gunstig voor de producent, maar ook voor de klant. Deze kan snel de goederen afnemen wanneer hij er behoefte aan heeft, terwijl hij geen risico loopt.[102]

McCarthy maakt een principieel onderscheid tussen een groothandel die het eigendom over de goederen wel of niet verkrijgt. Een voorbeeld van een groothandel die het eigendom niet krijgt, is een veilinghuis of makelaar. Een groothandel die het eigendom wel verkrijgt, splitst hij in een servicegroothandel die alle genoemde functies uitvoert en een 'beperkte functie groothandel' die slechts enkele functies vervult. Binnen die categorieën is weer een verdere onderverdeling mogelijk.[103]

Bovenstaande typering en beschrijving zijn sterk gericht op goederen. Er zijn daarentegen ook misdaadmarkten die zich richten op dienstverlening. Past daarbij het concept van groothandel wel? McCarthy rekent een veiling en makelaar in elk geval tot de groothandel. In de kern gaat het daarbij primair om dienstverlening. En in de reisbranche, ook typisch een dienstverleningstak, verkopen de grote reisorganisaties niet direct aan consumenten, maar aan reisbureaus. De reisorganisaties kopen accommodaties en vliegtuigstoelen in en lopen daarmee een risico. Het uitgangspunt is daarom dat het concept groothandel ook bruikbaar is voor dienstverlening.

Tot nu toe is wel gesproken over de functies van een groothandel, maar nog niet over eisen aan de omvang van de handel, de financiële omzet of periodiciteit. McCarthy hanteert geen ondergrens hiervoor. Hij vindt het kenmerkende onderscheid ten opzichte van de detailhandel dat de groothandel niet aan eindconsumenten levert. De detailhandel verkoopt

[101] {McCarthy, 1981, 337-406}.
[102] {McCarthy, 1981, 386-406, 752}.
[103] {McCarthy, 1981, 386-406}.

daarentegen wel producten aan eindconsumenten. Een verschil met de producent is dat de groothandel zich niet bezighoudt met productie van goederen.[104] Hoewel McCarthy dat niet doet, zouden we wel degelijk eisen kunnen stellen aan de grootschaligheid van de handel. We zouden als criterium kunnen hanteren dat de groothandel een hogere dan gemiddelde omzet heeft in termen van producten en/of financiële omzet. Dat criterium zouden we kunnen verbijzonderen per transactie en/of op jaarbasis. Tevens kunnen we als eis formuleren dat de groothandel vaker dan gemiddeld handelt (periodiciteit) en zich in elk geval niet bezighoudt met een eenmalige transactie.

Grootschaligheid is echter een relatief begrip. Wat in de ene markt groot is, is in een andere markt klein. Een verbijzondering per misdaadmarkt is daarom onontkoombaar. Grootschalige handel is derhalve op te vatten als 'meer dan gemiddeld in een specifieke misdaadmarkt'.[105] Maar, hoe dat te bepalen? Voor misdaadmarkten bestaan geen statistieken van transacties, omzetten en ondernemingen die actief zijn in de markt. De gegevens bij opsporingsinstanties over misdaadmarkten zijn, voorzover ze al bestaan, selectief en verre van compleet. Denkbaar is om gewoon een grens af te spreken. Als vuistregel hanteren Van Duyne e.a. voor groothandel in de hasjmarkt een omzet van tussen de 5000 en 10.000 kilo per jaar als ondergrens.[106] Extra lastig wordt het wanneer de misdaadmarkt een internationaal karakter heeft. In dat geval verdient het de voorkeur om de grens voor grootschaligheid te bepalen op basis van de mondiale misdaadmarkt en niet de misdaadmarkt per land. Maar, een omvang die in Schotland grootschalig is, hoeft dat in Nederland niet te zijn.[107] De noodzakelijke gegevens om grootschaligheid in te vullen zijn in dat geval nog moeilijker boven water te krijgen. En het zal veel tijd en inspanning vergen om internationaal overeenstemming te bereiken over een grens. Daarom is ervan afgezien om eisen te stellen aan de grootschaligheid van de handel voor de illegale groothandelsonderneming.

In sommige definities van georganiseerde criminaliteit stelt men eisen aan de omvang of structuur van de criminele groepen. Bijvoorbeeld de EU hanteert als criterium dat het samenwerkingsverband uit minimaal twee personen moet bestaan.[108] Redenerend vanuit het concept illegale groothandelsonderneming is er geen reden om eisen te stellen aan de omvang of structuur. In theorie zou een illegale groothandelsonderneming kunnen bestaan uit één persoon.

Op basis van de combinatie van de definitie van misdaadonderneming en groothandel luidt de definitie van een illegale groothandelsonderneming:

> *Een illegale groothandelsonderneming is een organisatie van kapitaal en arbeid die de volgende kenmerken vertoont:*
> - *zelfstandigheid (handelt onder eigen naam, voor eigen verantwoordelijkheid en voor eigen risico);*

[104] {McCarthy, 1981}.
[105] Van Duyne e.a. gaan eveneens in op dit vraagstuk op basis van enerzijds het begrip grootschalig en anderzijds de behandeling van de definitie van de BKA. Daar gaat het om het onderdeel 'major significance' in de definitie. Zij beargumenteren dat dit per misdaadmarkt moet worden bepaald en dat dit methodisch ook verantwoord is {Van Duyne e.a., 2001, 23, 55-57}.
[106] {Van Duyne e.a., 2001, 61}.
[107] In paragraaf 3.3 is aangegeven dat Nederland een doorvoerland is en Schotland een eindbestemming.
[108] Zie figuur 3.1 in paragraaf 3.3.

- *met als belangrijkste functie het leveren van illegale groothandelsactiviteiten;*
- *met een opzichzelfstaand illegaal winstoogmerk;*
- *voor haar bestaan afhankelijk van inkomsten uit criminaliteit;*
- *met een in beginsel niet beperkte kring van afnemers (detailhandelaren, andere groothandelsondernemingen of tussenconsumenten).*

3.8. Illegale groothandelsactiviteiten

Al eerder is beschreven dat misdaadondernemingen uiteenlopende rollen kunnen bekleden in misdaadmarkten, waaronder die van producent, groothandel, detailhandel en consument (zie figuur 3.3). In het concept van de criminaliteitspiramide zijn vanuit een andere invalshoek eveneens rollen verbijzonderd.[109] Aan de ene kant werkt de criminaliteitspiramide drie niveaus uit op grond van de middelen en bekwaamheden van de dader en aan de andere vanuit het soort criminaliteit. Op grond van de middelen en bekwaamheden van de daders onderscheidt men in de criminaliteitspiramide: 1) veelplegers, zoals autodieven en straatdealers, 2) faciliterende criminelen, zoals helers en witwassers en 3) plegers van georganiseerde criminaliteit.[110] In de misdaadmarkt van gestolen auto's nemen lokale autodieven het eerste niveau voor hun rekening. Op het tweede niveau bevinden zich de helers en de monteurs die de auto's omkatten. Op het derde niveau bevinden zich degenen die de gestolen auto's in het groot opkopen, verhandelen en distribueren naar andere landen. Het is relatief eenvoudig om de rol van autodief te vervullen in een specifieke plaats. De rol van omkatter en heler is veel lastiger te vervullen. Er zijn daarvoor andere ervaring en kennis vereist. Ook moeten de noodzakelijke financiële middelen beschikbaar zijn en moet een netwerk van dieven en afnemers zijn opgebouwd. De rol van groothandelaar in gestolen auto's is nog lastiger te vervullen. Er is een nog grotere financiële buffer vereist en een groter netwerk. De organisatiegraad op het eerste niveau is gering. Op het tweede niveau is al in meer of mindere mate sprake van een misdaadonderneming. Op het derde niveau kunnen we zeker spreken van een misdaadonderneming, veelal een illegale groothandelsonderneming.

Op grond van het soort criminele activiteiten zijn eveneens drie niveaus te onderscheiden: veelvoorkomende criminaliteit, lokaal ernstige criminaliteit en (zware en) georganiseerde criminaliteit.[111] Op het eerste niveau vinden overwegend zichtbare vormen van criminaliteit plaats. De activiteiten staan (ogenschijnlijk) op zichzelf. Het gaat bijvoorbeeld om inbraken in woningen, de (kleinschalige) illegale verkoop van vuurwapens, de (kleinschalige) illegale verkoop van drugs en autodiefstallen. Deze vormen van criminaliteit bevinden zich primair op het lokale niveau van een wijk of gemeente. Daarboven bevindt zich een niveau van criminaliteit die een hogere graad van professionaliteit, ervaring en

[109] Dit concept is bij sommigen van de Nederlandse politie in gebruik en maakt tevens onderdeel uit van het National Intelligence Model van de National Criminal Intelligence Service (NCIS) van het Verenigd Koninkrijk. Hiërarchische verhoudingen tussen criminelen spelen in het concept van de criminaliteitspiramide geen rol. Het concept is geen uitwerking van hoofdstroom één van Klerks.

[110] Deze uitwerking is mede gebaseerd op een presentatie van NCIS in Rotterdam 18 december 2000 en een studiebezoek aan NCIS in februari 2001. Overigens hanteert NCIS niet het concept van de illegale groothandelsonderneming.

[111] Soms maakt men een onderscheid naar middencriminaliteit, hetgeen zich bevindt tussen de lokale ernstige criminaliteit en georganiseerde criminaliteit. In het 'National Intelligence Model' is het uitgangspunt dat er drie niveaus van criminaliteit bestaan: (a) lokale criminaliteit (local issues), (b) regionale criminaliteit (cross border issues) en (3) serieuze en georganiseerde criminaliteit {NCIS, 2000A}.

een ruimere financiële basis vereist. Dit niveau maakt de criminaliteit aan de onderkant mogelijk. Het gaat daarbij bijvoorbeeld om het helen van gestolen goederen, de verkoop van drugs aan straatdealers, het ter beschikking stellen van een drugspand aan dealers en het leveren van valse paspoorten. Deze vormen van criminaliteit vinden op regionaal of bovenregionaal niveau plaats. Daarboven bevindt zich het niveau van criminaliteit die een nog hogere graad van professionaliteit en nog meer financiën vereist en de partijen die als afnemer optreden van de onderliggende niveaus. Het gaat daarbij bijvoorbeeld om het in- en uitvoeren van gestolen auto's, het importeren van drugs of het exporteren van XTC. Deze vormen van criminaliteit vinden op nationaal of internationaal niveau plaats.

Rol	Voorbeelden in drugsmarkt	Voorbeelden in illegale automarkt
Eind-consument	Verslaafde op straat	Een Pool die een in Nederland gestolen auto koopt
Producent	De boer in Colombia, de inkoper van de boeren, de laboranten	De autodief, de omkatter, de vervalser van papieren
Groothandel	De Colombiaanse maffia, een samenwerkingsverband van plegers van georganiseerde criminaliteit die een grote partij koopt, importeert en verder distribueert	Een Nederlandse illegale groothandelsonderneming die de auto's koopt van de heler en exporteert naar Polen
Detailhandel	De straatdealer	Degene die koopt van de illegale groothandel en de auto's verder verkoopt in Polen. Tevens de heler van de gestolen auto's in Nederland.

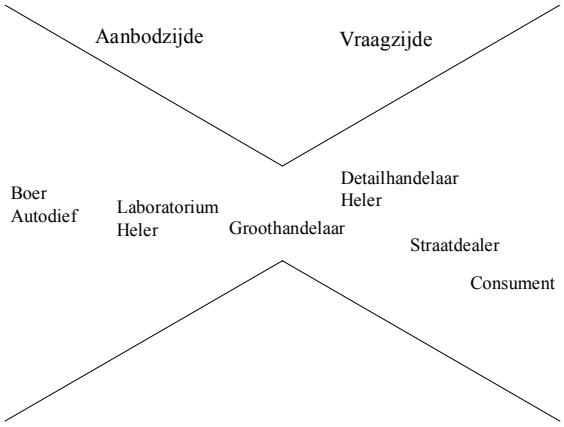
Figuur 3.3 Rollen in misdaadmarkten en voorbeelden daarvan

In potentie is het aantal individuen dat één gestolen auto in Polen kan verkopen groot. Het aantal individuen dat grote aantallen auto's kan opkopen en vervoeren naar Polen, is vele malen kleiner. Hetzelfde geldt in Polen voor de aanschaf en de distributie van de auto's. Aan zowel de vraagzijde als aan de aanbodzijde ontstaat als het ware een vernauwing (zie figuur 3.4). Dit sluit aan bij de constatering van Arlacchi dat in misdaadmarkten aan de vraagzijde twee sectoren zijn te onderscheiden. De ene sector bestaat uit vele kleine en middelgrote semi-onafhankelijke organisaties die leveren aan de eindconsumenten. De andere sector bestaat uit een beperkt aantal oligopolistische ondernemingen die aan de eerste sector leveren.[112]

Illegale groothandelsactiviteiten zijn uiteenlopend van aard. Het is bij legale organisaties gebruikelijk om een onderscheid te maken tussen primaire en ondersteunende activiteiten. De primaire activiteiten hangen direct samen met de rol van de groothandel, namelijk het kopen, verkopen, sorteren, opslaan, transporteren, financieren, nemen van risico's en marktinformatie vergaren. Deze activiteiten genereren de winst waar het allemaal om te doen is. Een voorbeeld daarvan is het importeren en verkopen van partijen drugs. De tweede soort (criminele) activiteiten zijn de ondersteunende activiteiten. Net als in legale ondernemingen zijn personele, informatie- en financiële activiteiten belangrijk. Binnen legale ondernemingen vecht men conflicten met leveranciers, afnemers en medewerkers uit met behulp van juridische procedures. Binnen een misdaadonderneming vormt het dreigen met of gebruiken van geweld hiervoor een substituut. Net als een legale moet een

[112] {Arlacchi, 1998, 204}.

misdaadonderneming de eigen bezittingen beveiligen en zorgen dat geen bedrijfsgeheimen naar buiten komen. Hiervoor hanteert zij specifieke afschermingsmethoden die van invloed zijn op de personele, financiële en informatieactiviteiten. Daar waar legale ondernemingen op zoek kunnen gaan naar informatie over concurrenten, kan de misdaadonderneming op zoek gaan naar informatie van opsporingsinstanties. Dit kan zowel passief als heel gericht plaatsvinden. Eenzelfde vergelijking gaat op voor het dwarsbomen van de concurrentie en/of mediacampagnes van legale ondernemingen om de beeldvorming te beïnvloeden. Misdaadondernemingen kunnen proberen om opsporingsinstanties te dwarsbomen en de beeldvorming te beïnvloeden via offensieve strategieën. Naast genoemde ondersteunende activiteiten moet een misdaadonderneming ook allerlei activiteiten ontplooien om de opbrengsten veilig te kunnen stellen. Williams en Godson veronderstellen in elk geval dat misdaadondernemingen op zoek gaan naar constructies en landen om dat te bewerkstelligen. Legale ondernemingen gaan daarentegen op zoek naar fiscaal gunstige constructies en landen.[113]



Figuur 3.4 Trechtereffect in misdaadmarkten[114]

Een twijfelgeval vormen (criminele) activiteiten die direct dienen ter ondersteuning van de primaire activiteiten, maar geen winst genereren. In sommige gevallen moet een drugshandelaar bijvoorbeeld ambtenaren corrumperen of identiteitsdocumenten vervalsen. Deze activiteiten genereren geen winst en zijn ook niet primair bedoeld om de misdaadonderneming te laten functioneren. Daarentegen zouden die (criminele) activiteiten niet hoeven plaats te vinden zonder de primaire criminele activiteiten. In dat kader zouden we kunnen spreken van secundaire activiteiten. In potentie is het gehele Wetboek van Strafrecht hierop van toepassing.

Zoals eerder aangegeven kan een illegale groothandelsonderneming bepaalde activiteiten zelf organiseren of inhuren via netwerken. Activiteiten die voor de een van secundaire of ondersteunende aard zijn, kunnen daarentegen voor een ander de primaire activiteiten zijn. Misdaadondernemingen kunnen zich specialiseren in bijvoorbeeld witwassen, het vervalsen van documenten of het uitvoeren van liquidaties. Wanneer een legale

[113] {Williams & Godson, 2002, 326}.
[114] Gebaseerd op {Lupsha, 1996}.

onderneming ondersteuning verleent, kan het gaan om organisatiecriminaliteit. Analytisch zouden we de ondersteuning kunnen beschouwen als een onderdeel van de illegale groothandelsactiviteiten. Deze keuze wordt niet voorgestaan. De activiteiten van de externe accountants of transporteurs rekenen we immers ook niet tot de groothandels- of detailhandelsactiviteiten van bijvoorbeeld het Ahold-concern. Wanneer andere (misdaad)ondernemingen ondersteuning verlenen, in wel sprake van *betrokkenheid* bij georganiseerde criminaliteit.

Samenvattend kunnen we stellen dat de illegale groothandelsactiviteiten zijn onder te verdelen in: primaire, secundaire en ondersteunende (criminele) activiteiten. In het vervolg zijn de twee eerste soorten, ook wel aangeduid als de *uitoefening van de groothandelsfuncties*. In plaats van over 'illegale groothandelsactiviteiten' wordt ook wel gesproken over 'illegale bedrijfsvoering'. In dat geval ligt het accent op de bedrijfsvoering in plaats van op de activiteiten zelf. De illegale groothandelsactiviteiten resulteren ook in betrokkenheid van leveranciers, afnemers en ondersteuners. Die betrokkenheid is weliswaar instrumenteel, maar maakt daar geen onderdeel van uit.

3.9. Omgeving van georganiseerde criminaliteit

Vroegtijdige criminaliteitsbeheersing begint met het verkrijgen van inzicht in ontwikkelingen in de samenleving.[115] Daartoe moeten we wel nader bepalen wat de afbakening is tussen de samenleving en georganiseerde criminaliteit.

Het is gangbaar om een onderscheid aan te brengen tussen de legale wereld en het criminele milieu[116], ook wel aangeduid als bovenwereld en onderwereld. Hoewel analytisch relevant, gaat het om beladen begrippen en om een glijdende schaal. De begrippen zijn beladen, omdat het een normatief onderscheid aanbrengt.[117] Tevens is de grens van legaal naar illegaal veelal vloeiend en moeilijk te bepalen. Ook criminelen maken onderdeel uit van de samenleving, terwijl ogenschijnlijk eerzame burgers en bedrijven toch als consument, producent of handelaar kunnen opereren in misdaadmarkten. In de misdaadmarkt van verboden producten opereren vooral misdaadondernemingen en die kunnen we rekenen tot het criminele milieu. Zij maken echter wel in meer of mindere mate gebruik van de dienstverlening van legale bedrijven, bijvoorbeeld voor transport. In deze 'criminele dienstverleningsmarkt van de bovenwereld' opereren primair legale ondernemingen waar ook legale bedrijven zaken mee doen. Bij de handel in goederen met een fiscale prijswig doen de misdaadondernemingen hun best om zo veel mogelijk onopvallend zaken te doen in de legale wereld. Eerder is deze problematiek aan de orde geweest bij het onderscheid tussen georganiseerde en organisatiecriminaliteit. Voor een zinvol onderscheid moeten we vooral de rol die een partij vervult, in beschouwing nemen. De crimineel die overdag zijn kinderen naar school brengt, valt analytisch onder de samenleving. Hij heeft dan de rol van een gewone burger. De crimineel die daarentegen in een café rondhangt om handel te bedrijven, valt onder een misdaadmarkt. Hier vervult hij de rol van misdaadondernemer.

[115] Zie subparagraaf 1.2.2.
[116] {Kleemans e.a., 1999}.
[117] Zie hiervoor ook paragraaf 3.4.

Het criminele milieu omvat meer dan alleen georganiseerde criminaliteit. Illegale groothandelsondernemingen voeren hun activiteiten uit in misdaadmarkten. Daarin opereren ook andere marktpartijen. Wanneer bijvoorbeeld zich een tendens voordoet dat misdaadondernemingen onderling strategische allianties aangaan in misdaadmarkten, mogen we aannemen dat dit van invloed is op georganiseerde criminaliteit. Het criminele milieu beperkt zich echter niet tot alleen misdaadmarkten. Zo opereren overvallers niet in misdaadmarkten. Toch kan zich bijvoorbeeld een ontwikkeling voordoen dat overvallers hun geld gaan investeren in de handel in illegale producten of zich juist laten inhuren door anderen omdat zij op zoek zijn naar nieuwe, minder riskante, activiteiten. Ontwikkelingen in het criminele milieu kunnen daardoor ook leiden tot veranderingen in misdaadmarkten en daardoor (mede) tot veranderingen in georganiseerde criminaliteit.

In dit proefschrift worden onder de noemer ‘ontwikkelingen in de samenleving’ uitsluitend de ontwikkelingen gerekend die zich voordoen in de legale wereld (bovenwereld). Voorbeelden daarvan zijn: de EU-uitbreiding, biotechnologie, mondiaal islamisme en ICT-ontwikkelingen. Dit sluit aan bij het ‘van buiten naar binnen redeneren’.[118] Ontwikkelingen in misdaadmarkten en in het overige criminele milieu, vallen niet onder die noemer. Dit laat onverlet dat het ook zinvol is om die ontwikkelingen te analyseren.

[118] Zie paragraaf 1.1.

4. Kader voor risicoanalyse georganiseerde criminaliteit

4.1. Inleiding

Dit hoofdstuk beschrijft het derde onderdeel van het risicoanalyse-instrumentarium. Het gaat om een analysekader dat inzicht moet geven in de trits 'ontwikkeling(en) – veranderingen – ongewenste effecten' en in de waarschijnlijkheid van die veranderingen. Het vertrekpunt is het conceptuele model van georganiseerde criminaliteit als een stelsel van illegale groothandelsondernemingen. Een aanname is dat de gelegenheidstheorie bruikbaar is voor de vertaling van een ontwikkeling in de samenleving naar veranderingen in georganiseerde criminaliteit en voor de beoordeling van de waarschijnlijkheid van de veranderingen. Een ontwikkeling kan immers één of meer gelegenheidsfactoren beïnvloeden en zo leiden tot een verandering. De mate van invloed van de ontwikkeling op de verandering bepaalt de waarschijnlijkheid daarvan.

Omdat de gelegenheidstheorie van oorsprong is gericht op vermogenscriminaliteit, is een aanpassing nodig. Deze theorie gaat uit van vier met elkaar samenhangende gelegenheidsfactoren: doelwit, dader, sociale controle en 'locatie en tijdstip'. Voor georganiseerde criminaliteit kunnen we, in plaats van over dader, beter spreken over illegale groothandelsonderneming. Deze handelt in illegale producten in plaats van zich bezig te houden met diefstal van goederen en geld. Daarom is het beter om te spreken over 'illegale groothandelswaar' in plaats van over doelwit. Omdat het tijdstip voor illegale groothandelsondernemingen geen rol van betekenis speelt, is de betreffende gelegenheidsfactor 'locatie' genoemd in plaats van 'locatie en tijdstip'.[1] De paragrafen 4.2 tot en met 4.5 werken de gelegenheidsfactoren stuk voor stuk uit. Paragraaf 4.6 onderscheidt enkele soorten veranderingen op basis van de uitwerking van de gelegenheidsfactoren. Met behulp van die typologie kunnen we gericht kijken naar een ontwikkeling en dreigingen identificeren.[2] Paragraaf 4.7 vertaalt de uitwerking van de gelegenheidsfactoren naar de risicofactoren. Dat is van belang voor de beoordeling van de waarschijnlijkheid. Wanneer een verandering in georganiseerde criminaliteit zich voordoet, kunnen daaruit ongewenste effecten voortkomen. Paragraaf 4.8 beschrijft enkele analytische uitgangspunten daarvoor en benoemt er enkele.

4.2. Gelegenheidsfactor illegale groothandelswaar

Illegale groothandelsondernemingen handelen in illegale producten. Niet elk product leent zich echter voor de groothandel. Van Duyne e.a. benoemen de volgende karakteristieken van misdaadmarkten waarin ruimte is voor grootschalige handel:

- *"They are widespread, in terms of participants and customers;*
- *They have a continuous and substantial turnover in terms of merchandise;*
- *They generate a substantial and continuous flow of money."*[3]

[1] Voor de onderbouwing, zie paragraaf 4.5.
[2] Zie paragraaf 6.2 voor een voorbeeld daarvan.
[3] {Van Duyne e.a., 2001}.

Ze onderbouwen deze karakteristieken niet, noch in de vorm van argumenten, noch in de vorm van een bronverwijzing. Hierna volgt een eigen uitwerking van de factoren die een illegaal product geschikt maken voor de illegale groothandel, gebruikmakend van genoemde karakteristieken. De factoren zijn beredeneerd en niet empirisch getoetst.

Uit de definitie van een groothandel vloeit voort dat hij niet levert aan eindconsumenten en niet zelf produceert.[4] Dat impliceert dat er minimaal twee schakels zitten tussen de producent[5] en de eindconsument. Wanneer de producent immers rechtstreeks levert aan de eindconsument, dan kunnen we op basis van de definitie niet spreken van een groothandel. Wanneer de producent levert aan een partij die rechtstreeks verkoopt aan een eindconsument, kunnen we evenmin spreken van een groothandel. De extra schakels van groot- en detailhandel moeten wel een toegevoegde waarde hebben. Die waarde is gelegen in de specialistische rol die zij vervullen en/of de lagere kosten omdat zij schaalgroottevoordelen kunnen realiseren.[6] De andere marktpartijen moeten op hun beurt bereid zijn te betalen voor de rol van de groot- en de detailhandel en de transactiekosten voor lief nemen.

De specialistische rol van een groothandelsonderneming bestaat uit het kopen, verkopen, sorteren, opslaan, transporteren, financieren, nemen van risico's en marktinformatie vergaren. Zij doet zaken met producenten, andere groothandelaren en/of detailhandelaren. De specialistische rol heeft vooral een toegevoegde waarde wanneer er vele eindconsumenten en/of producenten zijn en deze praktisch gezien niet rechtstreeks met elkaar zaken kunnen doen. Dat sluit aan bij de eerste karakteristiek van Van Duyne e.a. Bij een beperkt aantal eindconsumenten kan de producent in beginsel rechtstreeks zakendoen met de eindconsument. Bij weinig producenten kan de eindconsument rechtstreeks zakendoen met de producent. Een handicap voor producenten en consumenten is wel dat misdaadmarkten niet transparant zijn. Al eerder is aangegeven dat daardoor misdaadmarkten meer marktschijven kennen dan vergelijkbare legale markten.

In de drugsmarkt heeft specialisatie een toegevoegde waarde. Een groothandelaar heeft het geld om grote partijen te kopen, beschikt over de relevante contacten in het criminele milieu, kan grote partijen vervoeren en kan het ook nog eens op een afgesproken locatie afleveren. Omgekeerd heeft een verslaafde aan cocaïne praktisch gezien geen toegang tot de producenten en omgekeerd de producenten niet tot de drugsverslaafden. Bij de handel in kinderpornomateriaal kunnen producenten en eindconsumenten daarentegen wel rechtstreeks met elkaar zakendoen. Eenmaal gekocht door een eindconsument, is het kopiëren en manipuleren van het oorspronkelijke materiaal eenvoudig. De eindconsumenten kunnen daarom op hun beurt ook als producent en distributeur gaan optreden. Via het internet kunnen eindconsumenten en producenten rechtstreeks met elkaar in contact komen en is sprake van een levendige ruilhandel. Daar komt niet tot nauwelijks geld aan te pas. Daardoor is handel in kinderpornomateriaal niet interessant op groothandelsniveau.

Massaproducten, zoals drugs en vuurwapens, lenen zich eerder voor een specialistische rol van de groothandel dan maatwerkproducten. Voor massaproducten zijn immers meer eindconsumenten te vinden. Tevens ligt het handelen in grote partijen meer voor de hand

[4] Zie paragraaf 3.7.
[5] Dit begrip omvat zowel fabrikanten van fysieke goederen, dieven die goederen stelen voor de handel (et cetera), als dienstverleners.
[6] Zie de paragrafen 3.5 en 3.8.

dan bij maatwerkproducten. Zeker dienstverlening heeft veelal een individueel en maatwerkkarakter. Daarbij moeten de producent en de eindconsument rechtstreeks contact met elkaar hebben. Een voorbeeld daarvan is de videoproductie van een huwelijk. Daarbij is geen behoefte aan een groothandel. In misdaadmarkten is orgaanhandel een voorbeeld waarbij producent (medicus), leverancier (donor) en afnemer met elkaar in contact moeten staan en sprake is van maatwerk.

Een ander aspect van de toegevoegde waarde van een groothandel zijn de lagere kosten als gevolg van schaalgroottevoordelen. De reis naar Colombia voor de aanschaf van een kleine hoeveelheid cocaïne, het uitdenken van een smokkelroute en dergelijke kost in beginsel niet veel minder moeite dan voor de aanschaf van een grote hoeveelheid. Toch leent niet elk product zich voor handel in grote volumes en dus voor schaalgrootte. Bij unieke schaarse producten, zoals gestolen kunstvoorwerpen, is geen sprake van grootschalige omzetmogelijkheden. Het aantal gestolen voorwerpen is op jaarbasis immers niet groot, de diefstal is snel bekend en het is maar de vraag of er veel consumenten zijn die een specifiek gestolen voorwerp willen kopen. Als belegging is het in elk geval niet geschikt, omdat verkoop buiten het criminele milieu nauwelijks mogelijk is. Kortom, gestolen kunstvoorwerpen lenen zich naar de aard niet om in grote hoeveelheden te verhandelen. De tweede karakteristiek van Van Duyne e.a. van een continue en substantiële omzet, sluit hierbij aan. Zonder een continue en substantiële omzet zijn geen schaalgroottevoordelen te behalen.

De producenten, andere groothandelaren en afnemers moeten wel bereid zijn om te betalen voor de rol van de groothandel. Dat sluit aan bij de derde karakteristiek van Van Duyne e.a. Voor bijvoorbeeld de handel in kinderpornomateriaal is de winstpotentie gering, omdat er is sprake van een levendige ruilhandel, waar niet echt geld aan te pas komt. Daardoor is deze handel niet interessant op groothandelsniveau.

Resumerend gaat het om de volgende factoren die bepalen of een product geschikt is als illegale groothandelswaar:
1. De hoeveelheid eindconsumenten en/of producenten.
2. De mate waarin eindconsumenten en producenten praktisch gezien in staat zijn om rechtstreeks zaken met elkaar te doen.
3. De mate waarin sprake is van een massaproduct.
4. De mate waarin met de uitoefening van de groothandelsfuncties in het product schaalgroottevoordelen zijn te behalen.
5. De mate waarin afnemers van de groothandel bereid zijn een hogere prijs te betalen dan de prijs die de groothandel heeft betaald aan zijn leveranciers.

4.3. Gelegenheidsfactor illegale groothandelsonderneming

4.3.1. Invalshoeken illegale groothandelsonderneming

Voor de daadwerkelijke handel in geschikte producten zijn misdaadondernemingen nodig die de functies van de groothandel voor hun rekening *willen* en *kunnen* nemen. Deze paragraaf werkt de factoren uit die daarbij een rol spelen.

4.3.2. Illegale groothandelsonderneming: het willen

Waarom zou iemand overgaan tot de handel in illegale waar? De reden is evident: hij wil geld verdienen aan die handel en dus winst maken. Het feit dat bepaalde handelswaar winstpotentie heeft, betekent niet automatisch dat de misdaadondernemer dat inziet. Dit geldt zelfs al voor een legale ondernemer. Microsoft ontdekte pas in een laat stadium dat internetgerelateerde software het helemaal zou gaan maken. En als een legale onderneming van het kaliber Microsoft niet altijd de winstpotentie inziet, is het niet aannemelijk dat dit anders ligt voor misdaadondernemingen. Overigens kan het omgekeerde ook voorkomen. De misdaadondernemer denkt winst te kunnen genereren, maar dit valt in de praktijk tegen. Het willen wordt dus (mede) bepaald door de indruk dat de misdaadondernemer winst kan maken met de handel in een bepaald product (winstperceptie).

Toch vormt de winstperceptie niet de enige factor. De misdaadondernemer streeft mede naar het instandhouden van de misdaadonderneming en de eerdere verdiensten. Tevens zal hij proberen om lijf en leden van zichzelf en zijn dierbaren te behouden. Toch loopt hij voortdurend het risico dat hij zijn handelswaar of geld kwijt raakt als gevolg van diefstal of inbeslagname, dat de overheid hem van zijn vrijheid berooft of dat een collega-crimineel fysiek geweld tegen hem gebruikt.[7] De rationeel opererende misdaadondernemer zal voortdurend een afweging maken tussen de gepercipieerde winstpotentie van de handel en het risico dat hij loopt. Net zomin als de misdaadondernemer de winstpotentie betrouwbaar kan beoordelen, geldt dit voor het risico. Het willen wordt dus ook bepaald door de risicoperceptie van de handel in een bepaald product.

Waaruit bestaat het risico? Voor een belangrijk deel komt die voort uit de sociale controle. Des te intensiever die controle en des te meer mogelijkheden er bestaan voor controle, des te riskanter. Dit aspect valt onder de gelegenheidsfactor sociale controle en blijft hier verder buiten beschouwing (zie paragraaf 4.4). De risico's zijn voor een deel ook afkomstig van de afnemers, leveranciers en ondersteuners. Al eerder is immers gewezen op spanningsvelden bij iedere transactie en de knelpunten van het opereren in de illegaliteit.[8]

Hoewel de winst- en risicoperceptie twee belangrijke factoren zijn voor het willen, verklaren deze nog niet alles. Waarom nemen sommigen onnodig risico's door zelf criminele activiteiten te ontplooien?[9] Waarom ging Charles Z., die volgens de politie beschikt over grote sommen geld na zijn vrijlating in 1997, weer door met de drugshandel?[10] Een verklaring hiervoor kunnen we wellicht vinden bij het profiel van de misdaadondernemer.

Er is hierover echter weinig onderzoek beschikbaar.[11] Onderzoek hiernaar is bovendien niet eenvoudig. Weliswaar praat een crimineel graag, maar het is niet in het eigen belang om het achterste van de tong te laten zien. Bovendien is het lastig om te controleren of men de waarheid spreekt. De meest succesvolle criminelen blijven wellicht buiten het vangnet van de politie. Hierdoor ontstaat een vertekend beeld. Er bestaan wel enkele journalistieke biografieën, waaronder die van Bruinsma en Charles Z. Klerks stelt dat de criminele

[7] {Van Duyne e.a., 1990}, {Van Duyne, 1995}, {Chang, 1998, 23}, {Lupsha, 1996, 34}, {NCIS, 2001}, {Adamoli e.a., 1998, 11}.
[8] Zie paragraaf 3.6 en subparagraaf 4.3.3.
[9] Kleemans e.a. geven hiervan enkele voorbeelden {Kleemans e.a., 2002}.
[10] {Husken, 2001}.
[11] {Klerks, 2000, 217}, {Jackson & Herbrink, 1996, 5}, {Bovenkerk, 2001, 41}.

normen en waarden liggen in het verlengde van de subcultuur van de handelaren. Uit onderzoek blijkt verder dat in de levensfilosofie van misdaadondernemers vrijheid, onafhankelijkheid en een afkeer van autoriteiten en sleur vooropstaan. Bestaanszekerheid en het vermijden van risico's spelen veel minder een rol. De misdaadondernemer heeft vooral een afkeer van burgerlijkheid. Hij associeert dit met saaiheid en weinig opwinding en beschouwt het opereren in de criminaliteit daarentegen als avontuurlijk. Hij vertaalt de behoefte aan onafhankelijkheid meestal in het verlangen naar een eigen bedrijf. De misdaadondernemer ervaart het laten slagen van een eigen zaak als een uitdaging en als een bron van trots. De behoefte aan geld is weliswaar de belangrijkste reden om crimineel actief te zijn, maar is ook een middel om aan de gevreesde burgerlijkheid te ontkomen. Dit verklaart waarom sommigen zich toch zelf met criminaliteit blijven bezighouden, terwijl ze financieel gezien dit zouden kunnen uitbesteden. Bovendien beleven sommigen ook plezier aan het lopen van een risico.[12] Op basis hiervan mogen we aannemen dat bepaalde handelswaar en activiteiten meer tot de verbeelding spreken dan andere. Een kapitein op de grote vaart zal niet zo snel overstappen naar het beroep van boekhouder. Net zomin zal een drugshandelaar snel overstappen op het vanachter zijn bureau met de pc plegen van criminaliteit. De handel moet dus wel passen bij de achtergronden en de competenties van de onderneming en ondernemer.

Samenvattend kunnen we stellen dat de volgende factoren bepalen of een illegale groothandelsonderneming wil handelen in illegale producten:

- de mate waarin de misdaadondernemer de indruk heeft dat hij winst kan maken met de handel;
- de mate waarin hij de risico's acceptabel acht in relatie tot de winstverwachting;
- de mate waarin hij het product en/of de activiteiten interessant vindt.

4.3.3. Illegale groothandelsonderneming: het kunnen

Stel dat een misdaadondernemer de indruk heeft dat hij winst kan maken met de handel in een bepaald product, dat de risico's acceptabel zijn en dat het product hem interesseert. In dat geval moet hij de groothandelsactiviteiten nog wel waar kunnen maken. Deze sub-paragraaf beschrijft de factoren die bepalen of een misdaadonderneming hiertoe in staat is.

We staan eerst stil bij hetgeen nodig is voor de uitoefening van de groothandelsfuncties. De essentie van de groothandel is vooral het kopen van leveranciers en het verkopen aan afnemers of het tegen betaling bemiddelen tussen die twee. Betrokkenheid van leveranciers en afnemers is dus randvoorwaardelijk. Dat is niet echter eenvoudig in misdaadmarkten. Een eerste reden is dat misdaadmarkten vooral mondiaal zijn. Een tweede reden is dat bepaalde producten, misdaadmarkten, en rollen zijn geclusterd rondom etniciteit. Colombiaanse criminelen houden zich bijvoorbeeld bezig met de productie en groothandel in cocaïne. Turkse criminelen houden zich voor een belangrijk deel bezig met heroïne en cannabis. Een derde reden is dat in sommige misdaadmarkten de afnemers of leveranciers zich bevinden in de bovenwereld. Bepaalde (medewerkers van) legale ondernemingen zijn genegen deze rol op zich te nemen, maar lang niet iedereen. Daar komt nog een vierde reden bij, namelijk dat misdaadmarkten níét transparant zijn en er dus geen overzicht bestaat van misdaadondernemingen die als leverancier of afnemer optreden. Kleemans e.a.

[12] {Klerks, 2000, 215-238, 357}, {Van de Bunt e.a., 1999, 401}, {Kleemans e.a., 2002}.

spreken in dat kader over barrières tussen verschillende landen, etnische groepen of tussen onderwereld en bovenwereld.[13] Deze barrières worden nog eens versterkt doordat bij het aangaan van een illegale transactie de eerdergenoemde spanningsvelden bestaan.[14]

Genoemde context leidt ertoe dat de koop en verkoop wel moeten plaatsvinden in netwerken. Netwerken zijn gebaseerd op sociale relaties, bijvoorbeeld sociale achtergrond, geboorteplaats of de gevangenis waarin men heeft gezeten. Hierdoor zijn netwerken in beginsel begrensd. Bovendien is het niet vanzelfsprekend dat er in die netwerken leveranciers en afnemers beschikbaar zijn die handel willen en kunnen drijven in het gewenste product. Misschien bevinden die zich niet in het eigen netwerk, maar wel in andere netwerken. Naast de eerdergenoemde barrières bestaan dus ook nog eens barrières tussen netwerken. Al eerder is betoogd dat een netwerk meerdere misdaadmarkten kan omspannen en dat een misdaadmarkt kan bestaan uit meerdere netwerken. Iemand die dus deel uitmaakt van meer dan één netwerk binnen en tussen misdaadmarkten verkeert in een goede uitgangspositie om de rol van groothandel op zich te nemen. Onderdeel uitmaken van de juiste netwerken is dus randvoorwaardelijk om überhaupt handel te kunnen drijven. Dit is overigens ook van belang om zaken te kunnen doen met de noodzakelijke ondersteuners.

Naarmate de misdaadondernemer meer groothandelsfuncties voor zijn rekening neemt, nemen de eisen toe. Wanneer de misdaadonderneming zich, naast koop en verkoop, bezighoudt met de functies sorteren, opslaan en transporteren, moet zij een *logistiek proces* opzetten. De onderneming moet immers de gekochte handelswaar ophalen, vervoeren, opslaan en weer afzetten. Daarvoor moet een *infrastructuur* beschikbaar zijn, zoals dekmantelfirma's (zie verderop), opslagplaatsen en transportroutes. Ook moeten de vereiste *middelen* voorhanden zijn, zoals vervoermiddelen en (vervalste) papieren. Verder moet de onderneming beschikken over een minimumniveau aan *materiekennis, -informatie en ervaring*. Voor mensensmokkel is inzicht in de immigratiewetgeving van Westerse landen bijvoorbeeld onontkoombaar. Voor de functies financieren en het nemen van risico's is een *bedrijfskapitaal* noodzakelijk. Zo vereist de import van drugs een aanzienlijke investering. Met behulp van een financiële buffer moet de misdaadonderneming tegenslagen kunnen opvangen. Het schaadt immers de reputatie en positie in netwerken wanneer bij een inbeslagname geen geld (meer) beschikbaar is om de partij alsnog te betalen en de afnemers te voorzien van een nieuwe partij drugs.

Op enig moment ontkomt een misdaadonderneming er niet aan om voor de uitoefening van de groothandelsfuncties illegale en legale activiteiten te verweven. Afnemers, leveranciers, ondersteuners (betrokkenen) en de benodigde infrastructuur bevinden zich immers (deels) in de bovenwereld. Allereerst moet de misdaadonderneming gebruikmaken van legale goederen en diensten, verder aangeduid als *legale faciliteiten*. Voorbeelden zijn: grondstoffen, vervoer, ontmoetings- en opslagplaatsen, vliegtickets, vereiste papieren of kennis en telecommunicatie. Wanneer de afname van goederen en diensten van legale instanties een grote omvang aanneemt, heeft de misdaadonderneming een plausibele verklaring nodig. Luchtvaartmaatschappijen moeten de papieren van passagiers controleren. De notaris moet de identiteit van een individu nagaan. Banken moeten contante stortingen die aan bepaalde formele criteria voldoen, melden. Zij moeten ervan

[13] {Kleemans e.a., 2002, 39-63}.
[14] Zie subparagraaf 3.6.4.

overtuigd zijn dat er een legale verklaring is voor de grote afname van producten. Naast inhuur van legale instanties, kan de misdaadonderneming ook zelf de noodzakelijke faciliteiten verzorgen door een eigen bedrijfje te runnen. In plaats van een ruimte te huren in een horecagelegenheid, kan zij natuurlijk ook zelf een horecagelegenheid of autoverhuurbedrijf gaan exploiteren. Dit is echter niet in alle gevallen mogelijk. Het ligt bijvoorbeeld niet voor de hand dat de misdaadonderneming een eigen vliegmaatschappij opzet.

Om aan de legale faciliteiten te kunnen komen, heeft de misdaadonderneming dus behoefte aan een *dekmantel*. De gesmokkelde drugs kan bijvoorbeeld meeliften met de legale lading van een legaal (dekmantel)bedrijf. De dekmantel kan ook dienen om in contact te komen met klanten of leveranciers, bijvoorbeeld in een coffeeshop. In sommige gevallen, zeker bij misbruik van invoer- en uitvoerregelingen, is een rechtspersoon noodzakelijk om de fraude te kunnen plegen. Hier is de dekmantel niet nodig om aan de faciliteiten te kunnen komen, maar juist om de criminaliteit überhaupt te kunnen plegen.

Ook de ondersteunende (criminele) activiteiten stellen eisen aan het kunnen van de illegale groothandelsonderneming. Het operen in de illegaliteit gaat immers gepaard met enkele spanningsvelden en knelpunten. De misdaadondernemer moet hier in de bedrijfsvoering rekening mee houden. Een illegale groothandelsonderneming loopt als gevolg van de schaalgrootte nog eens extra risico's. De handel verloopt in grotere volumes en omzet en hogere frequentie en er zullen veelal meer medewerkers of andere ondersteuners betrokken zijn. Dit valt niet alleen op bij de collega-criminelen, maar ook bij opsporingsinstanties. De rol van groothandel is bovendien niet gegroeid van de ene op de andere dag.[15] De onderneming zal daardoor bekend zijn bij collega-criminelen en opsporingsinstanties. Bijzondere aandacht behoeven personeelsbeheer, informatiebeheer, geldbeheer, afscherming en het veiligstellen van de opbrengsten.[16] Met uitzondering van afscherming, waaraan reeds in paragraaf 3.5 uitvoerig aandacht is besteed, volgt hierna een toelichting op die aandachtspunten.

De uitoefening van de groothandelsfuncties kan arbeidsintensief zijn. Betrouwbaar personeel is dan van groot belang om verraad of bedrog te voorkomen. Afspraken worden immers niet vastgelegd en betalingen vinden plaats met baar geld. Misverstanden kunnen snel ontstaan en bewezen betrouwbare persoonlijke contacten zijn dan van groot belang. Een personeelsadvertentie is niet mogelijk. De eigen familie en/of sociale relaties vormen in principe een beperkte kring om uit te werven. Bovendien kunnen zij wel betrouwbaar zijn, maar nog niet altijd bekwaam. Medewerkers met antecedenten kunnen onnodig de aandacht van de politie trekken.[17] Vanwege het ongereguleerde karakter van misdaadmarkten is soms geweld nodig om medewerkers in het gareel te houden.

Net als voor elke andere organisatie is informatie een cruciale factor. Maar, vanwege de noodzakelijke geheimhouding en vermijding van bewijssporen zijn communicatie en administratie een riskante aangelegenheid. Verstrekte of vastgelegde informatie kan

[15] Van Duyne e.a. wijzen er op dat misdadigers niet van de ene op de andere dag toetreden tot georganiseerde criminaliteit {Van Duyne e.a., 1990, 9}. Paoli geeft aan dat vertrouwen, noodzakelijk om zaken te doen, pas ontstaat na vele transacties {Paoli, 2002, 64}.

[16] Zie subparagraaf 3.6.4 en 3.8.

[17] {Arlacchi, 1998, 207}, {Van Duyne e.a., 1990, 20-22, 39}, {Kleemans e.a., 1999, 127-130}, {Van Duyne, 1995}, {Ruggiero, 1996, 119-125}, {Klerks, 2000, 191}.

terechtkomen bij opsporingsinstanties of de concurrentie. Toch is in elk geval communicatie met klanten, leveranciers en medewerkers belangrijk om te kunnen functioneren. Delegatie van taken en een gestroomlijnde organisatie vereisen nu eenmaal ook informatie-uitwisseling. Om vertrouwen te wekken in het criminele milieu, moet de misdaadondernemer bovendien zo af en toe toch zijn successen kenbaar maken. Bovendien geeft het een zekere mate van arbeidssatisfactie om daarover te praten.

De misdaadonderneming beperkt deels de risico's van communicatie door oog in oog communicatie. Hierdoor is in ieder geval het gevaar van het afluisteren van de communicatiemiddelen uitgesloten en kan de een de ander recht in de ogen kijken. Deze vorm van communicatie is echter wel arbeidsintensief, zeker bij overbrugging van grote afstanden. Het geeft ook ernstige beperkingen in noodsituaties.[18] Een andere methode om de risico's te beheersen is gefragmenteerde en late verstrekking van informatie. Misverstanden kunnen echter het gevolg zijn en ook hiervoor geldt dat deze methode in noodsituaties niet volstaat.

Het geldbeheer vormt eveneens een knelpunt. Betalingen vinden overwegend chartaal plaats. Chartaal geld heeft beperkingen. Het kan niet alleen leiden tot beroving, maar neemt bovendien veel fysieke ruimte in beslag en is moeilijk te transporteren. Bovendien zijn niet alle valutasoorten en coupures courant. De misdaadonderneming moet daarom op enig moment het chartale geld omwisselen en omzetten in giraal geld. Giraal geld kent dan wel niet de fysieke beperkingen, maar leidt wel tot zichtbaarheid van het geld. Een tussenvorm betreft het zogenaamde ondergronds bankieren en het gebruik van moneytransfers. Het geld kan worden verplaatst waarbij een zekere mate van anonimiteit mogelijk is. Volgens Kleemans e.a. leveren echter ook deze wijzen van bankieren bewijssporen op. De misdaadonderneming moet verder een deel van het verdiende geld investeren in de bedrijfsvoering en in nieuwe criminele activiteiten. Voor investeringen kan zij geen beroep doen op reguliere financiële instellingen en dus moet een eigen bedrijfskapitaal voorhanden zijn. Verzekeringen bestaan niet en bij tegenslag kan het kapitaal als sneeuw voor de zon verdwijnen.[19]

Ook voor de ondersteunende (criminele) activiteiten is verweving van illegale en legale activiteiten onontkoombaar. *Witwassen* is noodzakelijk om baar geld om te zetten in giraal geld en om geld en eigendom te kunnen verantwoorden tegenover de overheid. "Verdienen kan in de legale wereld door: inkomsten uit arbeid, vermogensstijging en vermogensoverdracht. De technieken van het witwassen sluiten aan bij deze normale manieren van geld verkrijgen. Het gaat hierbij dan vooral om het voorwenden van inkomsten, vermogensstijging of vermogensoverdracht".[20] Wanneer iemand elke week met een tas geld bij de bank aankomt, of beschikt over grote sommen geld, valt dit op. In dat geval volstaat het niet om te suggereren dat de inkomsten volledig in het casino zijn verdiend. Er is dan een dekmantel noodzakelijk om de inkomsten te kunnen verantwoorden. Door actief te zijn in bijvoorbeeld de seksbranche kan de misdaadonderneming legale inkomsten voorwenden.

[18] {Van Duyne e.a., 1990}, {Kleemans e.a., 2002}.
[19] {Reuter, 1984, 121}, {Van Duyne e.a., 1990}, {Kleemans e.a., 2002}.
[20] {Enquêtecommissie, 1996B, 128}.

Op enig moment kan ook de behoefte of noodzaak ontstaan om de verdiende gelden te *investeren*, bijvoorbeeld in onroerend goed of een legale onderneming. Een investering kan aantrekkelijk zijn omdat die niet alleen status geeft, een bron kan zijn voor legale inkomsten, maar ook een oudedagsvoorziening vormt. Een investering kan ook noodzakelijk zijn om aan een dekmantel te komen. In dat geval is de dekmantel het doel van de investering. In elk geval vereisen investeringen in bedrijven en onroerend goed tot op zekere hoogte dat de gelden zijn witgewassen. De notaris is immers bij dergelijke transacties betrokken, waardoor men een legale herkomst van de gelden moet kunnen verantwoorden. Dit geldt zeker voor grootschalige investeringen. Ook investeringen in onroerend goed vallen op enig moment op. Ook daarvoor is een plausibele verklaring nodig. In deze gevallen zijn een dekmantel en witwassen middelen om investeringen te kunnen plegen en vice versa. Volgens Van Duyne komen overigens de Nederlandse plegers van georganiseerde criminaliteit nauwelijks toe aan investeren. Zij spenderen vooral het verdiende geld. Volgens Kleemans e.a. gaan consumptieve bestedingen en investeringen daarentegen wel degelijk samen.[21]

De onderneming is dus voor vier vormen van ondersteuning afhankelijk van de bovenwereld, namelijk voor legitimering, facilitering, witwassen of investeringen.[22] Zoals hiervoor al bleek, zijn de verschillende functies analytisch wel te onderscheiden, maar zullen ze in de praktijk door elkaar lopen. Aan investeringen gaat bijvoorbeeld witwassen vooraf en is een dekmantelfirma soms randvoorwaardelijk.

Ook het betrekken van de noodzakelijke ondersteuning vanuit de bovenwereld stelt eisen aan de illegale groothandelsonderneming. Er bestaan enkele varianten om de bovenwereld te betrekken. Moerland en Boerman onderscheiden in de *mate van betrokkenheid* van legale bedrijven vier vormen: gebruik, afpersing, samenwerking en bezit. Gebruik houdt in beginsel in dat geen van de medewerkers op de hoogte is van de rol die de organisatie bij de criminele activiteiten speelt. In sommige gevallen had men zich echter wel degelijk bewust kunnen of moeten zijn van de betrokkenheid. Wanneer sprake is van afpersing, dwingt de misdaadonderneming de medewerking op enigerlei wijze af. In het geval van samenwerking zal de betrokkene zich daarvan niet alleen bewust zijn, maar deze ook als profijtelijk ervaren.[23] In het geval van bezit is veelal het formele eigendom in handen van een stroman. Om bedrijven te betrekken bij de illegale bedrijfsvoering kan de misdaad-onderneming een beroep doen op intermediairs. Zij voeren activiteiten uit die de misdaadonderneming niet zelf kan of wil uitvoeren en slaan een brug naar de boven-wereld.[24]

Vooral voor het witwassen en investeren zijn de diensten van vrijeberoepsbeoefenaars onmisbaar. Het gaat dan om accountants, advocaten en notarissen.[25] Zij hebben immers een maatschappelijke (monopolie)positie bij het autoriseren of uitvoeren van bepaalde transacties. Bij bijvoorbeeld de aankoop van onroerend goed of de verwerving van

[21] {Van Duyne, 1995}, {Enquêtecommissie, 1996C}, {Kleemans e.a., 2002}.
[22] De vier functies zijn ontleend aan de functies van legale branches voor georganiseerde criminaliteit: (1) faciliterende functie, (2) legitimerende functie, (3) witwasfunctie en (4) spenderende functie {Enquêtecommissie, 1996D}, {Moerland & Boerman, 1999} en {Kleemans e.a., 2002, 82}.
[23] {Moerland & Boerman, 1999, 145-146}.
[24] Kleemans e.a. gaan uitvoerig in op de functies van intermediairs, veelal aangeduid als facilitators {Kleemans e.a., 2002, 56-62}.
[25] {Kleemans e.a., 1999, 86}, {Enquêtecommissie, 1996B, 112-123}.

rechtspersonen is een notaris altijd betrokken. Zij nemen daarmee een sleutelpositie in in het maatschappelijke en economische verkeer. Ook hebben zij lang niet altijd de mogelijkheid om klanten te weigeren. Een notaris moet in principe het transport van een hypotheekakte regelen, ongeacht of de klant hem wel of niet aanstaat. Wanneer de notaris weigert, zal hij zich moeten verantwoorden. Dit in tegenstelling tot een transportondernemer die volledig vrij is om een lading te weigeren. De beroepsgroepen hebben niet alleen een monopoliepositie, maar ook een geheimhoudingsplicht en/of verschoningsrecht. Tevens hebben zij financiële en juridische kennis en een maatschappelijke status van respectabiliteit en betrouwbaarheid.[26] Dit maakt ze extra aantrekkelijk.

In het voorgaande is uitgewerkt wat nodig is ten behoeve van de illegale bedrijfsvoering en de ondersteuning vanuit de bovenwereld. Daarbij heeft het accent gelegen op de middelen en de randvoorwaarden waaraan voldaan moet zijn. Over welke bekwaamheden moet de misdaadondernemer zoal beschikken? Net zomin als iedereen er in slaagt om als gewone ondernemer een boterham te verdienen, slaagt iedere crimineel als misdaadondernemer. Bovenkerk stelt dat de misdaadondernemers niet zoveel verschillen van de managers van grote legale ondernemingen. Hij concludeert dat de misdaadondernemer in een persoonlijkheidstest hoog moet scoren op de dimensie extraversie en heel laag op het kenmerk altruïsme. Hij heeft een dominante persoonlijkheid en legt een zekere mate van consciëntieusheid in het handelen aan de dag. Hij beschikt over "[….] beheerste impulsiviteit, een avontuurlijke en megalomane verbeelding die hen boven de gewone mensen verheft". Bovendien is de diagnose 'narcissistic personality disorder' van toepassing voor een misdaadondernemer.[27] Een sterke sociale aanleg, zakentalent, ambitie, creativiteit, avontuurlijkheid en onverstoorbaarheid behoren volgens hem (1998) tot de pluspunten.[28]

In het legale bedrijfsleven noemt men vaak flexibiliteit en innovatie als noodzakelijke voorwaarden om te kunnen overleven.[29] Geldt dat ook voor illegale groothandelsondernemingen? Volgens sommigen is flexibiliteit kenmerkend voor georganiseerde criminaliteit en een vereiste om te kunnen opereren in misdaadmarkten. Voorbeelden hiervan zijn: het benutten van nieuwe mogelijkheden, het verleggen van transportroutes vanwege meer of minder intensieve grenscontroles en het neutraliseren van andere werkwijzen van opsporingsinstanties.[30] Veelal stelt men dat de flexibiliteit voortkomt uit het opereren in netwerken. Toch is maar de vraag hoe ver die flexibiliteit gaat. Al eerder is gewezen op de beperking van flexibiliteit op strategisch niveau in netwerken. Wanneer de misdaadonderneming in haar voortbestaan wordt bedreigd, zal ze haar werkwijze snel aanpassen. Ongetwijfeld heeft de Nederlandse penoze rekening gehouden met de verscherpte grenscontroles vanwege de MKZ-crisis begin 2001. Wanneer de douane op Schiphol een nieuwe controlemethode hanteert, reageert men snel. Maar of de misdaadonderneming flexibel inspeelt op nieuwe wensen van (criminele) klanten en innoveert, is maar de vraag. Zo wijst Aalbersberg in 2000, het hoogtepunt van de ICT-hype, op het feit dat Turkse misdaadondernemers in Nederland toen nog beperkt gebruikmaakten van

[26] {Enquêtecommissie, 1996B, 112, 131-132}.
[27] {Bovenkerk, 2001, 61-79}. Ondanks zijn kritiek op de definitie van de onderzoeksgroep Fijnaut, hanteert hij die definitie wel als vertrekpunt voor zijn redenering.
[28] Zie hiervoor {Van den Eerenbeemt, 1998}.
[29] Zie bijvoorbeeld {Castells, 1998B} en {Castells, 2001}.
[30] {Ruggiero, 1996, 156}, {Van Duyne, 1993, 11}, {Chang, 1998, 12}, {Mastrofski & Potter, 1987, 269, 275}, {NCIS, 2002}.

nieuwe communicatiemiddelen. Zij vervoerden bovendien nog op klassieke wijze geld naar het moederland.[31] Kleemans e.a. (2002) wijzen er op dat plegers van georganiseerde criminaliteit zich overwegend specialiseren. Als ze al overgaan tot verbreding van de activiteiten, dan liggen deze in het verlengde van de kernactiviteiten. Smokkel van cocaïne en heroïne liggen relatief dicht bij elkaar. Smokkel van cocaïne en EU-fraude daarentegen niet. Verder geven zij blijk van risicomijdend gedrag en gewoontevorming om onzekerheid en complexiteit te vermijden. Bovendien is er lang niet altijd een prikkel om te veranderen van handelswaar.[32] Verder stellen Kleemans e.a. dat misdaadondernemingen hechten aan vertrouwdheid en bekendheid met de sociale setting. Ook dit beperkt de flexibiliteit en innovatie.[33] Al met al zijn misdaadondernemingen niet echt flexibel of innovatief te noemen.[34]

Enkele factoren bepalen dus of een misdaadonderneming kan optreden als illegale groothandel, namelijk de mate waarin:

1. zij kan beschikken over betrouwbare leveranciers, afnemers, ondersteuners en medewerkers in de netwerken;
2. zij kan beschikken over een toereikend(e) logistieke proces, infrastructuur, middelen, financiën, materiekennis, -informatie en ervaring;
3. zij kan beschikken over de vereiste faciliteiten van legale bedrijven alsmede over dekmantels, witwas- en investeringsvoorzieningen in de bovenwereld;
4. zij de geheimhouding kan bewaren en bewijssporen vermijden;
5. zij de knelpunten van het opereren in de illegaliteit kan oplossen (personele, informatie en financiële knelpunten alsmede afscherming);
6. de misdaadondernemer beschikt over de capaciteiten om een onderneming te runnen.

4.4. Gelegenheidsfactor sociale controle

Het uitgangspunt van de gelegenheidstheorie is dat de bekwame bewakers die personen of organisaties zijn die in staat zijn om de gemotiveerde dader te behoeden van het plegen van criminaliteit. Het eendimensionale onderscheid van dader en bewaker is voor georganiseerde criminaliteit minder toepasbaar. Deze paragraaf werkt uit *waarop* de controle zich kan richten, *wie* de controle kan uitvoeren, *wat* het inhoudt en welke factoren bepalen dat partijen sociale controle *willen* en *kunnen* verrichten.

Er zijn diverse objecten waar de controle zich op kan richten. Het eerste object is de illegale groothandelsonderneming. Deze pleegt de criminaliteit. Het tweede object zijn degenen die optreden als afnemer, leverancier of ondersteuner, verder aangeduid als ‘betrokkenen’. Zonder hen kan de illegale groothandel niet functioneren. Sociale controle op hen kan dus de misdaadonderneming behoeden van het plegen van criminaliteit. Het derde object is de illegale groothandelswaar zelf. Zo kunnen goederenstromen worden gecontroleerd. Het vierde object zijn de illegale groothandelsactiviteiten.

[31] Gebaseerd op interview met Aalbersberg (zie bijlage 4).
[32] {Kleemans e.a., 2002, 6-7, 72-79}.
[33] {Kleemans e.a., 2002, 77}.
[34] Paragraaf 6.3 gaat verder in op de mate waarin aan randvoorwaarden voor innovatie is voldaan in misdaadmarkten.

Wie kunnen we voor georganiseerde criminaliteit beschouwen als bewakers? Allereerst moeten we een analytisch onderscheid maken tussen degenen die zich primair bewegen in de bovenwereld en degenen die zich primair bewegen in het criminele milieu.[35] Concurrerende en rivaliserende criminelen en criminelen die de gemaakte afspraken niet nakomen, kunnen de illegale groothandelsonderneming behoeden van het plegen van criminaliteit. Toch zouden we het begrip sociale controle wel heel erg oprekken als we dit daaronder zouden rekenen. Verder voeren betrokkenen in het criminele milieu sociale controle uit op de illegale groothandelsonderneming. Die controle is echter gericht op het instandhouden van de illegale handel en het vertrouwen en dus gericht op het tegendeel van wat hier wordt bedoeld. Daarom rekenen we degenen die zich primair bewegen in misdaadmarkten en het criminele milieu níét tot de bewakers. Het gaat dus om personen en instanties die zich primair bewegen in de bovenwereld.

In de bovenwereld kunnen we drie soorten bewakers identificeren, namelijk 1) betrokkenen, 2) de overheid en 3) overigen. Voor de *betrokkenen* moeten we onderscheid maken naar het soort betrokkenheid (zie figuur 4.1). In sommige gevallen is iemand bewust betrokken en heeft daar profijt van. Feitelijk is dan sprake van mededaderschap. Een mededader heeft er geen enkel belang bij om sociale controle uit te oefenen met als doel om die betrokkenheid te verbreken. Daarom vallen mededaders niet onder de bewakers. Bij de andere vormen van betrokkenheid is weliswaar een afweging nodig met andere belangen, maar kunnen we degenen die betrokken zijn wel degelijk rekening tot de bewakers (zie verderop). Binnen de *overheid* kan een onderscheid worden gemaakt tussen de overheid in het algemeen en de toezichthoudende en opsporingsinstanties, zoals de douane en de politie. Naast betrokkenen en de overheid kunnen ook anderen sociale controle uitoefenen. Een postbode kan bijvoorbeeld merkwaardige zaken bespeuren bij bedrijven waar hij de post bezorgt. Passanten kunnen aanvoelen dat zich ergens zaken afspelen die het daglicht niet kunnen verdragen. Een bijstandstrekker die regelmatig met het vliegtuig naar het buitenland gaat, zou toch op zijn minst vraagtekens moeten oproepen. Het betreft een vorm van sociale waakzaamheid en meldingsbereidheid aan toezichthoudende en opsporingsinstanties.

Soort betrokkenheid:	**Profijtelijk**	**Niet profijtelijk**
Bewust	Bordeel dat slachtoffers van mensenhandel prostitueert Vergunningverlening door corrupte ambtenaar	Afpersing van een legale onderneming door een misdaadonderneming om mee te werken aan criminaliteit
Onbewust	Telefoonmaatschappij die prepaid telefoons verkoopt	Een branche als geheel waarin enkelen als betrokkene fungeren

Figuur 4.1 Soorten betrokkenheid en voorbeelden daarvan

Wat houdt sociale controle in dit kader in? Hierbij moeten we onderscheid maken tussen de eerdergenoemde objecten van sociale controle alsmede naar de bewaker die de controle

[35] Eerder is al aangegeven dat de bovenwereld overlapt met misdaadmarkten en misdaadmarkten overlappen met het criminele milieu. Desondanks is het onderscheid analytisch van belang (zie ook paragraaf 3.9).

voor zijn rekening neemt (zie figuur 4.2). Vormen van sociale controle zijn onder andere preventie, toezicht, het melden aan opsporingsinstanties, zelfregulering en stimulering daarvan.

	Bewaker:		
Object van controle:	*Betrokkenen bij georganiseerde criminaliteit*	*Overheid*	*Overig*
Illegale groothandelsonderneming	Preventie, toezicht en aangifte	Preventie, toezicht en opsporing	Sociale waakzaamheid en meldingsbereidheid aan opsporingsinstanties
Betrokkenen bij georganiseerde criminaliteit	Preventie, toezicht en aangifte op individueel niveau Zelfregulering, tuchtraden (e.d.) op brancheniveau	Stimulering zelfregulering (e.d.) door betrokkenen Wet- en regelgeving om maatregelen door betrokkenen af te dwingen Preventie, toezicht en opsporing	
Illegale groothandelswaar	Preventie, toezicht en aangifte	Preventie, toezicht en opsporing	
Illegale groothandelsactiviteiten	Preventie, toezicht en aangifte	Preventie, toezicht en opsporing	

Figuur 4.2 Vormen van sociale controle en voorbeelden daarvan

Voor sociale controle is randvoorwaardelijk dat de bewakers de sociale controle ter hand willen en kunnen nemen. Omgekeerd geldt voor illegale groothandelsondernemingen dat er juist ruimte bestaat wanneer de bewakers de sociale controle níét ter hand willen en kunnen nemen.

Welke factoren bepalen het *willen*?[36] Wellicht de meest doorslaggevende factor is het belang dat het individu of de instantie heeft bij de sociale controle. Individuen en instanties houden uiteraard ook rekening met andere belangen. Slachtoffers zullen in het algemeen best bereid zijn om preventieve maatregelen te treffen en aangifte te doen. Zij worden direct in hun belangen aangetast. Toch blijkt dat zelfs slachtoffers niet altijd bereid zijn om preventieve maatregelen te treffen en aangifte te doen.[37] Voor hen die onbewust en profijtelijk betrokken zijn, is de afweging nog lastiger dan bij slachtoffers. Zelfs voor de overheid geldt dat beheersing van georganiseerde criminaliteit slechts één van de belangen is. Zo moet een afweging plaatsvinden tussen het privacybelang en het belang van opsporing of het fiscale belang versus het opsporingsbelang. Onderzoekers van het Kernteam Noord- en Oost-Nederland wijzen op het feit dat fiscale voorzieningen om buitenlandse investeerders aan te trekken ook worden misbruikt door buitenlandse criminelen. Deze voorzieningen zijn profijtelijk voor de staat.[38] Ondanks bekendheid met het misbruik blijven die voorzieningen intact en de controle erop beperkt.

[36] De uitwerking van het willen en kunnen zijn gebaseerd op inzichten verkregen uit: {Van Dijk e.a., 1999}, {Geerts & Boekhoorn, 1990, 70-76}, {Van den Anker, 1999}, {Hoogenboom, 2000, 107}, {Patijn, 1999, 45-47}, {Keesman & Scholtes, 1998}, {Van Lier, 1998A, 3-6}, {Van Lier, 1998B}, {De Bestuurlijke aanpak Boek 1, 16-19}, {Kleemans e.a., 1999, 135}.

[37] Van Dijk e.a. noemen daarvan diverse voorbeelden {Van Dijk e.a., 1999}.

[38] {Kernteam Noord- en Oost-Nederland, 2001}.

Betrokkenheid bij georganiseerde criminaliteit tast veelal slechts (indirect) abstracte belangen aan die veelal op de lange termijn spelen en vooral gelden voor de samenleving of branche als geheel. Het gaat dan om belangen zoals de integriteit van het financiële stelsel of van de overheid (zie paragraaf 4.8). De kosten die verband houden met sociale controle gaan dan ruimschoots voor de baten uit. De vraag speelt daarbij wie welke bijdrage kan of moet leveren en ten koste van wat. De gehele Nederlandse economie heeft profijt wanneer bijvoorbeeld de Russische maffia via Nederland crimineel geld zou doorsluizen naar andere landen. Moeten banken deze transacties weigeren? Moeten ze de transacties doorgeven aan de politie?[39] Is het een taak van de Nederlandsche Bank om transacties tussen Nederlandse en Russische banken per definitie kritisch te beoordelen? De Russische maffia misbruikt immers een deel van de Russische banken.[40] In afgeleide vorm speelt het vraagstuk ook voor de politie. In hoeverre is de politie überhaupt verantwoordelijk voor de integriteit van het financiële stelsel? In de afweging speelt het morele oordeel over het type criminaliteit waarschijnlijk wel een rol. Sommigen vinden drugs niet moreel verwerpelijk, terwijl men kinderporno in het algemeen wel verwerpelijk vindt. Logischerwijze ligt de drempel om betrokken te zijn bij drugs daarom minder hoog dan bij kinderporno. Andere belangen winnen het dan van de integriteit en normen en waarden.

Wat bepaalt het *kunnen*? Een eerste dimensie is de mate waarin men in de feitelijke situatie de sociale controle ter hand kan nemen. Vanuit het adagium 'waar een wil is, is een weg' kunnen we veronderstellen dat de wil om de controle ter hand te nemen voor een belangrijk deel het kunnen bepaalt. Enkelen wijzen op het feit dat gedogen van strafbare feiten een moreel schemergebied creëert. Langs elkaar heen werkende toezichthoudende en opsporingsinstanties kunnen voor misdaadondernemers interessante mogelijkheden bieden. Ze kunnen als het ware tussen de wal en het schip vallen.[41] Deze omstandigheden beperken dus de sociale controle. Vanwege het internationale karakter van georganiseerde criminaliteit is de speelruimte voor bijvoorbeeld de Nederlandse overheid beperkt. De overheden van de verschillende landen hebben immers verschillende belangen en bevoegdheden. In algemene zin geldt verder dat een zwakke overheid een gunstige uitgangssituatie vormt voor georganiseerde criminaliteit[42] en dus de mogelijkheden voor sociale controle beperkt.

Voor opsporingsinstanties geldt dat allerlei factoren het kunnen bepalen. Het gaat daarbij om de mate van onderlinge samenwerking, het kwaliteitsniveau van de medewerkers en werkwijzen, de beschikbare capaciteit en bevoegdheden en de beschikbare middelen, waaronder financiën.[43] Vrijwel alle strafrechtelijke onderzoeken op het terrein van georganiseerde criminaliteit vereisen internationale informatie-uitwisseling en/of operationele afstemming. Vanwege de verschillen in wetgeving tussen landen is dat arbeidsintensief en vereist een lange doorlooptijd. Bovendien is de aanpak van internationale georganiseerde criminaliteit primair gericht op het eigen territoir. Plegers van georganiseerde criminaliteit opereren juist internationaal. Dit belemmert de opsporing. In andere situaties kan sociale controle vrijwel onmogelijk zijn. Zo maken sommigen zich

[39] De Wet Melding Ongebruikelijke Transacties (MOT) richt zich niet op girale transacties, maar op chartaal geld.
[40] Zie {Williams, 1999} en {Sinuraya, 1997}.
[41] {Kleemans e.a., 1999}, {Kleemans e.a., 2002}, {Patijn, 1999, 45-47}, {Keesman & Scholtes, 1998}.
[42] Zie voor voorbeelden en een uitwerking hiervan {Albanese, 2002, 2002, 10} en {Williams & Godson, 2002, 315-323}.
[43] Zie bijvoorbeeld ook {Albanese, 2002, 10}.

ernstige zorgen over het gebrek aan controlemogelijkheden op de activiteiten die plaatsvinden via het internet. Dit onderwerp komt uitvoerig aan bod in de hoofdstukken 5 en 6.

Samenvattend kunnen we stellen dat de volgende factoren de sociale controle bepalen:
1. de mate waarin de betrokkenen bij georganiseerde criminaliteit, de overheid en overigen belang hebben bij de controle;
2. de mate waarin de betrokkenen, de overheid en overigen controle kunnen uitoefenen op de (activiteiten van de) illegale groothandelsonderneming, de betrokkenen zelf en de illegale handelswaar.

4.5. Gelegenheidsfactor locatie

De gelegenheidstheorie gaat uit van convergentie tussen doelwit, dader en de afwezigheid van sociale controle. Voor georganiseerde criminaliteit is de gelegenheidsfactor doelwit veranderd in illegale groothandelswaar en dader in illegale groothandelsonderneming. Op basis daarvan en de uitwerking van de overige gelegenheidsfactoren kunnen we stellen dat de volgende convergentie zich moet voordoen wil sprake zijn van illegale groothandelsactiviteiten:
a. er is handelswaar die geschikt is voor de illegale groothandel én;
b. er zijn misdaadondernemingen die de functies van de groothandel voor hun rekening willen en kunnen nemen én;
c. de betrokkenen, de overheid en anderen willen of kunnen onvoldoende maatregelen treffen om de risico's voor de groothandelsondernemingen zodanig hoog te maken dat zij afzien van de handel.

In hoeverre moeten alle drie de gelegenheidsfactoren convergeren, wil sprake zijn van illegale groothandelsactiviteiten? Voor vermogenscriminaliteit is de veronderstelling dat de combinatie van een doelwit en de afwezigheid van sociale controle vanzelf daders aantrekt.[44] Voor georganiseerde criminaliteit is dit niet aannemelijk. Handelswaar en/of gebrek aan sociale controle hoeven niet te resulteren in ondernemingen die de rol van illegale groothandel op zich willen en kunnen nemen. De drempels liggen hoog en de misdaadondernemers betreden vooral de gebaande paden.[45] Zonder illegale groothandelswaar bestaan natuurlijk evenmin illegale groothandelsactiviteiten. Daarentegen leidt de *aanwezigheid* van sociale controle niet altijd tot *afwezigheid* van handel in een bepaald product. Dit hangt mede af van de winstpotentie en of men de handel in het product interessant vindt.[46] De onderneming kan bijvoorbeeld op zoek gaan naar een land waar de controle minder is of kan de werkwijze aanpassen. Bovendien moet de misdaadonderneming toch al allerlei voorzorgsmaatregelen treffen. In de ongereguleerde misdaadmarkten zijn de collega-criminelen en andere betrokkenen immers niet altijd te vertrouwen. Desondanks gaat het te ver om te stellen dat de sociale controle er niet toe doet.[47] Een intensivering van toezicht en opsporing op een specifieke misdaadmarkt kan bijvoorbeeld

[44] Zie paragraaf 1.2.2.
[45] Zie subparagraaf 4.3.2.
[46] Zie subparagraaf 4.3.2.
[47] Zie bijvoorbeeld Kleemans e.a. die stellen dat een misdaadonderneming probeert de overheid te ontlopen {Kleemans e.a., 1999}, {Kleemans e.a., 2002}.

de handelswaar minder aantrekkelijk maken, waardoor misdaadondernemingen de bakens gaan verzetten. Dat sociale controle er toe doet, kunnen we ook afleiden uit de verschillen met landen als de Verenigde Staten en Italië. Het politieke systeem en de cultuur bieden daar meer mogelijkheden voor georganiseerde criminaliteit dan in Nederland.[48] Alle drie de gelegenheidsfactoren moeten dus gezamenlijk convergeren, wil sprake zijn van illegale groothandelsactiviteiten.

Waar vindt de convergentie dan plaats? Voor vermogenscriminaliteit is die vraag eenvoudig te beantwoorden. De locatie is daar waar het doelwit en de dader zich bevinden. Voor illegale groothandelsactiviteiten is het antwoord veel minder eenduidig. Leveranciers, afnemers, ondersteuners, medewerkers, misdaadondernemingen en bewakers, zij kunnen allen vanuit een andere locatie opereren. Bovendien kan een misdaadonderneming de verschillende activiteiten elk op een aparte locatie verrichten. Een voorbeeld kan dit verduidelijken. Een Nederlandse misdaadondernemer koopt een container cocaïne van een Colombiaanse misdaadonderneming in een Amsterdams café. Een dag daarna verkoopt hij de cocaïne in kleinere hoeveelheden aan Engelse en Scandinavische groothandelaren in een café in Londen. De Colombiaanse misdaadonderneming sorteert de cocaïne en vervoert deze vanuit Colombia naar een Panamees schip dat geankerd is op de Atlantische oceaan. Van daaruit wordt de cocaïne gedistribueerd naar het Verenigd Koninkrijk en Scandinavische landen. De cocaïne komt Nederland niet in. Het geld gaat via ondergrondse bankiers vanuit Engeland en Scandinavische landen naar Nederland en vanuit Nederland voor een deel naar Colombia. De opbrengsten van de cocaïne worden witgewassen via Belgische banken en uiteindelijk op een Zwitserse rekening geplaatst. Er vinden dus vele activiteiten plaats op diverse locaties in de wereld. Het is niet toevallig dat de cocaïne wordt overgeslagen op volle zee, want buiten de continentale wateren is sociale controle lastig. Evenmin is het toevallig dat gebruik wordt gemaakt van het Belgische en Zwitserse bankensysteem. In dit geval bepaalt de sociale controle in combinatie met de reguliere en legale voordelen van een land *waar* de misdaadonderneming bepaalde activiteiten uitvoert.

De factoren die een rol spelen bij de keuze voor een land kunnen variëren naargelang het soort groothandelsfunctie, het type groothandelsonderneming, het soort product, het type sociale controle et cetera. Voor een misdaadonderneming die zich ook bezighoudt met transport, vormen Schiphol en de Rotterdamse haven uiteraard gunstige omstandigheden. Factoren die Nederland aantrekkelijk maken voor het reguliere internationale bedrijfsleven, maken in dat opzicht Nederland ook aantrekkelijk voor buitenlandse misdaadondernemingen. Voor een groothandel in heroïne vormt de aanwezigheid van een Turkse minderheid in Nederland, de rol van Turkije in de internationale heroïnemarkt en de milde houding in Nederland tegen drugs een gunstige combinatie. Volgens NCIS hebben Colombiaanse smokkelaars hun afzetgebied verlegd van Noord-Amerika naar Europa, omdat de prijzen hier hoger liggen en dus de winstmogelijkheden groter zijn. Colombianen gebruiken vooral Spanje als invoerland in Europa vanwege de historische banden en de gemeenschappelijke taal. Zij gebruiken daarnaast Nederland als springplank voor de rest van Europa vanwege Schiphol en de Rotterdamse haven.[49]

Om welke soorten factoren gaat het zoal die de keuze bepalen? In studies zien we vaak het PEST-kwartet naar voren komen als verklarende factoren voor criminaliteit. Hiermee doelt

[48] Zie bijvoorbeeld {Wiebrens & Röell, 1988}.
[49] {NCIS, 2000B, 40}.

men op politieke, economische, sociale en technologische factoren.[50] Rosenthal e.a. onderscheiden in algemene zin een breder scala van contextuele factoren, namelijk geografische, sociaal-culturele, economische, technologische, historische, juridische, situationele en politieke factoren.[51] Bij situationele factoren gaat het bijvoorbeeld om een specifieke omstandigheid, zoals de MKZ-crisis begin 2001. Daarom is het beter om te spreken van tijdelijke factoren. Albanese noemt, naast de reeds aangegeven factoren, ook het criminele milieu als factor.[52] De ervaring van de penoze in een gebied speelt volgens hem mede een rol bij de criminaliteit waar men zich op toelegt. De meeste van de genoemde factoren zijn dynamisch en de geografische statisch. De historische factoren en het criminele milieu wijzigen slechts op de lange termijn.

Als we met al de genoemde factoren rekening zouden moeten houden, dan zou de onderzoeker al snel migraine krijgen. Er zijn dan te veel factoren om in de analyse te betrekken. Hij moet rekening houden met in Nederland woonachtige en in Nederland opererende groothandelaren. Hij moet ook beoordelen of groothandelaren mogelijkerwijze in Nederland gaan wonen of hun activiteiten gaan verleggen naar Nederland. Hij moet niet alleen kijken naar factoren die bepalen waarom ze hun oog op Nederland richten, maar ook op de factoren die bepalen waarom juist andere landen wel of niet aantrekkelijk zijn. En als hij het goed zou willen doen, moet hij die factoren ook nog eens in samenhang bekijken. Voegen we daar nog eens aan toe dat dit kan variëren naargelang het product, het type onderneming en afzonderlijke aspecten van de illegale bedrijfsvoering (et cetera) dan mag duidelijk zijn dat dit geen haalbare kaart is.

Per risicoanalyse zal daarom vooraf moeten worden bepaald waar de grenzen liggen. Voor een verkennende risicoanalyse zou kunnen worden volstaan met een beoordeling van de voordelen en risico's van een land en de mate van vertrouwdheid en bekendheid met de sociale setting.[53] Een misdaadonderneming zal namelijk niet zo snel haar activiteiten verleggen naar totaal onbekende gebieden, waar men bovendien geen springplank heeft. Politieke instabiliteit in een land bijvoorbeeld heeft weliswaar enkele voordelen, maar houdt ook risico's in. Een Afrikaanse dictator verwelkomt wellicht crimineel geld, maar bij het verdwijnen van de dictator kunnen de zaken er opeens heel anders voorstaan. Bovendien heeft niet iedereen zomaar toegang tot de dictator of de andere machtshebbers. Verder biedt het Zwitserse bankenstelsel meer wereldwijde mogelijkheden dan die van een geïsoleerd Afrikaans land.

Een andere variant is om specifiek te kijken naar functies die landen vervullen. Williams onderscheidt vier functies: thuisbasis, thuismarkt, doorvoergebied en servicegebied.[54] Daar kunnen we, op basis van de uitwerking van groothandelsfuncties, nog drie functies aan toevoegen, namelijk marktplaats, opslag- en sorteergebied. *Thuisbasis* is een land waar de misdaadondernemer en zijn medewerkers wonen en leven. *Thuismarkt* is het land waar de misdaadonderneming haar afnemers heeft en/of leveranciers. *Doorvoergebied* is het land dat wordt gebruikt voor het transport van de goederen of mensen. *Servicegebied* is het land

[50] Zie bijvoorbeeld {Hall, 1999} en {Bryson, 1995, 87}.
[51] {Rosenthal e.a., 1996, 100}.
[52] {Albanese, 2002}.
[53] Kleemans en Paoli beredeneren dat de mate van vertrouwdheid en bekendheid met de sociale setting een belangrijke rol speelt bij de keuze van misdaadondernemers {Kleemans e.a., 2002, 77}, {Paoli, 2002, 66, 86}.
[54] {Williams, 1999}. Williams heeft in de beschikbare stukken de vier onderscheiden functies niet uitgewerkt. De uitwerking hier betreft dus een eigen interpretatie.

waar de misdaadonderneming de secundaire of ondersteunende activiteiten uitvoert. *Marktplaats* is de locatie waar de koop of verkoop wordt gesloten. *Opslag- of sorteergebied* is het land waar de misdaadonderneming de producten opslaat of sorteert.

De gelegenheidstheorie gaat uit van convergentie in tijd en plaats. Voor vermogenscriminaliteit speelt het tijdstip immers een rol. Overdag zijn er bijvoorbeeld meer mensen op straat. Tevens werken dan velen, waardoor een woninginbreker zijn slag kan slaan. 's Nachts daarentegen zijn er minder mensen op straat, meer mensen thuis, maar is de sociale controle minder intensief. Bij georganiseerde criminaliteit speelt het moment eigenlijk geen rol van betekenis. Het moment waarop de koop wordt gesloten, het tijdstip van het transport en dergelijke is eigenlijk niet van belang. Hooguit zouden we kunnen zeggen dat tijdsverschillen tussen landen het sluiten van transacties in de weg staan. Maar dit geldt niet echt voor de groothandel waar geen sprake is van impulsaankopen, maar juist van de aankoop van grote partijen. Wel mogen we aannemen dat het transport en de overslag van illegale goederen bij voorkeur 's nachts plaatsvinden om zo weinig mogelijk op te vallen. Maar ook dit vormt geen dominante factor. Kortom, het moment van de convergentie speelt geen rol van betekenis voor georganiseerde criminaliteit.

Samenvattend kunnen we het volgende stellen omtrent de gelegenheidsfactor locatie en tijd voor georganiseerde criminaliteit. De convergentie van a) illegale groothandelswaar, b) illegale groothandelsonderneming en c) ontoereikende sociale controle bepaalt of illegale groothandelsactiviteiten zich voordoen. Diverse factoren bepalen waar de convergentie ontstaat, namelijk: geografische, sociaal-culturele, economische, technologische, historische, juridische, tijdelijke en politieke factoren alsmede kenmerken van het criminele milieu. Voor een verkennende risicoanalyse kan men volstaan met een beoordeling van de voordelen en risico's van een land en de mate van vertrouwdheid en bekendheid met de sociale setting. Een andere optie is om specifiek te kijken naar functies die een land kan vervullen voor illegale groothandelsactiviteiten. Het tijdstip van de convergentie speelt geen rol van betekenis.

4.6. Typologie van veranderingen en dreigingen

Eerder zijn vijf soorten veranderingen onderscheiden op basis van de algemene gelegenheidsfactoren, namelijk in: a) doelwitten, b) daders, c) locaties, d) tijdstippen en e) criminaliteitsvormen.[55] De naam van de eerste twee gelegenheidsfactoren is gewijzigd. Daarom is ook een aanpassing nodig van de corresponderende soorten veranderingen. De nieuwe namen luiden: 'veranderingen in illegale groothandelswaar' en 'veranderingen in illegale groothandelsondernemingen'. Geconstateerd is dat het tijdstip voor georganiseerde criminaliteit geen rol van betekenis speelt. Daarom is een verandering in tijdstippen niet relevant en kan dit soort vervallen. Het soort 'veranderingen in criminaliteitsvormen' behoeft aanpassing. Georganiseerde criminaliteit omvat een veel breder spectrum dan vermogenscriminaliteit. Er kunnen bovendien (ogenschijnlijk) legale activiteiten onder vallen. In essentie gaat het om activiteiten in het kader van de illegale bedrijfsvoering. De nieuwe naam luidt daarom: 'veranderingen in de illegale bedrijfsvoering'.

[55] Zie figuur 1.2 in subparagraaf 1.2.2.

Naar analogie van doelwitten, kunnen we voor veranderingen in illegale groothandelswaar een onderscheid maken tussen nieuw, een toename of een verschuiving. Er is sprake van een verandering in illegale groothandelswaar wanneer als gevolg van één of meer ontwikkelingen er 1) een nieuw illegaal product ontstaat die geschikt is voor illegale groothandelsondernemingen, 2) het volume en/of de financiële omzet van bestaande illegale groothandelswaar op jaarbasis toeneemt of 3) het volume en/of de financiële omzet van bestaande illegale groothandelswaar op jaarbasis toeneemt ten koste van andere bestaande illegale groothandelswaar.

De tweede soort, 'veranderingen in illegale groothandelsondernemingen', behoeft enige uitwerking. Voor daders is eerder een onderscheid gemaakt naar nieuwe soorten daders, een toename van bestaande of een verschuiving. Niet duidelijk is echter wat een soort illegale groothandelsonderneming inhoudt. Kleemans e.a. (2002) introduceren drie soorten criminele samenwerkingsverbanden op grond van de aard ervan. Zij spreken over een lokale held die als generalist een bepaald gebied voorziet van illegale producten. Verder spreken zij over specialistische criminele samenwerkingsverbanden die zich toeleggen op bepaalde producten. Tot slot hebben zij het ook over generalistische samenwerkingsverbanden die zich richten op enkele producten.[56] De onderzoeksgroep Fijnaut benoemt enkele soorten criminele groepen in Nederland: 1) autochtone groepen, 2) allochtone groepen en 3) buitenlandse groepen. Bij de allochtone groepen gaat het om groepen waarvan de leden zijn genaturaliseerd. Voorbeelden daarvan zijn Turkse, Marokkaanse en Surinaamse criminelen. De buitenlandse groepen kunnen worden onderverdeeld naar de functie die Nederland voor hen vervult. De onderzoeksgroep Fijnaut maakt daarbij onderscheid naar: 1) groepen die Nederland gebruiken om hun goederen te verkopen, 2) groepen die Nederland gebruiken om goederen te kopen, 3) groepen die zich toeleggen op het smokkelen van en naar Nederland en 4) transnationale groepen die wel in Nederland opereren, maar voor wie de activiteiten in Nederland geen hoofdactiviteit vormen.[57] In bovenstaande onderverdelingen gaat het deels om de aard van de groep (bijvoorbeeld lokale held of smokkelorganisatie), de samenstelling (bijvoorbeeld autochtoon) of de functie van Nederland. Naast de genoemde onderverdelingen, is veel discussie gevoerd over de structuur van de criminele groep (et cetera).[58] Blijkbaar vindt men de structuur ook van belang als variabele. Denkbaar is ook om rekening te houden met de handelswaar waarin men handelt. Zo zouden we kunnen spreken van een drugshandelsonderneming of een mensensmokkelonderneming. Hetzelfde geldt voor aspecten van de bedrijfsvoering zoals eigendom van legale ondernemingen. Wanneer we op basis van de handelswaar en/of de bedrijfsvoering en/of de functie van Nederland een illegale groothandelsonderneming zouden typeren, dan overlapt dat met (veranderingen in) groothandelswaar, bedrijfsvoering en locatie. Daarom is daarvoor niet gekozen. De verwantschap in soort wordt dus bepaald door een overeenkomst in aard, samenstelling of structuur. Er is dus sprake van een 'verandering in illegale groothandelsondernemingen' wanneer als gevolg van één of meer ontwikkelingen er een wijziging optreedt in de aard, samenstelling of structuur van illegale groothandelsondernemingen. Een verdere verbijzondering is mogelijk naar een nieuwe soort, een toename van een bestaande soort of een verschuiving tussen soorten.

[56] {Kleemans e.a., 2002, 74-79}.
[57] {Enquêtecommissie, 1996B, 59-64, 146}, {Enquêtecommissie, 1996A, 36-42}.
[58] Zie paragraaf 3.2 en 3.3.

Ook voor veranderingen in de illegale bedrijfsvoering kunnen we, naar analogie van criminaliteitsvormen, een onderscheid maken tussen nieuw, een toename of een verschuiving. Het gaat in dit geval echter primair om wijzigingen in de werkwijze waardoor zich nieuwe vormen van criminaliteit, een toename of een verschuiving kunnen voordoen. Er is dus sprake van een verandering in de illegale bedrijfsvoering wanneer als gevolg van één of meer ontwikkelingen de werkwijze in de bedrijfsvoering van illegale groothandelsondernemingen wijzigt. Die wijzigingen kunnen we verbijzonderen voor de uitoefening van de groothandelsfuncties en de ondersteunende activiteiten.

De aanpassing voor veranderingen in locaties is minder eenvoudig. Beargumenteerd is dat illegale groothandelsactiviteiten in principe overal ter wereld kunnen plaatsvinden. Een ontwikkeling kan leiden tot wereldwijde veranderingen. Deze kunnen verschillen per soort groothandelsfunctie, type groothandelsonderneming, soort product, continent, land et cetera.[59] Het zou de precisie ten goede komen wanneer we al deze nuances zouden aanbrengen. We zouden echter door de bomen het bos niet meer zien. Tevens richt de analyse zich primair op de Nederlandse situatie.[60] Daarom is de keuze gemaakt om dergelijke veranderingen te beschouwen als een mogelijke verdieping van de andere veranderingen.

Soort verandering/ dreiging	**Mogelijke verdiepingen**
Illegale groothandels-waar	• Nieuwe soort illegale groothandelswaar • Toename handel in een bestaande soort illegale groothandelswaar (ten behoeve van bestaande of nieuwe afzetgebieden) • Verschuivingen tussen bestaande soorten handelswaar Deze veranderingen kunnen verder worden verbijzonderd voor de functies die Nederland vervult ten aanzien van de handelswaar (marktplaats, thuismarkt, doorvoer-, opslag- of sorteergebied)
Illegale groothandels-ondernemingen	• Nieuwe soort illegale groothandelsonderneming • Toename bestaande soort illegale groothandelsonderneming • Verschuivingen tussen bestaande soorten groothandelsondernemingen en/of andere misdaadondernemingen Deze veranderingen kunnen verder worden verbijzonderd voor de functies die Nederland vervult voor de ondernemingen (thuisbasis, marktplaats, thuismarkt, doorvoer- opslag-, sorteer- of servicegebied)
Illegale bedrijfsvoering	• Wijzigingen in de uitoefening van de groothandelsfuncties • Wijzigingen in de uitoefening van de ondersteunende (criminele) activiteiten Deze veranderingen *kunnen* worden verbijzonderd voor: a) Afzonderlijke groothandelsfuncties (kopen, verkopen, sorteren, opslaan, transporteren, financieren, het nemen van risico's en marktinformatie vergaren) b) Afzonderlijke ondersteunende (criminele) activiteiten c) Afzonderlijke facetten van de ondersteunende (criminele) activiteiten (logistiek proces, infrastructuur, middelen, financiën, materiekennis, -informatie en ervaring) d) Specifieke vormen van ondersteuning door bedrijven e) Knelpunten voor personele, informatieprocessen, financiële processen en afscherming f) De functies die Nederland vervult (marktplaats, thuismarkt, doorvoer-, opslag-, sorteer- of servicegebied)

Figuur 4.3 Typologie van veranderingen georganiseerde criminaliteit en dreigingen

[59] Zie paragraaf 4.5.
[60] Zie paragraaf 1.3.

In figuur 4.3 zijn op basis van bovenstaande redenering de soorten veranderingen weergegeven. Uiteraard zijn daartussen interacties mogelijk. Een verandering in handelswaar kan leiden tot veranderingen in illegale groothandelsondernemingen en de bedrijfsvoering. Een verandering in illegale groothandelsondernemingen kan resulteren in veranderingen in de illegale bedrijfsvoering en/of in de handelswaar. Een verandering in de illegale bedrijfsvoering kan op haar beurt leiden tot de twee andere soorten veranderingen. Deze samenhang, waarbij sprake is van een oorzaak-gevolgrelatie, wordt als één verandering beschouwd en krijgt de naam van de oorzakelijke verandering. Uit de naamgeving moet in elk geval blijken om welke soort verandering het gaat. Voorbeelden van namen zijn: 'handel in nucleair materiaal' (nieuwe handelswaar) of 'toename betrokkenheid van Nederlandse vrijeberoepsgroepen bij illegale bedrijfsvoering' (wijziging in illegale bedrijfsvoering). Doordat veranderingen het analyseobject vormen, zijn met de soorten veranderingen tevens soorten dreigingen gespecificeerd.

4.7. Analysekader waarschijnlijkheid

De mate van invloed die een ontwikkeling heeft op één of meer gelegenheidsfactoren, bepaalt de waarschijnlijkheid van de verandering. De gelegenheidsfactoren kunnen we daardoor ook gebruiken als risicofactoren. De achterliggende vraag daarbij is: hoe waarschijnlijk is het dat de dreiging zich voordoet?

Voor een verandering in illegale groothandelswaar is de achterliggende risicofactor primair de mate waarin de handelswaar geschikt is voor de illegale groothandel. De mate waarin illegale groothandelsondernemingen daarin willen en kunnen handelen en de mate waarin daarop sociale controle mogelijk is, vormen eveneens twee risicofactoren. De mate van geschiktheid van Nederland voor die handelswaar kunnen we aanvullend bezien als afzonderlijke risicofactor. Het gaat dan om een beoordeling van de voordelen en risico's van Nederland en de mate van vertrouwdheid en bekendheid met de sociale setting. Er zijn dus vier risicofactoren te onderkennen voor de dreiging 'veranderingen in illegale groothandelswaar' (zie figuur 4.4).

Voor een verandering in illegale groothandelsondernemingen geldt een soortgelijke redenering. Alleen gaat het nu primair om een specifieke soort illegale groothandelsonderneming. Ook daarvoor zijn vier risicofactoren te onderscheiden (zie figuur 4.4).

Voor veranderingen in de illegale bedrijfsvoering vormen de mate waarin andere mogelijkheden voor de bedrijfsvoering aantrekkelijk zijn, de primaire risicofactor. Verder gelden de overige risicofactoren ook hiervoor.

Soort dreiging	Risicofactoren
Illegale groothandels-waar	1. Mate waarin handelswaar geschikt is voor de illegale groothandel 2. Mate waarin misdaadondernemingen de functies van de groothandel voor hun rekening willen en kunnen nemen in de handelswaar 3. Mate waarin betrokkenen, de overheid en anderen onvoldoende maatregelen willen of kunnen treffen om de risico's voor groothandelsondernemingen zodanig hoog te maken dat zij afzien van de handel in de handelswaar 4. Mate waarin Nederland geschikt is voor (aspecten van) de uitoefening van de groothandelsfuncties in de handelswaar Eenzelfde verdieping is mogelijk als die is aangegeven in figuur 4.3.
Illegale groothandels-ondernemingen	1. Mate waarin een bepaalde soort misdaadonderneming de functies van de groothandel voor haar rekening wil en kan nemen 2. Mate waarin handelswaar geschikt is voor een bepaalde soort illegale groothandelsonderneming 3. Mate waarin betrokkenen, de overheid en anderen onvoldoende maatregelen willen of kunnen treffen om de risico's voor een bepaalde soort groothandelsonderneming zodanig hoog te maken dat zij afziet van de handel 4. Mate waarin Nederland geschikt is voor (aspecten van) de groothandelsactiviteiten van een bepaalde soort illegale groothandelsonderneming Eenzelfde verdieping is mogelijk als die is aangegeven in figuur 4.3.
Illegale bedrijfsvoering	1. Mate waarin andere mogelijkheden voor (aspecten van) de illegale bedrijfsvoering aantrekkelijk zijn voor illegale groothandelsondernemingen (voordelen, risico's, bekendheid met en toegankelijkheid sociale setting) 2. Mate waarin illegale groothandelsondernemingen die mogelijkheden willen en kunnen benutten 3. Mate waarin betrokkenen, de overheid en anderen onvoldoende maatregelen willen of kunnen treffen om de risico's voor de groothandelsondernemingen zodanig hoog te maken dat zij afzien van benutting van de mogelijkheden 4. Mate waarin Nederland geschikt is voor benutting van de mogelijkheden Eenzelfde verdieping is mogelijk als die is aangegeven in figuur 4.3.

Figuur 4.4 Risicofactoren per soort dreiging

4.8. Analysekader ongewenste effecten

4.8.1. Uitgangspunten

In de voorgaande paragrafen zijn soorten dreigingen en risicofactoren benoemd. Een onderdeel dat nu nog ontbreekt, is een kader voor de beoordeling van ongewenste effecten. Eerder is als eis gesteld dat het kader moet aangeven waar de grens ligt voor de analyse. Deels is die grensbepaling analytisch van aard, deels normatief. Allereerst komen enkele uitgangspunten aan bod die logischerwijze voortvloeien uit de voorafgaande hoofdstukken en paragrafen. Vervolgens komt de beleidsmatige context van georganiseerde criminaliteit aan bod (subparagraaf 4.8.2). Deze context kan immers inzicht geven in het normatieve kader dat de overheid hanteert. Vervolgens vindt een uitwerking plaats van de ongewenste effecten. Daarbij is gebruikgemaakt van beleidsdocumenten en literatuur (zie bijlage 1).

Eerder is gekozen om de ongewenste effecten te benoemen in termen van aangetaste belangen en niet in termen van kenmerken van bijvoorbeeld de daders of criminaliteitsvormen.[61] Dit is het *eerste uitgangspunt*.

Illegale groothandelsactiviteiten kunnen we vanuit uiteenlopende invalshoeken beschouwen en dus ook de ongewenste effecten ervan. En, hoewel een dode een dode is, is het wel belangrijk om in de analyse duidelijk te maken als gevolg waarvan die dode is gevallen. Is dat een gevolg van de handelswaar of een gevolg van de illegale bedrijfsvoering? Eerder is een onderscheid aangebracht tussen drie soorten veranderingen. Op grond daarvan ligt het voor de hand om op zijn minst afzonderlijk te kijken naar de ongewenste effecten van de illegale groothandelswaar, de illegale groothandelsondernemingen en de illegale bedrijfsvoering. Het *tweede uitgangspunt* is daarom dat afzonderlijk voor de groothandelswaar, de ondernemingen en de bedrijfsvoering de ongewenste effecten moeten worden bepaald. Omdat veranderingen het analyseobject vormen van dit proefschrift, gaat het om de ongewenste effecten van de veranderingen daarin: het *derde uitgangspunt*.

Voor de illegale bedrijfsvoering is niet op voorhand duidelijk wanneer de gevolgen analytisch vallen onder de ongewenste effecten. Sommigen noemen (o.a.) corruptie, aantasting van de integriteit of de opbouw van een machtspositie als ongewenste effecten. Het gaat hier echter om drie totaal verschillende soorten effecten. Corruptie kan soms onvermijdelijk zijn. Het is zowel instrumenteel voor de handel als een gevolg daarvan. Corruptie heeft daarmee dus een causale én een doel-middel-relatie (finale relatie). Aantasting van de integriteit en een machtspositie zijn daarentegen niet instrumenteel, maar kunnen wel een gevolg zijn van de activiteiten van een misdaadonderneming.

Het *vierde uitgangspunt* is dat gevolgen die een finale relatie hebben met de illegale groothandelsactiviteiten níét behoren tot de ongewenste effecten. Deze behoren tot de illegale bedrijfsvoering en daarmee tot georganiseerde criminaliteit. Witwassen en corruptie, twee voorbeelden daarvan, zijn dus geen ongewenste effecten. Activiteiten en/of aspecten die wel het gevolg, maar niet instrumenteel zijn, behoren wel tot de ongewenste effecten. De integriteitaantasting is daarom een ongewenst effect. Bij een machtspositie is niet duidelijk welke belangen in het geding zijn. Niet helder is of dit bijvoorbeeld resulteert in verstoring van de marktwerking, prijsopdrijving van onroerend goed en dergelijke. Een machtspositie voldoet dus niet aan het eerste uitgangspunt. De gevolgen daarvan kunnen we wel weer beschouwen als ongewenst effect. Een machtspositie is dan als het ware een tussenvariabele. Soortgelijke argumenten gelden voor het crimineel verdiende geld en/of de besteding ervan, soms afzonderlijk genoemd als ongewenst effect. De achterliggende gedachte is dat criminaliteit niet lonend mag zijn. Het verdienen van geld vormt echter de primaire drijfveer evenals het besteden of investeren daarvan. Wanneer je geld verdient dat je niet kunt uitgeven, heb je er niets aan. Ook de besteding of investering van crimineel verdiend geld vormt daarmee een doel. Bovendien is het een middel om als groothandel te kunnen functioneren. Daarom zijn noch het geld zelf, noch de besteding ervan ongewenste effecten. De gevolgen daarvan, zoals prijsopdrijving van onroerend goed, vallen er daarentegen wel onder. Deze staan immers niet in een doel-middel-relatie tot de illegale groothandelsactiviteiten. Betrokkenheid van vrije beroepsgroepen, zoals advocaten, notarissen en accountants, beschouwt men ook regelmatig als ongewenst effect. Die

[61] Zie subparagraaf 1.2.2.

betrokkenheid is echter instrumenteel voor de illegale groothandelsactiviteiten en een rechtstreeks gevolg daarvan. De betrokkenheid is dus analytisch gezien geen ongewenst effect. De effecten van die betrokkenheid, zoals aantasting van de integriteit van die beroepsgroepen, behoren er wel toe.

Het *vijfde uitgangspunt* is dat het gaat om de ongewenste effecten voor de Nederlandse samenleving op macroniveau. Op grond van het eerste uitgangspunt gaat het dan om de aantasting van Nederlandse belangen. Deze moeten voortkomen uit illegale groothandels-activiteiten die in of vanuit Nederland plaatsvinden.[62] Daarbij wordt geen onderscheid gemaakt naar specifieke belanghebbenden zoals de financiële sector of de overheid. Bij de beoordeling speelt het internationale karakter van georganiseerde criminaliteit ons parten. Bijvoorbeeld voor de drugshandel fungeert Nederland als een transitoland. Leidt dit tot ongewenste effecten voor Nederland als de drugs Nederland niet inkomen? Een keuze is normatief van aard en hangt mede af van de belangen die we in ogenschouw willen nemen. Deze variëren naargelang de functies die Nederland vervult voor illegale groothandels-ondernemingen.

Sociale controle brengt kosten met zich mee. Zo moeten banken kosten maken om transacties te beoordelen aan de hand van de Wet Melding Ongebruikelijke Transacties. Toezicht en opsporing kunnen ook leiden tot een beperking van de grondrechten van individuen, zoals het recht op privacy. Deze gevolgen van sociale controle vallen analytisch niet onder de ongewenste effecten, maar onder de kosten van risicobeheersing.[63] Wanneer een verandering leidt tot minder mogelijkheden voor sociale controle, is analytisch evenmin sprake van een ongewenst effect. Sociale controle is immers één van de risicofactoren die meespeelt in de beoordeling van de component waarschijnlijkheid van de dreiging. Het *zesde uitgangspunt* is dus dat de kosten van sociale controle en/of negatieve gevolgen van veranderingen daarvoor, niet vallen onder de ongewenste effecten.

Uitgangspunten zijn dus:
1. Als meeteenheid voor ongewenste effecten fungeert de aantasting van belangen.
2. De ongewenste effecten moeten afzonderlijk worden bepaald voor de illegale groothandelswaar, de illegale groothandelsondernemingen en de illegale bedrijfs-voering.
3. Het gaat om de ongewenste effecten van veranderingen.
4. Gevolgen die een finale relatie hebben met de illegale groothandelsactiviteiten vallen niet onder de ongewenste effecten.
5. Het gaat om de ongewenste effecten voor de Nederlandse samenleving op macroni-veau.
6. De kosten van en gevolgen voor sociale controle vallen analytisch niet onder de ongewenste effecten.

4.8.2. Beleidsmatige en normatieve context georganiseerde criminaliteit

De aandacht van de Nederlandse politie, overheid en politiek voor georganiseerde criminaliteit is niet nieuw. De jaren zeventig kenmerkten zich door een ontwakende politie.

[62] Zie paragraaf 1.3. Hier is georganiseerde criminaliteit vervangen door 'illegale groothandelsactiviteiten' omdat dit, op basis van het gehanteerde concept van georganiseerde criminaliteit, beter de essentie aangeeft.
[63] Zie paragraaf 2.2.

De politie constateerde toen veranderingen in het criminele milieu. In de jaren tachtig zetten die veranderingen door en ontstond een toenemende bezorgdheid over georganiseerde criminaliteit. De eerste beleidsstukken verschenen in de tweede helft van de jaren tachtig. In de jaren negentig stond georganiseerde criminaliteit volop op de politieke agenda. Naast aandacht voor repressie kreeg ook preventie toenemende aandacht. In plaats van over bestrijding sprak men toen in toenemende mate over beheersing.[64] Tot veel concrete maatregelen leidde de preventiegedachte niet. Dit in tegenstelling tot repressie waar uiteindelijk de IRT-affaire uit voortkwam. Na het onderzoek van de Parlementaire Enquêtecommissie onder leiding van Van Traa ontstond een nieuwe periode waarin vooral de strafvorderlijke waarborgen op de voorgrond kwamen te staan. Tijdens de regeringsperiode van het kabinet-Kok II en van de kabinetten-Balkenende I en II verschoof de aandacht weer naar het boeken van vooral repressieve resultaten.

Vooral begin jaren negentig stond georganiseerde criminaliteit hoog op de politieke agenda en zijn vele beleidsstukken geschreven. Het IPIT heeft in 1996 een studie verricht naar het landelijke criminaliteitsbeleid over de jaren 1992-1996. De onderzoekers constateerden dat er in die periode maar weinig doelen en doelstellingen voor het beleid ter bestrijding van georganiseerde criminaliteit zijn geformuleerd. Voorzover er doelen af te leiden zijn, waren die gericht op het voorkomen dat georganiseerde criminaliteit zou infiltreren in de bovenwereld. Een instrumenteel doel was om het crimineel verdiende geld zoveel mogelijk te ontnemen.[65] De beleidsmakers benoemden in die tijd enkele zorgelijke kwesties, zoals de grote sommen crimineel geld, invloed op de overheid via corruptie, invloed op economische sectoren, symbiose tussen bovenwereld en onderwereld en betrokkenheid van vitale beroepsgroepen zoals advocaten en het internationale karakter van georganiseerde criminaliteit.[66]

Het kabinet-Kok II heeft in de periode 1998-2002 drie beleidsdocumenten geproduceerd als beleidskaders voor de beheersing van criminaliteit. In het eerste document, het 'Beleidsplan Nederlandse Politie 1999-2002', is als doelstelling voor georganiseerde criminaliteit genoemd:

> *"Nederland moet onaantrekkelijk zijn om criminele activiteiten te ontplooien. Dit wordt bewerkstelligd door een hoge pakkans een lage opbrengst van criminele activiteiten en geen mogelijkheden voor criminele organisaties om te infiltreren in de legale economie."*[67]

Deze doelstelling is niet verder geoperationaliseerd. In het tweede beleidsdocument, het integrale veiligheidsprogramma uit 1999, komt georganiseerde criminaliteit niet aan de orde. Vanuit de rol die georganiseerde criminaliteit vervult in misdaadmarkten, is dit opmerkelijk en een gemiste kans. In het derde beleidsdocument, de nota Criminaliteitsbeheersing uit 2001, staat het kabinet-Kok II weer wel stil bij georganiseerde criminaliteit. Het kabinet constateert dat het met de beheersing ervan niet goed gaat. Er is bijvoorbeeld te weinig capaciteit en op landelijk niveau is de recherche niet goed georganiseerd. Een inhoudelijke probleemschets ontbreekt. Wel stelt het kabinet dat georganiseerde

[64] {Klerks, 2000, 97-134}, {Parlementaire Enquêtecommissie, 1996B, 12-22}.
[65] {Van der Leest & Bruinsma, 1996, 49}.
[66] Ontleend aan {Klerks, 2000, 97-134}, {Parlementaire Enquêtecommissie, 1996B, 12-22}.
[67] {Ministerie BZK, 1998, 15}.

criminaliteit een permanente dreiging vormt voor de integriteit van de samenleving, nationaal en internationaal. Besteding van misdaadgeld benoemt het kabinet als een bedreiging voor de integriteit van de legale economie. Een onderbouwing en uitwerking hiervan zijn niet gegeven. Expliciete en concrete inhoudelijke doelstellingen ontbreken.[68]

In het Veiligheidsprogramma 'Naar een veiliger samenleving' van het kabinet-Balkenende I, komt georganiseerde criminaliteit éénmaal voor. En die ene keer staat het woord georganiseerd ook nog eens tussen haakjes. Wel stelt het kabinet ingrijpende maatregelen voor om de landelijke recherche, die zich grotendeels bezighoudt met de bestrijding van georganiseerde criminaliteit, anders te organiseren.

Uit de beleidsdocumenten van diverse kabinetten uit de afgelopen jaren kunnen we dus niet tot nauwelijks ongewenste effecten afleiden die voldoen aan de geformuleerde analytische uitgangspunten. In hoeverre noemen anderen die direct zijn gelieerd aan de politiek of overheid die wel? De Parlementaire Enquêtecommissie (1996) gaat in haar conclusies summier in op de ernst van georganiseerde criminaliteit.

> *"De ernst van de georganiseerde criminaliteit is vooral gelegen in het grote illegale gewin van honderden miljoenen guldens, de economische macht die daaruit voortkomt. [….] Daarnaast speelt schade in andere opzichten een rol. In delen van Amsterdam en Arnhem dreigt de georganiseerde criminaliteit te veel macht in bepaalde wijken te krijgen. [….] Tevens dient veel meer aandacht te worden besteed aan georganiseerde criminaliteit binnen etnische groepen, die een desastreuze uitwerking kan hebben op de maatschappelijke positie van minderheden in onze samenleving."*[69]

Deze conclusie lijkt te zijn gebaseerd op door de onderzoeksgroep Fijnaut genoemde zorgelijke kwesties.[70] Van een echt structurele analyse van ongewenste effecten is geen sprake geweest.

De vergadering van Procureurs-generaal (PG's) heeft in 1996 criteria geformuleerd voor de prioriteitstelling van opsporingsonderzoek naar georganiseerde criminaliteit. De basis hiervoor zijn de schadelijke effecten van specifieke criminele groepen (zie figuur 4.5). In de beleidsnota 'Perspectief op 2006' van het Openbaar Ministerie uit 2002 staat het woord georganiseerde misdaad viermaal genoemd. Een keer is het gebruikt bij wijze van voorbeeld. Tweemaal komt het voor omdat het OM vindt dat het beeld van georganiseerde criminaliteit niet toereikend is. De vierde keer wordt het genoemd om aan te geven dat meer samenhang moet komen in de aanpak ervan.[71] Hoewel deze nota het beleidskader voor het Openbaar Ministerie én voor de aansturing van de politie vormt, ontbreken hierin doelstellingen voor de beheersing van georganiseerde criminaliteit en een specificatie van de ongewenste effecten.

Het interdisciplinaire CriminaliteitsOverleg (ICO) van het ressort 's-Gravenhage kwam in 1998 met een indeling voor maatschappelijke gevolgen van specifieke criminele groepen.

[68] {Integraal Veiligheidsprogramma, 1999}, {Criminaliteitsbeheersing, 2001, 32}.
[69] {Enquêtecommissie, 1996A, 419}.
[70] {Enquêtecommissie, 1996B, 146-151}.
[71] {Ministerie van Justitie, 2002}, {Openbaar Ministerie, 2002}.

Een veertiental criteria is hiervoor ontwikkeld. De criteria worden onderverdeeld in drie categorieën, die onderling een verschillend gewicht hebben (zie figuur 4.5).

Instantie	Doel	Criteria
Vergadering Procureurs-Generaal	Prioriteitstelling van opsporingsonderzoek door kernteams op basis van de schadelijke effecten van specifieke criminele groepen	Hoofdcategorieën zijn: 1) aantasting van de integriteit van lijf en goed of de persoonlijke/zakelijke levenssfeer, 2) geldelijk gewin en geldelijke doorwerking, 3) uitwerking op overheden, 4) uitwerking op legale markten, 5) tegenstrategieën en 6) internationaal actief zijn van de criminele groepering of het netwerk. Binnen de hoofdcategorieën is een nadere onderverdeling aangebracht.
Interdisciplinaire Criminaliteits Overleg van het ressort 's-Gravenhage (ICO)	De beoordeling van de maatschappelijke gevolgen van specifieke criminele groepen ten behoeve van de prioriteitstelling van opsporingsonderzoek op ressortelijk niveau	De (veertien) criteria zijn onderverdeeld in drie groepen, die onderling een verschillend gewicht hebben: • Groep 1: psychische/fysieke schade buiten het criminele milieu, bedreiging van de volksgezondheid, aantasting van de bestuurlijke integriteit (de overheid en haar organen) en actieve belemmering van de overheid bij het uitvoeren van haar controlerende en opsporende taak. • Groep 2: psychische/fysieke schade binnen het criminele milieu, bedreiging van het milieu, aantasting van de integriteit van dienstverleners en openbaar ambtsdragers, passieve belemmering van de overheid bij het uitvoeren van haar controlerende en opsporende taak, negatieve gevolgen voor de (lokale) gemeenschap en verstoring marktwerking. • Groep 3: schade aan eigendom, materiële schade voor de overheid, aantasting van de integriteit van maatschappelijke organisaties en het aantal strafbare feiten of de frequentie hiervan.

Figuur 4.5 Gehanteerde criteria voor prioritering opsporingsonderzoeken naar georganiseerde criminaliteit[72]

In de uitwerkingen van de vergadering van PG's en het ICO is het onderscheid tussen kenmerken van de bedrijfsvoering en ongewenste effecten lang niet altijd duidelijk. De hoofdcategorieën 'tegenstrategieën' en 'internationaal actief zijn' zijn duidelijk kenmerken van de bedrijfsvoering. Dit geldt (in elk geval) ook voor 'het aantal strafbare feiten of de frequentie hiervan' in de indeling van het ICO. De achterliggende gedachte is dat deze kenmerken van de bedrijfsvoering überhaupt ongewenst zijn. Er is bovendien geen onderscheid aangebracht naar de bron van de ongewenste effecten. Bijvoorbeeld de 'aantasting van de integriteit van lijf en goed' kan voortkomen uit de aard van de illegale dienst, zoals bij mensenhandel. Het kan ook het gevolg zijn van de bedrijfsvoering, bijvoorbeeld bij toepassing van geweld ter naleving van afspraken. Bovendien zijn de criteria toegespitst op specifieke criminele groepen en niet op georganiseerde criminaliteit als geheel. Een specifieke groep kan zich op zeer gewelddadige wijze bezighouden met mensensmokkel, terwijl dit geen kenmerk hoeft te zijn van mensensmokkel als zodanig. Overigens zijn de genoemde criteria met enige creativiteit wel toepasbaar voor georgani-

[72] Zie {Holthuis, 1996} en {Kernteam Noord- en Oost-Nederland, 2001, 147-154}, voor de criteria van de vergadering van PG's en {Pols & Visser, 1998} voor de andere criteria

seerde criminaliteit als geheel.[73] Tot slot maakt men onderscheid wie schade lijdt of de gevolgen ondervindt, bijvoorbeeld de overheid of dienstverleners. In de uitwerking van het ICO gaat niet alleen om een analytisch, maar ook om een normatieve verbijzondering. Aantasting van de bestuurlijke integriteit weegt men bijvoorbeeld zwaarder dan aantasting van de integriteit van dienstverlenende beroepsgroepen en openbare ambtsdragers.

In het in 1997 ontwikkelde 'Referentiekader resultaten politiewerk' zijn vier resultaatgebieden benoemd: veiligheid, leefbaarheid, maatschappelijke integriteit en kwaliteit van de dienstverlening. Het referentiekader is primair gericht op het meten van de resultaten van het politiewerk in plaats van op beleidsvorming en -uitvoering. Het referentiekader gaat niet specifiek in op de belangen die in het geding zijn. Desondanks geeft het wel een beeld van de impliciete doelstellingen voor en van de politie. Bovendien is dit kader door de politiedepartementen omarmd. De beheersing van georganiseerde criminaliteit valt alléén onder het resultaatgebied Maatschappelijke integriteit.[74] Men rekent dus georganiseerde criminaliteit niet tot het resultaatgebied veiligheid of leefbaarheid.

De beleidsdocumenten uit de afgelopen jaren van de kabinetten en het Openbaar Ministerie blinken dus niet uit in helderheid over de doelstellingen van het beleid. Voorzover deze al worden genoemd, is niet expliciet gemaakt op welke probleemschets en/of normen deze zijn gebaseerd. Evenmin wekt de formulering de indruk dat sprake is van een expliciete visie op de beheersing ervan en/of de ongewenste effecten die men wenst te vermijden. De vergadering van PG's en het ressort 's-Gravenhage hebben daarentegen wel criteria geformuleerd voor de prioriteitstelling van opsporingsonderzoeken. Hoewel men daarmee beoogt om prioriteiten te stellen op basis van de schadelijke effecten voor de samenleving, hanteert men ook kenmerken van de criminele groep als criterium. De belangen die in het geding zijn, zijn niet expliciet geformuleerd. Verder maakt men geen expliciet onderscheid tussen de ongewenste effecten van de illegale groothandelswaar, de illegale groothandelsonderneming en de illegale bedrijfsvoering. Het object van de beoordeling is de criminele groep, hier aangeduid als misdaadonderneming. De bestudeerde beleidsdocumenten en criteria bieden al met al geen geschikt kader voor de beoordeling van ongewenste effecten van dreigingen. Evenmin kunnen objectieve gewichten voor de afzonderlijke belangen of ongewenste effecten worden gedestilleerd uit de bestudeerde stukken.

4.8.3. Kader voor ongewenste effecten

In de voorgaande subparagrafen zijn ongewenste effecten de revue gepasseerd. Enkele van de in beleidsstukken of literatuur genoemde effecten vallen af op grond van de gehanteerde uitgangspunten.[75] Het uitgangspunt is dat de ongewenste effecten afzonderlijk moeten worden bepaald voor illegale groothandelswaar, illegale groothandelsondernemingen en de illegale bedrijfsvoering.

In enkele van de beschreven uitwerkingen worden in meer of mindere mate ook de *ongewenste effecten van de illegale groothandelswaar* apart beschouwd.[76] Zo beoordeelt

[73] Zie hiervoor bijvoorbeeld {Kernteam Noord- en Oost-Nederland, 2001, 147-154}. De onderzoekers passen de criteria van de vergadering van PG's toe op criminaliteitsvelden, in dit proefschrift aangeduid als misdaadmarkten.
[74] {Jansonius & Kuiper, 1997, 40-48}.
[75] Zie hiervoor subparagraaf 4.8.2 en bijlage 1.
[76] Dit geldt voor de systematiek van de vergadering van PG's, het interdisciplinaire criminaliteitsoverleg, de National Crime Authority, Maltz en Klerks (zie bijlage 1).

men de gezondheidseffecten, de effecten voor het milieu of de kosten van diefstal van goederen. Voor zover de aangehaalde beleidsdocumenten van uiteenlopende kabinetten al iets zeggen over ongewenste effecten, noemen zij de effecten van de producten daarentegen niet. Ook de Parlementaire Enquêtecommissie noemt die niet.[77]

Illegale producten kunnen zelf schadelijk zijn of een object zijn voor criminaliteit. Voor verboden producten geldt dat de wetgever deze op zichzelf schadelijk acht, bijvoorbeeld voor de gezondheid in het geval van drugs. Voor streng gereguleerde producten geldt dat de wetgever deze in beperkte mate en onder voorwaarden voor specifieke doelgroepen toestaat. Deze producten zijn dus niet voor iedereen of in alle gevallen als schadelijk gekwalificeerd. Vervalste of gemanipuleerde goederen kunnen in enkele gevallen schadelijk zijn. Dat is bijvoorbeeld het geval bij vervalste vliegtuigonderdelen. Bij een vervalste cd of een nagemaakt merkkledingstuk is dat veel minder aan de orde. Bij gestolen goederen zijn de producten zelf niet schadelijk. Het verdient de voorkeur om de ongewenste effecten van de afzonderlijke illegale producten te bepalen. In het kader van dit proefschrift voert het te ver om deze van alle geschikte groothandelswaar in kaart te brengen. Volstaan wordt met het cluster ‘productgerelateerde aantasting van belangen’.

De uitoefening van de groothandelsfuncties kan eveneens resulteren in ongewenste effecten. Daarbij moeten we een onderscheid maken tussen de groothandelsactiviteiten zelf en de afname en levering van die producten van/aan anderen in misdaadmarkten. De handel zelf leidt niet tot ongewenste effecten. Een illegale groothandelsonderneming levert immers niet rechtstreeks aan eindconsumenten. Schadelijke effecten bij hen, bijvoorbeeld bij drugsverslaafden, zijn niet direct aan de groothandel toe te rekenen. Evenmin produceren zij zelf verboden goederen, stelen, vervalsen of manipuleren zij goederen. De schade die bijvoorbeeld softwareproducenten lijden als gevolg van illegale kopieën, of de schade bij slachtoffers van autodiefstal zijn niet direct op het conto van de groothandel te schrijven. Desondanks geldt natuurlijk wel dat de illegale groothandel die producten afneemt en weer aan anderen levert. Zonder die rol zouden anderen wellicht niet kunnen functioneren in misdaadmarkten. De stimulans van de groothandel op andere criminelen is niet geformuleerd in termen van belangen. Wel kunnen we spreken van ‘aantasting van de veiligheid’ en ‘afname van de leefbaarheid’.[78] Deze twee categorieën samen vormen een afzonderlijke cluster van ongewenste effecten genaamd: ‘aantasting veiligheid en leefbaarheid’. Analytisch bestaat er geen aanleiding om deze effecten verder uit te werken. Het gaat immers om indirecte effecten. Deze keuze is normatief van aard.

Een uitzondering op bovenstaand betoog is de groothandel in producten die fungeren als instrument voor misbruik van invoer- en uitvoerregelgeving. Bij deze producten vloeien juist uit de koop, de verkoop, de opslag en het transport de ongewenste effecten voort. Tijdens deze activiteiten misbruikt de groothandel immers de fiscale regelgeving hetgeen de illegale winst genereert. De ongewenste effecten hiervan zijn bijvoorbeeld inkomstenderving bij de overheid en te hoge uitgaven bij de overheid (aantasting van economische belangen). Bovendien kunnen de groothandelsactiviteiten ook anderen in misdaadmarkten stimuleren tot criminaliteit.

[77] Zie subparagraaf 4.8.2.

[78] Het ‘Referentiekader resultaten politiewerk’ hanteert deze indeling voor allerlei criminaliteitsvormen en inspanningen van de politie. De indeling is in dat referentiekader niet gehanteerd voor de beoordeling van ongewenste effecten, maar leent zich daar in beginsel wel voor.

De uitoefening van de groothandelsfuncties gaat tevens gepaard met secundaire activiteiten. Veelal gaat het daarbij om criminele activiteiten. In potentie is het gehele Wetboek van Strafrecht daarop van toepassing. Het specificeren van de ongewenste effecten van de secundaire criminaliteit is daardoor in algemene zin niet zinvol. Volstaan wordt met de categorieën 'aantasting van de veiligheid' en 'afname van de leefbaarheid'. Ook hier is een normatieve keuze nodig in hoeverre deze effecten toe te rekenen zijn aan de illegale groothandelsactiviteiten.

De *ongewenste effecten van illegale groothandelsondernemingen* bestaan uit de combinatie van de effecten van de handelswaar en de bedrijfsvoering (zie hiervoor en hierna). De aard, samenstelling of structuur van de onderneming[79] bepalen weliswaar voor een deel de handelswaar waarin men handelt en de opzet van de bedrijfsvoering, maar resulteren niet zelfstandig in ongewenste effecten. Bovendien gaat het daarbij om kenmerken van de onderneming en deze vormen niet het uitgangspunt om ongewenste effecten van af te leiden.[80] Wanneer dus bepaalde etnisch samengestelde criminele groepen sneller geneigd zijn om geweld te gebruiken, dan zijn de ongewenste effecten daarvan een onderdeel van de ongewenste effecten van de illegale bedrijfsvoering.

In enkele van de bestudeerde uitwerkingen beoordeelt men de schadelijke/maatschappelijke gevolgen van de criminele groep/ crimineel samenwerkingsverband, hier aangeduid als illegale groothandelsonderneming. Die keuze houdt verband met het doel waarvoor men de uitwerking gebruikt, namelijk voor de prioritering van opsporingsonderzoeken. Men maakt daarbij geen expliciet onderscheid tussen de handelswaar en aspecten van de bedrijfsvoering.[81] In dit proefschrift is de voorkeur gegeven aan wel een expliciet onderscheid op grond van de eerdergenoemde argumenten.

De *ongewenste effecten van de illegale bedrijfsvoering* komen in de bestudeerde beleidsdocumenten en literatuur in meer of mindere mate aan bod. In enkele gevallen gaat de aandacht daarbij vooral uit naar specifieke activiteiten, zoals corruptie, samenwerking met legale bedrijven en dergelijke, in plaats van naar ongewenste effecten.[82] Analytisch moeten we afzonderlijk kijken naar de uitoefening van de groothandelsfuncties en de ondersteunende (criminele) activiteiten. Het eerste aspect is hiervoor reeds uitgewerkt. De ondersteunende (criminele) activiteiten resulteren eveneens in allerlei ongewenste effecten. Een voorbeeld daarvan is de aantasting van de integriteit van de overheid om de criminele activiteiten af te schermen. Vanuit het personeelsbeheer kunnen (criminele) activiteiten voortkomen, zoals het (dreigen met het) gebruik van geweld. Dit kan leiden tot fysieke en psychologische schade. Omdat we dergelijke criminele activiteiten beoordelen op de uitwerking voor de Nederlandse samenleving, kunnen we volstaan met de reeds benoemde categorieën 'aantasting veiligheid' en 'afname leefbaarheid'. Een ander element van het personeelsbeheer is dat de misdaadondernemer sociale relaties betrekt bij de criminele handel en wandel. Hierdoor kunnen bepaalde bevolkingsgroepen meer dan gemiddeld betrokken raken bij georganiseerde criminaliteit. Dit kan nadelige gevolgen hebben voor de integratie en de acceptatie van die groepen. Ten behoeve van geldbeheer is witwassen

[79] Dit zijn de aspecten waarnaar wordt gekeken of sprake is van een verandering (zie paragraaf 4.6).
[80] Zie hiervoor het eerste uitgangspunt in subparagraaf 4.8.1.
[81] Dit geldt voor de uitwerking van de vergadering van PG's, ICO en Klerks {Holthuis, 1996}, {Kernteam Noord- en Oost-Nederland, 2001}, {Pols & Visser, 1998}, {Klerks, 2000}. Zij spreken overigens over criminele groep.
[82] Dit geldt voor de beleidsdocumenten en de uitwerking van de vergadering van PG's, ICO, National Crime Authority, Maltz en Klerks (zie subparagraaf 4.8.2 en bijlage 1).

onontkoombaar. Witwassen kan leiden tot aantasting van de integriteit van het financiële stelsel en verstoring van de marktwerking. Bij sommige misdaadondernemingen maken offensieve vormen van afscherming onderdeel uit van de bedrijfsvoering. Dit kan leiden tot vooral aantasting van de integriteit van de overheid. Deze ongewenste effecten zijn te clusteren tot: 'aantasting van economische belangen' en 'aantasting van maatschappelijke belangen'.

In deze subparagraaf zijn dus enkele soorten ongewenste effecten benoemd:
1. Productgerelateerde aantasting van belangen.
2. Aantasting veiligheid en leefbaarheid.
   - Aantasting veiligheid.
   - Afname leefbaarheid.
3. Aantasting van economische belangen.
   - Financieel verlies (minder inkomsten, meer uitgaven).
   - Verstoring van de marktwerking.
4. Aantasting van maatschappelijke belangen.
   - Aantasting integriteit overheid.
   - Aantasting maatschappelijke positie minderheden.
   - Aantasting integriteit financiële stelsel.

Het gaat hierbij niet om een limitatieve opsomming. Daarvoor zijn een uitputtende analyse en een normatieve standpuntbepaling vereist.

5. ICT-ontwikkelingen

5.1. Inleiding

In de voorgaande drie hoofdstukken is het risicoanalyse-instrumentarium uitgewerkt. Hier start de tweede component van het proefschrift, namelijk de toepassing ervan op de ICT-ontwikkelingen. Dit hoofdstuk analyseert die ontwikkelingen. Het volgende hoofdstuk beschrijft de risico's van veranderingen in georganiseerde criminaliteit die daar uit voortkomen.

Technologische innovaties uit het verleden, zoals de uitvinding van de stoommachine, hebben grote invloed gehad op de samenleving van toen. De samenleving van nu zou er bovendien heel anders hebben uitgezien zonder deze vernieuwingen. De afgelopen jaren heeft de informatiecommunicatietechnologie (ICT) zich in een snel tempo ontwikkeld. Men spreekt zelfs over een ICT-revolutie.[1] Technologische innovaties creëren nieuwe mogelijkheden voor het bedrijfsleven, de overheid, de politie en de burgers. Zij hebben echter tevens een schaduwzijde. Ook criminelen kunnen immers profiteren.

Diverse auteurs bestuderen de invloed van de ICT-innovatie op de samenleving. Zij hanteren daarbij uiteenlopende invalshoeken en concepten. Sommigen zijn van mening dat we ons bevinden in een transformatie van een industriële naar een informatiesamenleving.[2] Anderen spreken, al dan niet in combinatie met andere ontwikkelingen, over nieuwe economie,[3] netwerksamenleving,[4] informatie-economie[5], kenniseconomie[6], interneteconomie[7] of informatietijdperk[8].

In dit proefschrift ligt het accent op de interactie tussen de ICT-innovatie en veranderingen in de samenleving als gevolg daarvan. Het begrip 'ICT-innovatie' is gereserveerd voor de technische kant van de ontwikkelingen, zoals de toename van de capaciteit van geheugenchips. Paragraaf 5.2 beschrijft de innovatie. Het begrip 'ICT-ontwikkelingen' wordt daarentegen gebruikt als verzamelbegrip voor de interactie tussen de ICT-innovatie en de veranderingen in de samenleving (en vice versa). Paragraaf 5.3 gaat daar nader op in. Paragraaf 5.4 benoemt vier kenmerken van de ICT-ontwikkelingen. Die kenmerken vormen de basis voor de identificatie van dreigingen in hoofdstuk 6. De ICT-ontwikkelingen hebben enkele gevolgen voor legale bedrijven (paragraaf 5.5) en sociale controle (paragraaf 5.6). Hoewel ICT, informatie en de virtuele ruimte vele nieuwe mogelijkheden in zich hebben, bestaan er toch ook beperkingen. Paragraaf 5.7 beschrijft deze. Inzicht in de gevolgen voor legale bedrijven en sociale controle en de beperkingen zijn van belang voor de onderbouwing van de waarschijnlijkheid van de dreigingen (zie hoofdstuk 6). Paragraaf 5.8 geeft tot slot een overzicht van de bevindingen.

---

[1] {Castells, 1998A, 60-65}, {Infodrome, 2001}.
[2] {Commissie ICT en overheid, 2001}, {Infodrome, 2000}, {Infodrome, 2001}, {Ministerie van Justitie, 1998, 4}, {Castells, 1998A}.
[3] {Soete, 1999}, {Herings & Schinkel, 2000}, {Bartelsman & Hinloopen, 2000}, {Strikwerda, 2001}, {Vuijsje, 2000}, {Lof, 2001}.
[4] {Castells, 1998A}, {Pieper, 2000}.
[5] {Meijers, 2000}.
[6] {Infodrome, 2000, 9}.
[7] {University Texas, 2000}.
[8] {Castells, 1998A}, {Castells, 1998B}.

5.2. ICT-innovatie

Sommigen zijn van mening dat we ons bevinden in een transformatie van een industriële naar een informatiesamenleving. De uitvinding van de stoommachine en nieuwe energievormen in de achttiende eeuw resulteerden in een industriële samenleving. De ICT-innovatie heeft op haar beurt een revolutie tot stand gebracht en leidt tot het ontstaan van een informatiesamenleving.[9] Spreekt men bij de industriële samenleving over industrialisering, nu spreekt men over digitalisering. Soms rekent men ook biotechnologie of genetica daartoe of nog ruimer ook kennistechnologie.[10] Omdat het daarbij gaat om andersoortige technologieën met andere effecten, worden deze in dit proefschrift niet meegenomen.

We kunnen niet bij elke technologische vernieuwing spreken van een revolutie en al helemaal niet van een die leidt tot een overgang naar een ander type samenleving. Kenmerkend voor technologieën die een revolutie op gang brengen, is hun alomvattendheid. Zij dringen door in alle domeinen van het menselijke bestaan als gevolg van de grote variëteit aan toepassingen. De technologie is meer dan een nieuw product, het is de aanjager van tal van andere veranderingen. De uitvinding van bijvoorbeeld de auto, telefoon en televisie waren weliswaar vernieuwend, maar niet in die mate dat we kunnen spreken van een revolutie. ICT is echter wel een revolutionaire technologie.[11] Anders dan bij de industriële revolutie gaat het nu om technologieën van informatieverwerking en -communicatie in plaats van spierkracht. Omdat informatie een integraal en onmiskenbaar onderdeel is van ons menselijk bestaan, dringen de effecten van ICT door in de gehele samenleving. Kenmerkend ten opzichte van andere revoluties is verder de positieve spiraal tussen innovatie en de toepassing ervan. Deelontwikkelingen versterken elkaar daardoor.[12]

Castells beschouwt ontwikkelingen in drie technologieterreinen als het meest belangrijk, namelijk in micro-elektronica (transistors, chips en microprocessoren), computers en telecommunicatie. Deze ontwikkelingen, gestart in de jaren zeventig, hebben elkaar onderling beïnvloed en gestimuleerd. De echte doorbraak kwam in de jaren negentig. De ICT-revolutie is dus niet van de ene op de andere dag ontstaan en is nog niet gestopt. In vergelijking met de industriële revolutie heeft de ICT-revolutie zich snel voltrokken en snel verspreid over de gehele wereld. De basiskennis die ten grondslag lag aan de industriële revolutie bestond al 100 jaar voordat deze werd toegepast. Vervolgens duurde het meer dan een eeuw voordat deze volledig zijn beslag kreeg. De ICT-revolutie voltrekt zich daarentegen in decennia in plaats van eeuwen.[13]

De ICT-innovatie is dus reeds gestart in de jaren zeventig. Vanaf die tijd is de capaciteit van ICT kwantitatief en kwalitatief exponentieel toegenomen in combinatie met een

[9] Deze paragraaf is voor een belangrijk deel gebaseerd op Castells {Castells, 1998A}. Castells spreekt overigens over Informatietechnologie (IT) in plaats van ICT. Hij verstaat onder IT "[….] the converging set of technologies in microelectronics, computing (machines and software), telecommunications/ broadcasting, and optoelectronics" {Castells, 1998A, 30}. Verder rekent hij ook biotechnologie tot IT. Dit aspect wordt verder in dit hoofdstuk niet meegenomen. Anderen, zoals {Infodrome, 2000}, {Infodrome, 2001}, {Commissie ICT en overheid, 2001} baseren zich voor een groot deel op zijn analyse.

[10] {Infodrome, 2000, 9}.

[11] {Castells, 1998A, 31}, {Infodrome, 2000, 16}, {Infodrome, 2001}. Ook de kabinetten Kok I en II waren overtuigd van het doordringende karakter van de ICT-innovatie {Ministerie van EZ e.a., 1999, 5} en {Contract met de toekomst, 2000, 4-9}.

[12] {Castells, 1998A, 31-33, 60-65}, {Castells, 2001, 1}.

[13] {Castells, 1998A, 34-47, 51}, {Commissie ICT en overheid, 2001, 12}.

voortdurende prijsdaling. Dit geldt voor opslag- en communicatiemedia en verwerkingsapparatuur. Daardoor is het eenvoudiger geworden om informatie te vergaren, op te slaan, te bewerken en te creëren vanuit verschillende bronnen (informatieverwerking). ICT biedt niet alleen meer mogelijkheden, maar maakt de verwerking per eenheid informatie bovendien goedkoper en minder arbeidsintensief. De omvang van de informatie is daarbij nauwelijks een beperking.[14] Vanaf de jaren zeventig zijn verder mondiaal aaneengeschakelde netwerken tot stand gebracht, waarvan het internet het meest prominente voorbeeld is. Via de netwerken kan men informatie distribueren en verwerken over grote afstanden, zonder noemenswaardig tijdverlies en naar vele partijen.[15] De Hond gebruikt een metafoor van rondreizende zintuigen: het lichaam kan op één plaats blijven, terwijl de ogen, mond en oren wereldwijd rond kunnen kijken, boodschappen achter kunnen laten en geluid kunnen horen. Met de telefoon konden de mond en de oren ook al wereldwijd rondreizen. En met de televisie kun je vanuit de luie stoel gebeurtenissen aan de andere kant van de wereld on line meemaken. Nieuw echter aan het internet is vooral de combinatie van ogen, oren en mond, het interactieve karakter en het multimediale karakter.[16] Een ander aspect is dat de afzonderlijke technieken en infrastructuren steeds meer geïntegreerd raken. Tele- en datacommunicatie zijn bijvoorbeeld vervlochten geraakt evenals de kabelinfrastructuur voor radio en televisie. Als gevolg van die toegenomen integratie ontstaat als het ware een geïntegreerd informatiesysteem.[17] Tot slot hebben de deskundigen ook voortdurend de besturings- en applicatiesoftware verbeterd. Dat heeft eveneens stimulerend gewerkt op de overige ontwikkelingen.

5.3. Interactie ICT-innovatie en samenleving

De analyse van de interactie tussen technologische vernieuwingen en de samenleving is ingewikkeld. Volgens Castells is de interactie afhankelijk van bij toeval bepaalde relaties tussen een excessief aantal quasi-onafhankelijke variabelen. Het is te eenvoudig om te stellen dat een technologische vernieuwing leidt tot maatschappelijke veranderingen. Die veranderingen beïnvloeden namelijk op hun beurt ook weer de technologische vernieuwingen. Gezamenlijk kan dit leiden tot een maatschappelijke dynamiek, die groter is dan de som van de onderdelen. Eenvoudige oorzaak-en-gevolgredeneringen volstaan daarom niet.[18]

Dat de interactie ingewikkeld en divers is, blijkt wel uit de uiteenlopende invalshoeken en concepten die men hanteert. Zoals eerder is aangegeven, hanteren sommigen het concept van de informatiesamenleving.[19] Zo gaan de kabinetten-Kok I en II in drie nota's (1998, 1999 en 2000) uitvoerig in op de informatiesamenleving.[20] Infodrome legt het accent op het samenstel van maatschappelijke veranderingen die samengaat met de ICT-innovatie. De informatiesamenleving is " [….] het geheel aan verhoudingen van mensen onderling, van mensen en organisaties, van organisaties onderling, van instituties en van overheids-

[14] In paragraaf 5.7 komen desondanks enkele beperkingen aan bod.
[15] {Commissie ICT en overheid, 2001, 13-14}, {Infodrome, 2001}, {Soete, 2000, VII-XI}.
[16] {De Hond, 1997, 91}.
[17] {Castells, 1998A, 60-65}, {Commissie ICT en overheid, 2001, 13-14}, {Infodrome, 2001}, {Soete, 2000, VII-XI}.
[18] {Castells, 1998A, 52}, {Infodrome, 2001}, {Infodrome, 2000, 9-10}.
[19] {Commissie ICT en overheid, 2001}, {Infodrome, 2000}, {Infodrome, 2001}, {Ministerie van Justitie, 1998, 4}, {Castells, 1998A}.
[20] {Ministerie van Justitie, 1998}, {Ministerie van EZ e.a., 1999}, {Contract met de toekomst, 2000}.

handelen, zoals zich dat door de informatierevolutie aan het ontwikkelen is".[21] Omdat de ICT-innovatie niet stilstaat en evenmin de maatschappelijke veranderingen (en vice versa), is de informatiesamenleving nog niet volledig uitontwikkeld en uitgekristalliseerd.[22]

De informatiesamenleving is vanuit uiteenlopende gezichtspunten bestudeerd. In de nota 'Wetgeving voor de elektronische snelweg' uit 1998 keek het toenmalige kabinet vooral naar de consequenties voor de wetgeving. Als belangrijkste aspecten van de informatiesamenleving benoemen de auteurs dematerialisering, zoals een digitale in plaats van een papieren krant, internationalisering en technologische turbulentie.[23] In 2001 heeft de Commissie ICT en Overheid de informatiesamenleving bestudeerd vanuit het perspectief van de " [….] positie, rol en institutionele structuur van de Nederlandse overheidsorganisatie". In samenhang met andere maatschappelijke ontwikkelingen leiden de ontwikkelingen in ICT volgens de commissie tot een aantal trends. Een eerste is een aanmerkelijke horizontalisering van communicatie- en informatierelaties binnen en vooral tussen organisaties. Dit wordt versterkt door een maatschappelijke trend van horizontalisering en vice versa. Een tweede trend is die van deterritorialisering. Tijd en ruimte spelen in de informatiesamenleving nog nauwelijks een rol. Een derde trend is virtualisering. De commissie doelt hiermee op processen, activiteiten en producten die volledig immaterieel zijn, zoals een digitale krant. Een vierde is versnelling. Het tempo van de ontwikkelingen ligt hoog en de aard en de richting zijn turbulent. Voorspelbaarheid en beheersbaarheid nemen daardoor af. Volgens de commissie hangen deze trends niet alleen rechtstreeks samen met ICT, maar ICT versterkt bovendien deze trends.[24] Infodrome heeft eveneens in opdracht van de toenmalige regering in 2001 geadviseerd over de rol van de overheid in de informatiesamenleving. Zij keek vooral naar de gevolgen van de ICT-revolutie voor de politiek, economie en individu en dus naar die aspecten van de informatiesamenleving. Zij identificeert in het rapport drie krachten die daarop van invloed zijn. Net als de commissie ICT en overheid noemt Infodrome deterritorialisering en horizontalisering, dat zij overigens vernetwerking noemt. Als derde kracht noemt zij vervlechting. Voorbeelden zijn vervlechting tussen overheid en markt, tussen overheid en bedrijven die steeds vaker collectieve belangenbehartiging nastreven en vervlechting tussen werk en privé op individueel niveau.[25]

Naast deze analyses die specifiek zijn gericht op de overheid, hebben anderen de gevolgen geanalyseerd voor de economie. Zij nemen ook andere factoren en ontwikkelingen mee in de beschouwingen, waaronder internationalisering. Zij hanteren uiteenlopende invalshoe ken, resulterend in begrippen als nieuwe economie, informatie-, kennis- of interneteconomie.[26]

Castells kijkt in de breedte naar de 'nieuwe wereld'. Hij spreekt in dit kader van het informatietijdperk. Nieuw zijn sociale structuren (netwerksamenleving), economische

[21] {Infodrome, 2000, 16} en {Infodrome, 2001}. Tussen de omschrijving in het eerste en tweede rapport zit een klein verschil. De omschrijving/ typering uit het tweede rapport is gebruikt.
[22] {Ministerie van Justitie, 1998}, {Ministerie van EZ e.a., 1999}, {Contract met de toekomst, 2000}, { Infodrome, 2000}, {Infodrome, 2001}, {Commissie ICT en overheid, 2001, 12}.
[23] {Ministerie van Justitie, 1998, 51}.
[24] {Commissie ICT en overheid, 2001}.
[25] {Infodrome, 2001}.
[26] Zie bijvoorbeeld {Soete, 2000} voor de nieuwe economie, {Meijers, 2000} voor de informatie-economie, {University Texas, 2000} voor de interneteconomie.

verschijnselen (informatie-/globale economie) en de cultuur (cultuur van reële virtualiteit). Hij beschouwt de ICT-revolutie als één van de drie onafhankelijke processen die samen hebben geleid tot de nieuwe wereld. De twee andere processen zijn volgens hem de economische crisis van zowel het kapitalisme als de planeconomie en de er op volgende herstructurering en opkomst van culturele sociale bewegingen zoals liberalisme en feminisme. Aan de ene zijde beperkt Castells zijn analyse dus niet uitsluitend tot de ICT-innovatie, maar neemt hij ook de twee andere ontwikkelingen mee. Aan de andere zijde richt zijn analyse zich op zowel nieuwe sociale structuren, economie en cultuur.[27] In een later boek analyseert hij de wisselwerking tussen het internet, de samenleving en de economie.[28]

Wanneer het gaat om de interactie tussen de ICT-innovatie en veranderingen in de samenleving is in dit proefschrift gekozen voor het begrip 'ICT-ontwikkelingen'. Eerder is al aangegeven dat die interactie niet eenvoudig valt te analyseren. Eenvoudige oorzaak-gevolgredeneringen zijn niet bruikbaar. De volgende paragraaf benoemt vier specifieke kenmerken. De daaropvolgende paragrafen beschrijven enkele gevolgen voor het legale bedrijfsleven en sociale controle, alsmede enkele beperkingen.

5.4. Kenmerken ICT-ontwikkelingen

Verwerking en communicatie van informatie spelen een belangrijke rol in organisaties.[29] Al vanaf de jaren zestig is een trend te onderkennen van fysieke naar denkarbeid. Tevens is een trend te onderkennen dat informatie steeds belangrijker wordt als productiefactor naast de klassieke productiefactoren van grondstoffen, arbeid en kapitaal.[30] De ICT-innovatie heeft geleid tot een verschuiving van fysieke naar digitale informatieverwerking. Bovendien heeft ICT nieuwe toepassingen mogelijk gemaakt. De omvang van de informatie voor bijvoorbeeld opslag, manipulatie en distributie vormt nauwelijks een beperking. De materiële en personele kosten van informatieverwerking per eenheid van verwerking zijn bovendien afgenomen.[31] ICT in netwerken creëert bovendien tal van voorzieningen voor informatieverwerking zonder beperkingen van plaats en tijd. Zelfs in een traditionele sector als de landbouw neemt ICT een prominente plaats in. ICT maakt bovendien onderdeel uit van allerlei apparatuur, bijvoorbeeld van een parkeerautomaat. Men gebruikt zelfs chips tijdens het vervoer van bijvoorbeeld kroppen sla om te weten hoe lang deze onderweg zijn en waar deze uiteindelijk terechtkomen. *ICT* is dus een belangrijk *kapitaalgoed* (geworden). De samenleving is daardoor in sterke mate afhankelijk van het goed functioneren van ICT. De keerzijde is dat de samenleving kwetsbaar is voor het niet goed functioneren van ICT.

Naast kapitaalgoed, is *ICT* ook een *consumptiegoed*. In het merendeel van de huishoudens in Nederland zijn pc's aanwezig. Vrijwel alle Nederlanders beschikken over een gsm, ongeacht de leeftijd. ICT maakt bovendien onderdeel uit van allerlei andere consumptie-goederen, waaronder auto's en, op niet al te lange termijn, ook in de koelkast thuis. ICT is

[27] {Castells, 1998B, 336-340}.
[28] {Castells, 2001}.
[29] Informatieverwerking is gebruikt als verzamelbegrip voor vergaring, opslag, manipulatie, creatie en distributie van informatie.
[30] {Marchand & Horton, 1986, 25}.
[31] In paragraaf 5.7 komen enkele beperkingen aan bod.

doorgedrongen in alle haarvaten van onze samenleving. Daardoor is de afhankelijkheid en ook de kwetsbaarheid toegenomen van ICT voor het functioneren van de samenleving.

Een ander kenmerk is dat *informatie* een belangrijk *consumptiegoed* en belangrijke *productiefactor* is. Een eerste verklaring is dat ICT het mogelijk maakt om informatie te digitaliseren. Digitale informatie heeft immers een aantal voordelen ten opzichte van fysieke informatie. Het kan een combinatie zijn van tekst, beeld en geluid: het is multimediaal. Digitale informatie kost minder opslagruimte en is makkelijker terug te vinden. Het is vrijwel kosteloos te dupliceren en laat zich eenvoudiger manipuleren en distribueren. Een tweede verklaring is dat ICT ook de wijze van verwerken van informatie positief heeft beïnvloed: meer mogelijkheden en per eenheid minder kosten. Met ICT zijn zowel de voordelen van informatie in digitale als in fysieke vorm te benutten, zoals in de fotografie waarbij men digitale opnamen analoog afdrukt. Een derde verklaring is dat via de mondiaal aaneengeschakelde netwerken informatie kan worden gedistribueerd over grote afstanden, zonder noemenswaardig tijdverlies en naar vele partijen. Voorbeelden van (digitale) informatie als consumptiegoed zijn: digitale foto's, digitale kranten en digitale spelletjes. Voorbeelden van informatie als productiefactor zijn: informatie over de voedingsconsumptie van koeien, de verblijfplaats van een vrachtwagen en de voortgang van een vergunningsaanvraag. Informatie als productiefactor en consumptiegoed vloeien deels in elkaar over. Een bank kan steeds eenvoudiger informatie vergaren van bedrijven die niet tot de eigen cliëntèle horen. De analyses op basis van deze gegevens kan de bank als service aanbieden aan beleggers. Doordat het gebruik en het belang van informatie steeds verder toenemen, groeit ook de afhankelijkheid van informatie voor het functioneren van de samenleving en daarmee de kwetsbaarheid.[32]

ICT is ook gebruikt om netwerken mondiaal aan elkaar te koppelen, waarvan het internet het meest prominente voorbeeld is. Hierdoor is als het ware een *virtuele ruimte* ontstaan, het derde kenmerk. De virtuele ruimte is in de kern een communicatieomgeving waarin het mogelijk is om met velen mondiaal interactief te communiceren op elk gewenst moment van de dag.[33] Doordat communicatie cruciaal is voor het menselijk bestaan,[34] beïnvloedt de virtuele ruimte vele facetten van onze hedendaagse samenleving. Zo gebruikt het bedrijfsleven in toenemende mate de virtuele ruimte voor communicatie en het afsluiten van transacties, aangeduid als e-commerce of e-business. Castells verstaat daaronder "[….] any business activity whose performance of the key operations of management, financing, innovation, production, distribution, sales, employee relations, and customer relations takes place predominantly by/on the internet or other networks of computer networks, regardless of the kind of connection between the virtual and the physical dimensions of the firm".[35] De overheid benut eveneens de virtuele ruimte. Zij probeert zo de toegankelijkheid van het overheidsapparaat te vergroten, de efficiëntie te bevorderen en de kwaliteit van de dienstverlening te verhogen.[36] Ook individuele burgers gebruiken de virtuele ruimte. Voorbeelden zijn het verzenden van e-mail, het uitzoeken van de vakantie, het spelen van spelletjes en internetbankieren.

[32] In paragraaf 5.7 komen enkele beperkingen aan bod van digitale informatie.
[33] Zie voor dat laatste bijvoorbeeld {Castells, 2001, 2}.
[34] {Castells, 2001, 5}. Castells heeft het in zijn boek specifiek over het internet, maar zijn analyse is zeker ook van toepassing op de andere netwerken.
[35] {Castells, 2001, 66}.
[36] {Infodrome, 2000, 15}.

De virtuele ruimte integreert steeds verder met de fysieke wereld.[37] Wanneer iemand aan de andere zijde van de wereld een fototoestel bestelt, is fysiek transport daarvan nodig. Een futuristisch voorbeeld is dat met behulp van ICT de koelkast zelf nieuwe artikelen via het internet bestelt. Vanwege zowel het toenemend gebruik van de virtuele ruimte en de groeiende integratie neemt de afhankelijkheid van de virtuele ruimte voor het functioneren van de samenleving eveneens toe en daarmee de kwetsbaarheid.

De creatie en het gebruik van ICT, informatie en de virtuele ruimte is mensenwerk. Castells maakt daarbij een onderscheid tussen generieke en zelfprogrammeerbare arbeid. Dit onderscheid is primair gelegen in het niveau van de opleiding en het vermogen om zich voortdurend bij te scholen en eigen initiatieven te ontplooien. Generieke arbeid is snel te vervangen en niet schaars. Zelfprogrammeerbare arbeid is daarentegen minder snel vervangbaar en wel schaars. Voorbeelden van zelfprogrammeerbare arbeiders, verder in dit kader aangeduid als *ICT-deskundigen*, zijn website-ontwerpers, beveiligingsdeskundigen en programmeurs. Zij kunnen niet in elke organisatie gedijen. Zij komen vooral tot hun recht in een platte organisatie, in teamverband, in een open dialoog tussen medewerkers en management binnen en tussen de niveaus van een organisatie en bij een zekere mate van autonomie. Bedrijven betalen hen mede met opties en aandelen in de eigen organisatie. Daardoor ontstaat meer flexibiliteit in de arbeidsverhoudingen. Medewerkers die niet aan de eisen van zelfprogrammeerbare arbeid kunnen voldoen, hebben het moeilijk op de arbeidsmarkt. De behoefte aan een ander type arbeid is niet alleen een gevolg van de ICT-innovatie, maar stimuleert deze ook.[38]

Naast het aantrekken van ICT-deskundigheid, kan een organisatie de activiteiten uitbesteden. Er zijn tal van nieuwe bedrijfstakken ontstaan, waaronder een complete *ICT-sector*. Deze sector bestaat uit een breed scala aan bedrijven en dienstverleners. Voorbeelden daarvan zijn providers en ontwerpers van websites. Juist de nieuwe deskundigen beginnen vaak zelf een eigen onderneming. Leidde de industriële revolutie tot een verschuiving van individuele ondernemers naar grotere organisaties, nu is een omgekeerde beweging gaande.[39] Ook hier geldt dat de ICT-sector niet alleen een gevolg is van de ICT-innovatie, maar ook een oorzaak.

5.5. Gevolgen voor legale bedrijven

De ICT-ontwikkelingen resulteren in voortdurende innovatie van de technologie zelf, processen en producten.[40] Innovatie van processen richt zich bijvoorbeeld op andere managementstijlen, werkwijzen en organisatievormen (zie verderop).[41] Het kan zich ook richten op integratie van losse toepassingen, processen en transacties binnen en buiten de organisatie.[42] Zo creëert ICT de gelegenheid om informatieprocessen te vervlechten met productieprocessen en/of logistieke ketens. Via een satellietverbinding weet bijvoorbeeld een transportonderneming waar de vrachtwagens zich bevinden. Daardoor kan de

[37] Gebaseerd op {Gerstner, 1999}, {Contract met de toekomst, 2000, 9} en interview met ICT-bedrijf (bijlage 4).
[38] {Castells, 1998B, 341-342}, {Castells, 2001, 90-96}.
[39] {Castells, 1998B, 341-342}, {Castells, 2001, 90-96}.
[40] Diverse rapportages gaan in op de snelheid en omvang van de veranderingen, waaronder {Castells, 1998B}, {Castells, 2001}, {Commissie ICT en overheid, 2001}, {Infodrome, 2000}, {Infodrome, 2001}, {Ministerie van Justitie, 1998}.
[41] {Castells, 2001, 65-115}, {Castells, 1998B, 341-342}.
[42] {Gerstner, 1999}, {Vuijsje, 2000}, {University Texas, 2000, 38}.

transportonderneming file-informatie en nieuwe vrachten doorgeven aan de chauffeurs. Hierdoor kan de productiviteit stijgen en bedrijven kunnen daarmee een concurrentievoordeel behalen. Voorbeelden van innovatie van producten zijn het internetbankieren en het beleggen via het internet. Innovatie van processen en producten stimuleert op haar beurt de vernieuwing van ICT.

De inzet van ICT kan resulteren in een daling van de transactiekosten tussen en binnen organisaties. Zo kunnen vragende en aanbiedende partijen in de virtuele ruimte eenvoudiger en wereldwijd op zoek gaan naar elkaar. Zij kunnen met behulp van slimme software relevante informatie opvragen en aantrekkelijke partijen selecteren. Een voorbeeld daarvan zijn websites waar makelaars huizen aanbieden. Hierdoor dalen de zoekkosten voor kopers, waardoor meer transacties tot stand kunnen komen. Gebrek aan informatie, onvolledige informatie of ongelijke verdeling van informatie verhogen namelijk de transactiekosten. Hoge transactiekosten belemmeren transacties tussen en binnen organisaties. Omgekeerd stimuleren lage transactiekosten juist transacties. Daardoor kan het aantrekkelijker worden om bepaalde activiteiten niet langer binnen de eigen organisatie uit te voeren, maar uit te besteden aan externe marktpartijen. Volgens Jägers e.a. stimuleren lagere transactiekosten organisaties om in netwerken samen te werken.[43] In de kern is zo sprake van gecoördineerde decentralisatie van werkzaamheden. In combinatie met individualisering van arbeid en andere arbeidsverhoudingen leidt dat tot een grotere flexibiliteit. Een voorbeeld daarvan is dat bedrijven snel kunnen inspelen op nieuwe wensen van klanten, op nieuwe omstandigheden en maatwerk kunnen leveren terwijl ze toch kunnen profiteren van de voordelen van massaproductie. Een grotere flexibiliteit leidt volgens Castells tot een toename van het concurrentievermogen van een onderneming.[44]

ICT draagt ook nog op een andere wijze bij aan flexibiliteit. Netwerkorganisaties hebben een groot aanpassingsvermogen en grote flexibiliteit.[45] Zij hebben echter ook nadelen. Bij een grotere omvang en complexiteit ontstaan namelijk problemen in de coördinatie van activiteiten en doelgerichte taakuitvoering. Met behulp van ICT in het algemeen en het internet in het bijzonder zijn deze nadelen te neutraliseren. ICT-netwerken vormen daarbij het elektronische zenuwstelsel. Daarom is deze organisatievorm in combinatie met het gebruik van ICT geschikt voor de snelle veranderingen die zich in de huidige samenleving voordoen.[46] En ook zo draagt ICT bij aan flexibiliteit en daarmee aan een toename van het concurrentievermogen.

ICT beïnvloedt volgens Porter de concurrentiekrachten die bepalend zijn voor de winstgevendheid van een bedrijfstak. Sommige invloeden zijn positief. Zo ontstaan nieuwe distributiekanalen en kan de omvang van de markt groeien. Het merendeel is echter negatief. Zo kunnen leveranciers rechtstreeks aan klanten gaan leveren. Vooral de tussenhandel komt daardoor onder druk te staan en verdwijnen er marktschijven. De computerfabrikant Dell levert bijvoorbeeld zijn computers alleen via de telefoon en het internet aan eindconsumenten. De tussenhandel is buitenspel gezet. Als gevolg daarvan

[43] {Infodrome, 2001}, {Jägers e.a., 1997}, {Herings & Schinkel, 2000}, {Bartelsman & Hinloopen, 2000, 66-69}, {Vuijsje, 2000, 152-154}.
[44] {Castells, 1998A, 60-65}, {Castells, 1998B, 341-342}.
[45] Network enterprise: [….] the organizational form built around business projects resulting from the cooperation between different components of different firms, networking among themselves for the duration of a given business project, and reconfiguring their networks for the implementation of each project {Castells, 2001, 67}.
[46] {Castells, 2001, 1-2}

neemt de macht van de leveranciers toe ten koste van de winstgevendheid van de tussenhandel. Klanten kunnen op hun beurt verschillende bedrijven benaderen en tegen elkaar uitspelen, waardoor ook hun macht toeneemt. Ook dat gaat ten koste van de winstgevendheid van de tussenhandel. Toetredingsbarrières voor nieuwe bedrijven nemen af. ICT verhoogt namelijk de transparantie doordat informatie breder en sneller toegankelijk wordt. Niet alleen gevestigde bedrijven kunnen daardoor snel beschikken over noodzakelijke productkennis, informatie over de markt en dergelijke, maar ook nieuwkomers. Verder ontstaan er mogelijkheden voor substituten van bestaande producten. De wijze van opereren van Amazon.com is daarvan een voorbeeld in de boekenbranche. Dit bedrijf verkoopt (onder andere) boeken via het internet en hanteert een ander concept voor de bedrijfsvoering. Zo recenseren kopers de boeken en krijg je aanbiedingen op basis van de eigen interesse en het koopgedrag. Rivaliteit tussen concurrenten neemt toe evenals het aantal concurrenten. Vanwege de daling van de marginale kosten van producten, zal de neiging bestaan om te concurreren op prijs. De omvang van de markt zal weliswaar stijgen, maar ten koste van de gemiddelde winstgevendheid.[47] De consument profiteert hiervan. Desondanks zijn zowel individuele bedrijfstakken als individuele bedrijven genoodzaakt om ICT te benutten. Zij moeten wel inspelen op de ontwikkelingen vanwege de concurrentie. Omgekeerd zijn, als gevolg van de openheid van het internet, succesvolle formules veel sneller na te bootsen.[48]

Het bedrijfsleven gebruikt de virtuele ruimte voor e-commerce. Men maakt wel onderscheid tussen e-commerce tussen bedrijven en consumenten (business-to-consumer-commerce) en tussen bedrijven onderling (business-to-business-commerce). Een sterk voorbeeld van het eerste zijn de activiteiten van ‘Amazon.Com’. Voorbeelden van e-commerce tussen bedrijven zijn het gezamenlijk inkopen van goederen met andere bedrijven of het plaatsen van een order bij een ander bedrijf via het internet. Een ander onderscheid is dat naar bedrijven die alleen bestaan in de virtuele ruimte, de virtuele organisaties of dot-coms, en klassieke bedrijven die een deel van de activiteiten in of via de virtuele ruimte laten verlopen.

Bedrijven gebruiken als eerste het internet om de producten te etaleren (brochurefunctie). Vervolgens verschaffen ze informatie aan de klant. Daarna geven ze klanten toegang tot informatie. Pas daarna gaan bedrijven transacties afhandelen via het internet.[49] Niet alle bedrijven kunnen in gelijke mate profiteren van de mogelijkheden van e-commerce. Dit is afhankelijk van het type product en de wijze van levering (zie figuur 5.1). Castells noemt enkele opties van het opereren in de virtuele ruimte. De activiteiten kunnen zowel op wereldwijde schaal als lokaal verlopen (schaalbaarheid). Medewerkers, organisatie-onderdelen, leveranciers en klanten kunnen interactief communiceren. Activiteiten kunnen zo wereldwijd plaatsvinden, terwijl deze toch gecoördineerd kunnen blijven verlopen (beheersing van flexibiliteit). Ondanks de uiteenlopende locaties van waaruit een organisatie opereert, kan toch gebruik worden gemaakt van de naamsbekendheid. Maatwerk is mogelijk, terwijl toch gebruik kan worden gemaakt van massaproductie.[50] Bedrijven die hun producten digitaal kunnen leveren, zijn in staat om optimaal gebruik te

[47] {Porter, 2001, 66-70}. Jägers e.a. gaan in op de bijdrage van ICT in de verlaging van transactiekosten in markten en daarmee in verlaging van de toetredingsbarrières {Jägers e.a., 1997, 24}.
[48] {Porter, 2001}, {Vuijsje, 2000}, {Jägers e.a., 1997, 24}.
[49] Gebaseerd op het interview met het ICT-bedrijf (bijlage 4) en {University Texas, 2000}.
[50] {Castells, 2001, 76}

maken van de potentie van e-commerce. Bedrijven die fysieke producten leveren, moeten daarentegen de bedrijfsvoering fundamenteel aanpassen. Wanneer een klant via het internet een fysiek product aanschaft, verwacht hij natuurlijk wel dat het bedrijf het product ook snel levert en/of lagere kosten hanteert.

Type product	Transactiewijze	Wijze van levering	Voorbeelden
Digitaal	Digitaal	Digitaal	Financiële diensten, digitale krant, digitale videobeelden
Fysiek	Digitaal	Fysiek	Aanschaf via het internet van een boek, (fysieke) cd, videoband, pc of vliegticket. Via het internet bestellen van een huurauto of het aanvullen van de voorraad van een bedrijf
	Digitaal	Deels fysiek, deels digitaal	Thuis uitgeprint bioscoopkaartje, thuis uitgeprinte vliegtickets
Informatie over producten of bedrijf	Digitaal	Digitaal	Digitale brochure, productinformatie, catalogus, bedrijfsinformatie

Figuur 5.1 Vormen van e-commerce

De ICT-ontwikkelingen hebben fundamentele wijzigingen tot stand gebracht in financiële markten. Deze hebben een mondiaal karakter gekregen en de snelheid van financiële stromen is aanzienlijk toegenomen. Er kan wereldwijd worden ingespeeld op investeringsopties en het geld kan overal vandaan komen en naartoe vloeien. De transactiekosten zijn aanzienlijk gedaald. Tevens is informatie op grote schaal en snel beschikbaar om beslissingen op te baseren. Castells benadrukt dat innovatie grote investeringen vereist. Financiers moeten hiertoe wel bereid zijn. De financiering verloopt veelal via aandelen. De wereldwijde en digitale financiële markten hebben die financiering eind jaren negentig mogelijk gemaakt. Vooral toen namen financiers grote risico's en werden vele vormen van innovatie gefinancierd. Begin 2000 kwam hierin een kentering. Als gevolg van de terughoudendheid van de financiële markten is de innovatie fors gereduceerd en daardoor hapert de motor achter de innovatie.[51]

Een echte doorbraak van het gebruik van ICT en de virtuele ruimte ten behoeve van verbeteringen in de bedrijfsvoering moet nog komen. Onvermijdelijk daarvoor is niet alleen innovatie van ICT, maar ook van processen en producten. Innovatie op macroniveau komt voort uit enkele bronnen. De eerste is de creatie van nieuwe kennis in zowel de wetenschap, technologie als management. De tweede bron zijn hoogopgeleide zelfprogrammeerbare arbeiders die de nieuwe kennis kunnen omzetten in productiviteitsverhoging. De derde zijn ondernemers die het risico willen nemen om de innovatie te omarmen.[52] Verder moet op macroniveau convergentie plaatsvinden van investeringscycli, innovatiecycli, bedrijfsvoeringcycli en een innovatieve cultuur.[53]

[51] {Castells, 1998B, 342-346}, {Castells, 2001, 78-84, 109-112}
[52] {Castells, 2001, 65-115}, {Castells, 1998B, 341-342}.
[53] {Castells, 1998B, 342-346}, {Castells, 2001, 78-84, 109-112}

Innovatie op mesoniveau, in organisaties, kan alleen plaatsvinden wanneer aan enkele randvoorwaarden is voldaan. Er is een andere organisatievorm noodzakelijk, de netwerkorganisatie. Een netwerkorganisatie vergroot namelijk het adaptieve vermogen, terwijl de activiteiten wel gecoördineerd blijven verlopen. Voor innovatie is bovendien een ander type werknemer vereist, de zelfprogrammeerbare werknemer. Ook samenwerking tussen de kennisontwikkelaars is onvermijdelijk om zo optimaal te kunnen profiteren van de gezamenlijke denkkracht. Ook aan een open samenwerking tussen producenten en consumenten moet zijn voldaan.[54] Innovatie vergt verder een andere mentale houding van managers om bestaande strategieën, ervaringen en kennis om te vormen. Deze veranderingen kosten tijd. Bedrijven staan daarom nog aan de vooravond van de ontwikkeling van strategieën voor e-commerce en de implementatie ervan.[55] Met name het midden- en kleinbedrijf benut nog maar in beperkte mate de mogelijkheden. Grote bedrijven zoals Unilever en Ahold zijn nog niet eens zo lang geleden gestart met e-commerce-experimenten. Toch zullen bedrijven uit concurrentieoverwegingen op de lange termijn wel moeten inspelen op de mogelijkheden. Dat wat op macroniveau geldt voor convergentie van investeringscycli, innovatiecycli, bedrijfsvoeringscycli en een innovatieve cultuur, geldt ook op mesoniveau. Hoewel in klassieke bedrijven veelal minder ruimte bestaat voor innovatie, hebben die bedrijven toch een voorsprong op nieuwe virtuele bedrijven. Deze moeten op andere terreinen nog leren en bijvoorbeeld nog distributiekanalen opbouwen.[56]

5.6. Gevolgen voor sociale controle

De ICT-ontwikkelingen hebben gevolgen voor sociale controle. Valt het bijvoorbeeld nog op wanneer iemand met dossiermappen onder de arm een pand verlaat, het meenemen van een USB-key met daarop omvangrijke bestanden zal de beveiliging niet snel opmerken. Daar waar de juridische kaders voor een brief duidelijk zijn en eigenlijk iedereen wel weet wat de risico's zijn, geldt dat nog niet voor e-mail. Het gemak waarmee je een nieuwe gsm inclusief nieuw nummer kunt verwerven, maakt afluisteren op naam er niet eenvoudiger op. Daarentegen creëren de ICT-ontwikkelingen ook voordelen. Toezicht is mogelijk met op afstand bestuurde camera's, de videobanden van observaties kunnen automatisch worden geanalyseerd et cetera.

Zeker het ontstaan van de virtuele ruimte heeft grote invloed op sociale controle. Deze paragraaf behandelt die invloed. Allereerst komen de kenmerken aan bod die sociale controle bemoeilijken, namelijk: a) het internationale karakter, b) het informationele karakter, c) de mogelijkheden om anoniem te blijven, d) de vluchtigheid van contacten en identiteiten, e) de diversiteit van gemeenschappen en technische omgevingen en f) de nieuwe en dynamische aard.[57] Daarna komen factoren aan bod die nu juist sociale controle vereenvoudigen. Vervolgens worden de mogelijkheden voor sociale controle verkend en de partijen die dat ter hand kunnen nemen.

De virtuele ruimte is *internationaal* en er bestaan geen landsgrenzen. Dat heeft alles te maken met de open architectuur van de netwerken die ten grondslag liggen aan de virtuele

[54] {Castells, 2001, 65-115}, {Castells, 1998B, 341-342}.
[55] {Porter, 2001, 70-78}, {Strikwerda & de Ridder, 2001}, {University Texas, 2000}.
[56] {Porter, 2001, 70-78}, {Strikwerda & de Ridder, 2001}, {University Texas, 2000}.
[57] De kenmerken a tot en met d zijn ontleend aan {Zouridis, 2004, 1, 9} en e aan {Zouridis & Frissen, 2004, 88}.

ruimte. Daardoor kan iedereen met de geschikte apparatuur en software aansluiten. Dat heeft ook te maken met de 'centrumloosheid'.[58] De fysieke verblijfplaats van iemand en de plaats van handelen kunnen daardoor ver uit elkaar liggen en bij één feit kunnen vele nationaliteiten en landen betrokken zijn. Een bekend voorbeeld, namelijk de casus van de European Union Bank, is illustratief hiervoor. De regering van Antigua gaf in 1994 een licentie aan een bank met de naam European Union Bank.

> *"Papieren uit die tijd suggereren dat het een offshoredochter was van Menatep, een Russische bank die naar verluidt van doen had met de georganiseerde misdaad. EUB's belangrijkste aandeelhouder schijnt Alexander Konanykhire te zijn geweest, een man die in Rusland gezocht werd op beschuldiging van verduistering [….]. Hij zat, op het moment dat het project in Antigua van start ging, in de gevangenis in de Verenigde Staten omdat hij de visumregels had overtreden. Toch stond de regering de EUB toe zijn deuren te openen. Of beter, om zijn website te openen. In werkelijkheid bestond de bank niet op Antigua, noch ergens anders trouwens, alleen in cyberspace. Zijn enige aanwezigheid was op internet. Het was de bank toegestaan om rekeningen te openen, stortingen aan te nemen, orders van creditcards aan te nemen en om 24 uur per dag geld over te kunnen maken naar alle bestemmingen [….]. Het bleek dat de computer, die de werkelijke bank was, zich in Washington DC bevond en dat de man die de computer bediende en de eigenlijke bankier was, in Canada zat. Hoeveel geld er uiteindelijk precies door de bank gesluisd werd en witgewassen door Russen, voor andere Russen en voor enkele van hun Latijns-Amerikaanse drugshandelspartners, is niet bekend. Het zal ook nooit bekend worden omdat halverwege 1997 – op een dag net als alle andere – iemand de stekker uit de computer getrokken heeft. En dat is het laatste wat men van de bank gehoord heeft, of beter, van het geld van de inleggers. Meer dan 12 miljoen dollar verdween."*[59]

Het internationale karakter heeft tal van gevolgen voor sociale controle en roept vele vragen op voor rechtshandhaving en toezicht. Zo is het moeilijk verenigbaar met de territoriaal georganiseerde wetgeving en overheden en de cultuurverschillen tussen landen. Wat het ene land verbiedt, is in een ander land toegestaan. Waar in het ene land iets sociaal is geaccepteerd, hoeft dat elders niet het geval te zijn. Stel dat iemand kinderporno-afbeeldingen aanbiedt via een website in een land waar dat niet strafbaar is. Is die persoon dan strafbaar? En wie controleert het aanbod? Volgens Boni en Kovacich evenals Power bestaan zelfs binnen de Verenigde Staten verschillen in wetgeving voor kinderporno tussen staten en ontbreekt in veel landen adequate wetgeving voor computergerelateerde criminaliteit.[60] En wat is überhaupt het uitgangspunt? Het land waar de aanbieder is gevestigd, de provider, de website of waar de consument woont? Vragen rijzen zoals waar de strafbare feiten zijn gepleegd, wie bevoegd is tot rechtshandhaving en welke wetsbepalingen van toepassing zijn. Als afgeleide van de centrumloosheid is er geen partij die verantwoordelijk is voor het geheel. Waar moet een slachtoffer van oplichting zich dan melden? Kortom, vele nieuwe vraagstukken ontstaan voor wetgevende, opsporings- en controlerende instanties, zoals de douane en de politie, maar ook voor slachtoffers van wantoestanden en andere belanghebbenden.

[58] Zouridis en Frissen noemen deze twee technische karakteristieken van het internet {Zouridis & Frissen, 2004, 90}.
[59] {Robinson, 2000, 242-243}. Zie ook {Boni & Kovacich, 1999, 139} en {Nelson, 1997} voor deze casus.
[60] {Boni & Kovacich, 1999}, {Power, 2000B}.

Als opsporingsinstanties in een land zich geroepen voelen om tegen iets op te treden, moeten zij wel kunnen bewijzen wie welke delicten waar en wanneer heeft gepleegd. Stol e.a. signaleren daarbij diverse problemen. Als bewijsvoerings- en opsporingsproblemen noemen zij: het eenduidig vaststellen van de plaats van het delict, het lokaliseren van de verdachte, het tijdig veiligstellen van bewijsmateriaal, het regelen van internationale rechtshulpverzoeken, het achterhalen van naam-, adres- en woonplaatsgegevens aan de hand van digitale sporen en het bewijzen dat de verdachte feitelijk degene was die het delict heeft gepleegd.[61] De bewijsvoering is complex omdat in de virtuele ruimte zich een hele keten van gegevenstransport heeft voltrokken. Tijdens bijvoorbeeld de communicatie tussen een crimineel in de Verenigde Staten en in Nederland vindt het gegevenstransport plaats langs vele knooppunten over de hele wereld. Voor alle tussenliggende landen is een rechtshulpverzoek nodig. Dit is arbeidsintensief, kost een lange doorlooptijd en levert de nodige juridische haken en ogen op. Bovendien kan de transactie elk uur van de dag en elke dag van het jaar plaatsvinden. Iemand op heterdaad betrappen is daardoor vrijwel onmogelijk[62], tenzij men valstrikken opzet.

Een ander kenmerk is het *informationele karakter*. Geweld kun je niet fysiek toepassen in de virtuele ruimte, wel informationeel. Informatie kan je er niet fysiek stelen, maar wel digitaal. Kinderporno-afbeeldingen kunnen totstandkomen zonder dat er noodzakelijkerwijze kinderen misbruikt zijn.[63] Logischerwijze kan sociale controle alleen digitaal plaatsvinden. Feitelijke sanctionering kan deels digitaal, bijvoorbeeld door iemand niet meer toe te staan in een virtuele gemeenschap of websites uit de lucht te laten halen. Toch zal men veelal naar de fysieke organisatie of persoon moeten voor echte sanctionering, zeker in het geval van een strafrechtelijke aanpak. Daarbij is lang niet altijd eenvoudig traceerbaar wie achter bepaalde feiten zit en waar hij zich bevindt. Verder kan iedere gebruiker als het ware zijn eigen werkelijkheid creëren door een gewenste identiteit aan te nemen op uiteenlopende momenten en in diverse gemeenschappen.[64]

Nog een kenmerk zijn de opties om *anoniem* te opereren in de virtuele ruimte. Berichten en websites kunnen tot op zeker hoogte onzichtbaar blijven. Het gaat om grote aantallen aangesloten computers, websites, documenten en transacties. Binnen de immense omvang van het totale berichtenverkeer is het traceren van individuele berichten daardoor lastig. Als ze al zijn getraceerd, is het nog maar de vraag of daarmee de ware identiteit kan worden achterhaald. Er bestaan sites van waaruit je anoniem een e-mail kunt versturen, al dan niet via een omweg. Bovendien kan iemand regelmatig van digitale identiteit wisselen en gelijktijdig vele gedaanten aannemen. Ook websites kunnen tot op zekere hoogte onzichtbaar blijven ondanks de vele zoekmachines die actief zijn. Een andere naamgeving kan mensen op een verkeerd been zetten en één zoekslag kan immense hoeveelheden treffers opleveren. Als de website al is getraceerd, is daarmee de identiteit van hen die daarachter zitten nog lang niet altijd bekend. Ook hier kan regelmatig een nieuwe website worden opgezet en de oude worden opgeheven. Dit effect wordt nog versterkt wanneer iemand gebruik maakt van een provider in een dubieus land. Hiervan zijn er voldoende op de wereld aanwezig. De genoemde opties maken het mogelijk om anoniem te opereren in

[61] {Stol e.a., 1999B, 372-374}.
[62] {Sussmann, 2001}.
[63] {Zouridis, 2004, 1}.
[64] Zie voor dat laatste {Zouridis & Frissen, 2004, 137}.

de virtuele ruimte.[65] Hoewel er toch mogelijkheden bestaan om sociale controle uit te oefenen, bijvoorbeeld door een website uit de lucht te laten halen, reduceert de anonimiteit het aantal wel. Svensson en Van Wijk stellen in dat kader:

> *"Waar het gedrag van relevante anderen zich systematisch aan de waarneming onttrekt en waar niet over dat gedrag gecommuniceerd wordt, zullen normen niet totstandkomen en zullen bestaande normen ook niet worden gehandhaafd."*[66]

Nog een kenmerk van de virtuele ruimte is de *vluchtigheid van contacten en identiteiten*. Sommigen merken op dat in de virtuele ruimte nieuwe sociale gemeenschappen ontstaan. Deels zijn deze een verlengstuk van gemeenschappen die bestaan in de fysieke wereld. Een voorbeeld daarvan is een vereniging die haar activiteiten aankondigt via het internet. Deels ontstaan nieuwe gemeenschappen die in de fysieke wereld (nog) niet bestaan. Mensen met een gemeenschappelijke hobby of probleem kunnen de ervaringen wereldwijd uitwisselen met soort- of lotgenoten.[67] Toch roepen deze gemeenschappen ook wel vraagtekens op. Doordat individuen zeer uiteenlopende achtergronden hebben, is communiceren niet eenvoudig. De contacten zijn bovendien vrijblijvend en veelal slechts tijdelijk. De drempels om uit de gemeenschap te stappen, zijn laag. Is eigenlijk wel sprake van een gemeenschap?[68] Als gevolg van die vluchtigheid weet je eigenlijk niet met wie je contact hebt en diegene kan weer snel verdwijnen. Personen en organisaties kunnen bovendien nog eens vele identiteiten aannemen en deze snel veranderen en het aanbrengen van een scheiding tussen een elektronische en een natuurlijke identiteit is eenvoudig. Dit maakt sociale controle er niet eenvoudiger op. Iedere ouder kijkt bijvoorbeeld wel uit om wildvreemden in hun huis te halen. Toch kunnen via het internet pedofielen of zelfs moordenaars zomaar contacten aangaan met de kinderen, zonder dat de ouders dat weten. Er kunnen bovendien subculturen ontstaan die afwijkende normen en waarden legitimeren. De aanwezigheid van grote gemeenschappen waar men vrijelijk de nieuwste films uitwisselt, kan het beeld doen postvatten dat dit de gewoonste zaak van de wereld is.[69] De vluchtigheid van contacten en identiteiten beperkt dus de mogelijkheden voor sociale controle.

Net zomin als sprake is van dé fysieke wereld is sprake van dé virtuele ruimte. De virtuele ruimte bestaat volgens Zouridis en Frissen uit een grote *diversiteit van gemeenschappen en technische omgevingen*. Voorbeelden van gemeenschappen zijn hiervoor al genoemd. Denkbaar is dat elke gemeenschap er eigen normen en waarden op nahoudt die afwijken van de gangbare. De normen en waarden zijn daardoor geen universeel gegeven en kunnen sterk divergeren evenals de gevoelde noodzaak van sociale controle daarop. Bovendien zijn uiteenlopende regimes van sociale controle mogelijk of noodzakelijk.[70] Naast de diversiteit van gemeenschappen kenmerkt de virtuele ruimte zich volgens hen door uiteenlopende technische omgevingen. De onderliggende karakteristieken conditioneren tot

[65] Zie bijvoorbeeld voor het vraagstuk van de anonimiteit Svensson en van Wijk {Svensson & Van Wijk, 2004, 26-27}.
[66] {Svensson & Van Wijk, 2004, 15}.
[67] {Stol e.a., 1999A, 5-9}, {Stol e.a., 1999B}, {Svensson & Van Wijk, 2004, 25, 37}, {Zouridis & Frissen, 2004, 96-100}.
[68] {Svensson & Van Wijk, 2004, 24-25}, {Zouridis & Frissen, 2004, 96-100}.
[69] {Stol e.a., 1999A, 5-9}, {Stol e.a., 1999B}, {Svensson & Van Wijk, 2004, 25, 37}, {Zouridis & Frissen, 2004, 96-100}.
[70] {Zouridis, 2004, 4,7}, {Zouridis & Frissen, 2004, 88}.

op zekere hoogte de mogelijkheden voor interactie en daarmee voor sociale controle. Soorten omgevingen zijn:

- het internet (het netwerk der netwerken);
- het web (ook wel aangeduid als world wide web);
- Usenet dat vele nieuwsgroepen, discussies of beeldarchieven omvat over vele onderwerpen;
- e-mail;
- text chat, een omgeving waarin een groep mensen met elkaar op hetzelfde moment kan communiceren;
- MUDs en MOOs: "[….] dit zijn op tekst gebaseerde virtuele realiteiten die bestaan uit een aantal verschillende met elkaar verbonden (virtuele) ruimten. De realiteiten ondersteunen synchrone patronen van communicatie: mensen zijn tegelijkertijd aanwezig in de virtuele realiteit. In het algemeen hebben MUDs (Multi user Dungeons of Dimensions) het karakter van virtuele spelomgevingen, terwijl de MOO (Multi-user, Object Oriented) doorgaans meer lijkt op een sociale ontmoetingsplaats";
- grafische werelden waarin de op tekst gebaseerde virtuele realiteit van de MUDs en MOOs is vervangen door een multimediale grafische realiteit.[71]

De relevantie van dit onderscheid voor sociale controle is volgens Zouridis en Frissen gelegen in de mate waarin er een (centrale) autoriteit aanwezig is en de mate waarin sprake is van een gemeenschap. In (sommige) nieuwsgroepen, MUDs en MOOs is sprake van een (centrale) autoriteit die eventueel kan ingrijpen. In het geval van het word wide web is dat eigenlijk niet het geval. Weliswaar kan een provider een website weghalen, maar deze kan zo weer ergens opduiken. Nieuwsgroepen kunnen een meer of minder sterk gemeenschapskarakter hebben. Hierdoor kan men onderling communiceren over normen en waarden en elkaar daarop aanspreken. Voor het world wide web is geen sprake van een gemeenschap, waardoor dat niet tot de mogelijkheden behoort.[72]

De virtuele ruimte is een nog relatief *nieuwe* en tevens *dynamische omgeving*. In de fysieke wereld heeft het vele decennia geduurd om te komen tot marktregulering, adequate wet- en regelgeving, verdragen voor rechtshulp, optimale opsporingsstrategieën et cetera. In Rusland blijkt ook nu nog hoeveel tijd en moeite het kost om dat tot stand te brengen. Volgens sommigen zijn zaken die voor de reguliere opsporing zijn geregeld, nog niet op voorhand geregeld voor digitaal rechercheren. Allerlei strafrechtelijke vraagstukken doen zich voor, zoals de mate waarin de politie mag uitlokken via het internet. En als zaken juridisch geregeld lijken te zijn of sociaal geaccepteerd, kan de dynamiek weer nieuwe vraagstukken oproepen.[73] Sociale controle moet dus voortdurend blijven aansluiten bij de fase waarin de virtuele ruimte zich bevindt. De dynamiek kan overigens variëren tussen de afzonderlijke soorten technische omgevingen.[74] In een overheidsrapportage constateert men dat die dynamiek in elk geval niet altijd aansluit bij de noodzakelijke zorgvuldigheid van wetgeving.[75]

[71] {Zouridis & Frissen, 2004, 89, 91-93, 100-101}.
[72] {Zouridis & Frissen, 2004, 91-93}.
[73] Zie hiervoor bijvoorbeeld {Stol e.a., 1999B, 372-374}, {Boni & Kovacich, 1999}, {Power, 2000B}, {Van Rossum, 2000}, {Galeotti (Mickey), 2000}, {Sussmann, 2001} en interview met Vriesde (bijlage 4).
[74] {Svensson & Van Wijk, 2004, 27}, {Zouridis & Frissen, 2004, 101}.
[75] {Ministerie van Justitie, 1998, 51}.

Hoewel bovenstaande kenmerken sociale controle lastig maken, is geen sprake van totale anarchie[76] of het volledig ontbreken van mogelijkheden voor sociale controle.[77] Ondanks het *internationale karakter* en het ontbreken van één aanspreekbare partij, maken overheden en bedrijven internationale afspraken. Zo heeft de G8 afspraken gemaakt over samenwerking bij de opsporing van criminaliteit in de virtuele ruimte.[78] Verder heeft de Europese Gemeenschap de laatste jaren wetgeving ontworpen tegen computercriminaliteit. De lidstaten zijn verplicht om op onderdelen de eigen wetgeving aan te passen en te harmoniseren. Ook het bedrijfsleven, bijvoorbeeld de providers, proberen internationaal afspraken te maken. In sommige gevallen hebben de partijen immers gemeenschappelijke belangen om afspraken te maken. Het *informationele karakter* van de virtuele ruimte creëert ook nieuwe kansen voor sociale controle. Zo is het praktisch vrijwel ondoenlijk om alle lokale kranten te analyseren op heling van gestolen waar of verboden financiële dienstverlening. Aanbod daarvan via het internet is relatief eenvoudig te constateren. De virtuele ruimte kent dus een paradoxale spanning tussen *anonimiteit* en de gelegenheid voor observatie en surveillance.[79] De anonimiteit is namelijk relatief. Zo is de privacy-bescherming tijdens het opereren in de virtuele ruimte niet waterdicht. Ook zijn de beveiliging van de gegevens, de gegevensopslag en het gegevenstransport niet optimaal.[80] Hackers en opsporingsinstanties slagen er wel degelijk in om de identiteit, individuele transacties en websites te achterhalen. Een persoon kan in principe anoniem opereren wanneer hij bijvoorbeeld gebruikmaakt van een internetcafé. De eigenaar kan echter tips geven aan opsporingsinstanties. Bovendien laat zo iemand fysieke en digitale sporen achter in het café. Providers die anonieme e-mail aanbieden, werken wel degelijk mee met opsporingsinstanties. Wanneer iemand vanuit een eigen locatie opereert, laat hij veel digitale sporen na. Deze sporen zijn goed traceerbaar. Wanneer iemand fysieke goederen levert of koopt, creëert het transport allerlei bewijssporen. Dit fysieke transport beperkt de anonimiteit van de klant en de leverancier. Ook betalingen laten sporen na. Met voldoende geduld kan in veel gevallen een beeld worden gekregen van de identiteit en de activiteiten. Elk document op het world wide web heeft verder een uniek adres van de server. Van daaruit kunnen opsporingsinstanties een speurtocht starten naar de persoon die bij dat document hoort. Svensson en Van Wijk stellen dat in het geval men niet weet wie er meekijkt, men juist extra voorzichtig is met normoverschrijding. Hier gaat een disciplinerende werking van uit.[81] Ondanks de *vluchtigheid* van de contacten en identiteiten, de *diversiteit* van gemeenschappen en andere complicaties spreekt men in sommige gevallen elkaar wel degelijk aan op afwijkend gedrag. Tevens ontstaan wel degelijk normen en waarden. Accepteert men bijvoorbeeld wel het kopiëren van auteursrechtelijk beschermde werken, het verspreiden van kinderporno keurt men veelal af.[82] Naast problemen voor de opsporing ontstaan ook nieuwe mogelijkheden. "Opsporing en vervolging zijn in de virtuele wereld dus tegelijkertijd makkelijker en moeilijker voor de politie."[83]

[76] {Zouridis, 2004, 1}, {Svensson & Van Wijk, 2004, 39-40, 79-80}.
[77] {Zouridis & Frissen, 2004, 131}.
[78] {Van Rossum, 2000, 52}, {Valeri, 2001}.
[79] Enkele auteurs gaan in op die spanning {Zouridis, 2004, 8}, {Svensson & Van Wijk, 2004, 22-23, 27}, {Zouridis & Frissen, 2004, 86}.
[80] Zie paragraaf 5.7.
[81] {Svensson & Van Wijk, 2004, 27}.
[82] Zie voor dat laatste {Svensson & Van Wijk, 2004, 34, 40, 60, 79} en {Zouridis & Frissen, 2004, 103, 109}.
[83] {Zouridis & Frissen, 2004, 140}, {Zouridis, 2004, 9}.

Tot nu toe is alleen nog in het algemeen gesproken over sociale controle. Svensson en Van Wijk onderscheiden naast de gebruikers, zoals zij die muziek downloaden, specifiek voor de virtuele ruimte:

- belanghebbende industrieën, bijvoorbeeld de muziekindustrie in verband met schendingen van het auteursrecht;
- meldpunten die zich richten op specifieke onderwerpen of uitingen, bijvoorbeeld het meldpunt kinderporno;
- partijen die specifieke gebruikers afschermen, bijvoorbeeld ouders, scholen of werkgevers;
- internet service providers.[84, 85]

Hoewel deze partijen wel mogelijkheden hebben voor sociale controle, constateren Svensson en Van Wijk dat deze nog beperkt zijn in het geval van illegaal kopiëren en discriminatie. Zij noemen als belangrijke factoren voor sociale controle: "[….] de ontwikkeling van het recht (nationaal en internationaal), de (beperkte) bruikbaarheid van filters, de legitimiteit van invloedspogingen en het gemak waarmee ze via het internet kunnen worden omzeild". De randvoorwaarden zijn volgens hen nog niet optimaal voor sociale controle.[86]

Zouridis en Frissen daarentegen zijn optimistischer. Zij onderkennen vijf lagen van regels en gedragscodes waarop uiteenlopende partijen (kunnen) toezien. De eerste laag is die van de 'netiquette', vergelijkbaar met de 'etiquette' in de fysieke samenleving. Het gaat hier om een zaak van fatsoen en beschaving. De tweede laag wordt gevormd door de regels van providers en websitebeheerders, bijvoorbeeld ten aanzien van veiligheid en privacy. De derde laag bestaat uit de gedragscodes van de dienstverleners, bijvoorbeeld die van (gratis) e-mailaanbieders. Wanneer gebruikers willen deelnemen aan specifieke gemeenschappen, kunnen zij te maken krijgen met een vierde laag. Per gemeenschap kunnen namelijk regels zijn geformuleerd. Daar waar de eerste laag algemeen is, kunnen in de overige lagen afzonderlijke beheerders toezien op de naleving van de regels en codes en overtreding eventueel sanctioneren door bijvoorbeeld uitsluiting. Ook de overige leden van de gemeenschap kunnen overtredingen van de derde en vierde laag sanctioneren. Bovendien hebben gebruikers diverse mogelijkheden voor zelfbescherming, waaronder virusscanners, spamfilters et cetera. Tevens kunnen zij een beroep doen op anderen waaronder een 'netdetective' en providers.[87] Zouridis en Frissen stellen dat vooral providers en hun organisaties een belangrijke rol spelen bij regulering[88] en dus bij sociale controle. Verder differentiëren Zouridis en Frissen naar drie soorten sociale controle: 1) inactie, 2) unilaterale sociale controle en 3) bi- en trilaterale sociale controle. "Van inactie is sprake als er geen sancties volgen op gedrag dat afwijkt van de sociale normen zoals deze gelden binnen een gemeenschap". Dat kan door bijvoorbeeld tolerantie of ontwijking. Bij de tweede vorm is wel sprake van een agressieve reactie op een afwijking van de normen. Het slachtoffer maakt in dat geval aanspraak op fysieke, financiële of symbolische genoegdoening. Daarvoor moet men veelal een beroep doen op een derde partij of zelf overgaan

[84] {Svensson & Van Wijk, 2004, 64-70}.
[85] In paragraaf 4.4 is aangegeven wie sociale controle kunnen uitoefenen. Daarbij is een onderscheid aangebracht tussen: a) betrokkenen, b) de overheid, waaronder toezichthoudende en opsporingsinstanties en c) overigen, namelijk zij die niet onder a of b vallen en ook geen (mede)dader zijn.
[86] {Svensson & Van Wijk, 2004, 73-78}.
[87] {Zouridis & Frissen, 2004, 103-109, 111, 122-129}.
[88] {Zouridis & Frissen, 2004, 130}.

tot openbaarmaking, bijvoorbeeld in het geval van pedofielen. Bij de derde vorm "[….] doet de benadeelde een direct beroep op de overtreder ter genoegdoening" (bilateraal), al dan niet via een tussenpersoon zoals een provider of een meldpunt (trilateraal). Opvallend daarbij is dat vooral de eerste twee vormen voorkomen op het internet en dat de geschiktheid van de vorm van sociale controle sterk afhangt van de technische omgeving waarin die controle moet plaatsvinden (chat, e-mail en dergelijke).[89]

Hoewel dus enkele kenmerken van de virtuele ruimte sociale controle lastig maken, bestaan er wel degelijk mogelijkheden. De mate waarin varieert natuurlijk wel naargelang het type normovertreding, het type gemeenschap en het type technische omgeving alsmede naar de partij die sociale controle uitoefent. De noodzaak van differentiatie bestaat echter ook in de fysieke wereld.

5.7. Beperkingen van ICT, informatie en de virtuele ruimte

ICT kan de informatieverwerking goedkoper en minder arbeidsintensief maken. Toch zien organisaties zich vaak geconfronteerd met een hoge kostenpost voor ICT. Aan de inzet van ICT hangt immers ook een prijskaartje. Dat geldt voor de ontwikkeling, de investering, maar ook voor de exploitatie. En weliswaar daalt de kostprijs van ICT voortdurend in relatie tot de capaciteit en snelheid van verwerking, aan de andere kant vereisen de applicaties steeds meer capaciteit en snelheid. Per saldo blijven de kosten dan gelijk. Ontegenzeggelijk is het zo dat bijvoorbeeld het samenstellen van een rapport nu minder tijd kost dan vroeger met een typemachine. Aan de andere kant moeten we tegenwoordig veel meer rapporten produceren, waardoor per saldo het maken van rapporten even arbeidsintensief blijft. Hoewel dus per eenheid van informatie de verwerkingskosten en arbeidstijd zijn gedaald, is het nog maar de vraag of in zijn totaliteit de kosten en arbeidsinspanningen zijn gedaald.

Aan de ene kant is geconstateerd dat de omvang van de informatie nauwelijks een beperking vormt. Met ICT kan men immers grote hoeveelheden informatie op eenvoudige wijze vastleggen, bewerken, dupliceren en over grote afstanden communiceren. Slimme software zorgt ervoor dat men via geavanceerde zoekmechanismen snel informatie uit de grote berg informatie kan halen en allerlei impliciete verbanden kan leggen. Toch weet eenieder die wel eens heeft geprobeerd concrete informatie via het internet te vinden, dat dat niet zonder problemen gaat. Tienduizenden verwijzingen naar andere websites zijn even teleurstellend als geen verwijzing. Verder draait het niet alleen om de hoeveelheid gegevens. De kunst is om betekenis toe te kennen aan de vele puzzelstukjes informatie, vergaard uit een grote hoeveelheid bronnen waarvan de betrouwbaarheid lang niet altijd vaststaat. Niet zozeer de hoeveelheid informatie is veelal het probleem, maar de beperkte aandacht die we daar en aan de interpretatie kunnen besteden. De hoeveelheid aandacht is, ondanks de ICT-ontwikkelingen, gelijk gebleven. Bovendien is de houdbaarheid van de informatie beperkt. Eenieder die wel eens zoekt op het internet loopt tegen verouderde informatie aan of tegen verwijzingen naar informatie die niet langer toegankelijk is. Ook de digitale opslagmedia hebben een beperkte houdbaarheid. Zo is er nog nauwelijks

[89] {Zouridis & Frissen, 2004, 131-136}.

apparatuur beschikbaar om de oude grote floppy's te lezen. Ook bestaan twijfels of de informatie die op cd's is opgeslagen over enkele jaren nog wel leesbaar is.

Ook de virtuele ruimte kent, naast vele mogelijkheden, beperkingen.[90] Zeven daarvan komen hieronder aan bod. Deels hangen zij met elkaar samen.

Een *eerste* beperking vormt de onbetrouwbaarheid en onveiligheid van het betalingsverkeer in de virtuele ruimte. "De consument moet er zeker van zijn dat hij veilig kan betalen via het internet. Belangrijk voor de consument is tevens dat hij juridisch goed beschermd is tegen misbruik van zijn betaalmiddel".[91] Ook de leverancier moet erop kunnen vertrouwen dat hij geld ontvangt voor de geleverde producten. Aan die betrouwbaarheid en veiligheid schort echter nogal het een en ander. Zo verschijnen er regelmatig berichten dat het gebruik van creditcards in de virtuele ruimte onveilig is. Ook de wijze waarop bedrijven omgaan met betalingsgegevens en de wijze van opslag van die gegevens, vormt een zorgpunt. Bovendien kleven er nogal wat beperkingen aan betalingen in de virtuele ruimte. Dat geldt vooral voor betalingen van kleine bedragen en internationale betalingen. Al vele jaren zijn experimenten gaande met digitale betaalmiddelen, maar deze bevinden zich nog steeds in een experimentele fase.

Een *tweede* beperking is de geringe integratie met processen in de fysieke wereld. De processen van bedrijven zijn veelal nog onvoldoende geoptimaliseerd voor e-commerce.[92] De levering van bestelde goederen laat daardoor soms lang op zich wachten. Toch ontstaat in toenemende mate een samensmelting van e-commerce met reguliere distributiekanalen. De bestelling verloopt dan via het internet en de consument kan het bestelde product bij de winkel op de hoek afhalen.

Een *derde* beperking is dat de beveiliging van ICT en informatie nog sterk te wensen overlaat. Voor een toename van het gebruik van de virtuele ruimte is beveiliging cruciaal. Met name het hacken van computers en de verspreiding van virussen belemmeren het vertrouwen. Er bestaan mogelijkheden voor encryptie van de gegevens en het gegevenstransport. Encryptie vormt een krachtig beveiligingsinstrument, maar bevindt zich in een spanningsveld met het opsporingsbelang. Wanneer partijen encryptie toepassen, is het voor opsporingsinstanties lastig om communicatie af te tappen en gegevens voor de bewijsvoering te vergaren.

Een *vierde* beperking vormt de privacygevoeligheid van gegevensopslag en -transport. ICT maakt de opslag van privacygevoelige informatie steeds eenvoudiger. Ook laat het gebruik van het internet sporen na. Dit kan de privacy aantasten. Een adequate afscherming van de privacy vormt een belangrijke voorwaarde voor een verdere groei van het gebruik van het internet. Bezorgdheid over privacy leidt er mede toe dat men geen aankopen doet via het internet.[93] Het privacybelang bevindt zich in een spanningsveld met het opsporingsbelang, maar ook met het commerciële belang. Hoe meer waarborgen voor privacy, des te complexer het is voor opsporingsinstanties om de identiteit te achterhalen. Hoe meer

[90] De beperkingen zijn ontleend aan {Janssen & Haans, 1997}, {Randall, 1997}, {Vuijsje, 2000} en {Gartner, 2000}. Enkele daarvan zijn gebaseerd op een interview in 2000 met drie medewerkers van een internationaal ICT-bedrijf (zie bijlage 4).
[91] {Janssen & Haans, 1997}.
[92] Zie paragraaf 5.5 en {Castells, 2001, 106}.
[93] {Vuijsje, 2000, 79}.

privacy op het internet, des te minder aantrekkelijk het is voor bedrijven om zich bezig te houden met e-commerce. Gegevens over het gedrag van internetgebruikers vormen immers een belangrijke financieringsbron voor e-commerce en een voordeel daarvan. Op deze wijze beschikken bedrijven over gedetailleerde gegevens van klanten en hun voorkeuren. Aan de andere kant belemmert de bezorgdheid over privacy e-commerce en hebben bedrijven er weer belang bij om de behoefte aan privacy te waarborgen.

Een *vijfde* beperking en voor sommigen juist een sterk punt, is een zekere mate van anonimiteit. Er zijn de nodige opties om anoniem te opereren in de virtuele ruimte. Dat heeft bijvoorbeeld als voordeel dat je vrijelijk met gelijkgestemden kunt communiceren. Het nadeel is dat je niet weet met wie je te maken hebt, waardoor oplichting of andere vormen van misbruik op de loer liggen. Toch zijn er geen garanties voor anonimiteit en kan de vermeende anonimiteit ook contraproductief werken.[94]

Een *zesde* beperking is het ontbreken van garanties omtrent de betrouwbaarheid van consumenten en leveranciers. Bij het zakendoen in de fysieke wereld bestaan garanties die ontbreken in de virtuele ruimte. Deels heeft dit te maken met het ontbreken van betrouwbare en veilige digitale betaalsystemen, beperkingen in de beveiliging en bescherming van de privacy. Verder ontbreken garanties omdat de bestelling, de levering en de betaling niet gelijktijdig plaatsvinden. Levering kan lang op zich laten wachten, evenals de betaling. De klant moet erop vertrouwen dat de leverancier na de betaling ook daadwerkelijk de gewenste goederen levert op het gewenste moment, van het gewenste kwaliteitsniveau en op de gewenste plaats. Bovendien moet hij erop vertrouwen dat de leverancier geen misbruik maakt van de gegevens die hij heeft ontvangen om de transactie mogelijk te maken. De leverancier moet erop vertrouwen dat voorafgaand of na afloop van de levering de klant ook daadwerkelijk betaalt. Creditcardmaatschappijen nemen deels de garantie op zich van betaling. Echter niet alle transacties lenen zich voor betaling met de creditcard. Te verwachten valt dat in de toekomst steeds vaker bepaalde organisaties garanties verlenen voor de ware identiteit van zowel de leverancier als de consument. Overheden, de Europese Unie en consumentenorganisaties werken aan protocollen en wetgeving.

Een *zevende* beperking is de geringe bereidheid van consumenten tot het betalen voor informatie. Aanbieders van informatie verdienen de investeringen grotendeels terug via inkomsten van adverteerders of van degenen naar wie is doorverwezen.[95] Deze inkomstenbron is na maart 2000 aanzienlijk opgedroogd. Dit is mede aanleiding geweest voor het verdwijnen van menig virtueel bedrijf. Een andere bron van inkomsten is het bijhouden van gegevens van bezoekers. De consument staat hier kritisch tegenover in verband met de behoefte aan privacy. De consument zelf is nog niet echt bereid om te betalen voor het ontvangen van informatie of het bezoeken van een website. Bij het internet hoort nog het beeld dat informatie gratis is. Bovendien ontbreekt nog een universeel en internationaal digitaal betaalmiddel voor kleine bedragen.

[94] Zie paragraaf 5.6.
[95] {Castells, 2001, 106} en {Vuijsje, 2000}.

5.8. Overzicht van bevindingen

De ICT-ontwikkelingen hebben vier kenmerken: 1) ICT als consumptie- en kapitaalgoed, 2) informatie als consumptiegoed en productiefactor, 3) de virtuele ruimte en 4) de ICT-sector en -deskundigen. Voor het legale bedrijfsleven resulteren de ICT-ontwikkelingen in innovatie, vergroting van de flexibiliteit en verlaging van de transactiekosten. Bovendien beïnvloeden zij de concurrentiekrachten en verminderen de nadelen van netwerkorganisaties. Dat kan leiden tot een verhoging van de productiviteit en een vergroting van het concurrentievermogen van individuele ondernemingen, maar tevens tot een verlaging van de winstgevendheid van de bedrijfstak als geheel. De randvoorwaarden voor deze veranderingen zijn echter nog niet altijd optimaal. ICT, informatie en de virtuele ruimte kennen bovendien nog beperkingen. Verder rijzen er problemen voor sociale controle, maar ontstaan er ook nieuwe mogelijkheden.

6. Dreigingen en de beoordeling ervan

6.1. Inleiding

In de voorgaande hoofdstukken is het risicoanalyse-instrumentarium gepresenteerd en zijn de ICT-ontwikkelingen geanalyseerd. Nu kunnen we starten met het identificeren van dreigingen en met de beoordeling daarvan, het onderwerp van dit hoofdstuk. Daarmee wordt uitvoering gegeven aan de stappen 3 en 4 van een risicoanalyse. Alvorens nader in te gaan op de structuur van dit hoofdstuk, komen eerst de hoofdlijnen van de voorgaande hoofdstukken nog eens aan bod.

Het object van de risicoanalyse zijn 'veranderingen in georganiseerde criminaliteit als gevolg van de ICT-ontwikkelingen'. Georganiseerde criminaliteit is geconceptualiseerd als een stelsel van illegale groothandelsondernemingen. Er zijn drie soorten veranderingen benoemd, namelijk in de illegale groothandelswaar, groothandelsondernemingen en de bedrijfsvoering. Omdat de aandacht zich richt op veranderingen, vormen zij tevens de soorten dreigingen waarnaar we op zoek zijn. Per soort verandering zijn risicofactoren beschreven. Verder zijn uitgangspunten geëxpliciteerd voor de beoordeling van ongewenste effecten en enkele daarvan zijn gespecificeerd. Vier kenmerken van de ICT-ontwikkelingen zijn benoemd: 1) ICT als consumptiegoed en kapitaalgoed, 2) informatie als consumptiegoed en productiefactor, 3) virtuele ruimte en 4) ICT-sector en -deskundigen.

Paragraaf 6.2 geeft een overzicht van de geïdentificeerde dreigingen. Paragraaf 6.3 beschrijft in hoeverre de gevolgen van de ICT-ontwikkelingen voor het legale bedrijfsleven zich ook zouden kunnen voordoen in misdaadmarkten en -ondernemingen. De paragrafen 6.4 tot en met 6.10 beschrijven afzonderlijk de dreigingen en de waarschijnlijkheid en ongewenste effecten daarvan. Hoewel alle risicofactoren aan bod komen, zijn deze niet puntsgewijs opgesomd. Dit is gedaan omwille van de leesbaarheid. In bijlage 3 zijn de risicofactoren wel gespecificeerd. Paragraaf 6.11 geeft een overzicht van de waarschijnlijkheid en ongewenste effecten van alle dreigingen evenals van de deeldreigingen.

Met nadruk wordt er nog eens op gewezen dat dit hoofdstuk niet is gebaseerd op empirie. De algemene risicofactoren zoals beschreven in hoofdstuk 4 zijn niet specifiek voor de ICT-ontwikkelingen geoperationaliseerd in risico-indicatoren en ook niet empirisch getoetst. Dat heeft enerzijds te maken met het doel waarvoor deze analyse is uitgevoerd, namelijk toepassing van het ontwikkelde risicoanalyse-instrumentarium. Anderzijds heeft het te maken met het verkennende karakter van de analyse en het feit dat de analyse is bedoeld voor vroegtijdige criminaliteitsbeheersing. Wel is gebruikgemaakt van enige literatuur en zijn enkele interviews gehouden.[1] In aanvulling daarop is tevens gebruikgemaakt van het in 2004 uitgebrachte 'Nationaal Dreigingsbeeld zware of georganiseerde criminaliteit'.[2] Er zijn geen anderen betrokken geweest bij de beoordeling van de dreigingen om dezelfde redenen als hiervoor zijn genoemd.

[1] Zie hiervoor paragraaf 1.4.
[2] {DNRI, 2004}

6.2. Overzicht van dreigingen

Als vertrekpunt voor de identificatie van dreigingen fungeert de combinatie van de kenmerken van de ICT-ontwikkelingen en de soorten veranderingen. Deze combinatie resulteert in twaalf potentiële veranderingen (zie figuur 6.1). Niet elk kenmerk leidt echter vanzelfsprekend tot alle drie de soorten veranderingen. Bovendien hangen zowel de kenmerken als de soorten veranderingen onderling samen. Zo is informatie mede een belangrijke productiefactor geworden als gevolg van de inzet van ICT als kapitaalgoed. Omgekeerd had men ICT niet ingezet als informatie geen belangrijke productiefactor zou zijn. Doordat eenvoudige oorzaak-en-gevolgredeneringen tussen de kenmerken niet volstaan,[3] is per kenmerk beredeneerd of er één of meer van de drie soorten veranderingen uit voort kunnen komen. Met de mogelijke samenhang tussen de kenmerken is daarbij geen rekening gehouden. Wel rekening is gehouden met causale relaties tussen de soorten veranderingen. Een nieuw soort handelswaar zou kunnen resulteren in een nieuw type illegale groothandelsonderneming en bedrijfsvoering. Wanneer een verandering uitsluitend het gevolg is van één of meer andere veranderingen en dus geen zelfstandige betekenis heeft, dan is deze niet afzonderlijk benoemd.[4]

Als gevolg van de samenhang tussen de kenmerken en de soorten veranderingen, bestaan er relaties tussen de dreigingen. De ‘inzet van ICT in de illegale bedrijfsvoering’ kan bijvoorbeeld voortkomen uit de ‘omzetting van een gewone naar een virtuele bedrijfsvoering’. Die inzet kan daarentegen ook op zichzelf staan. In de beoordeling van de waarschijnlijkheid en de ongewenste effecten is expliciet rekening gehouden met die relaties. In bijlage 2 zijn deze gespecificeerd. In verband met de samenhang tussen de kenmerken is tevens voorzien in een analyse van de gezamenlijke effecten op misdaadmarkten en -ondernemingen (zie paragraaf 6.3). Bij de beoordeling van de waarschijnlijkheid van de afzonderlijke dreigingen is rekening gehouden met die bredere context.

Een dreiging kunnen we op uiteenlopende wijzen voorzien van een etiket. Zo kunnen we een dreiging benoemen als ‘inzet van ICT in de illegale bedrijfsvoering’. Evenzogoed zouden we kunnen spreken van ‘toename van de illegale handel door de inzet van ICT’ of ‘verbetering van de illegale bedrijfsvoering door de inzet van software’. De eerste naamgeving en het abstractieniveau sluiten het best aan bij de combinatie van het kenmerk en het soort verandering. Bovendien moet nog maar blijken of de inzet van ICT resulteert in een toename van de handel en/of een verbetering van de bedrijfsvoering. Het uitgangspunt is om met de naamgeving en het abstractieniveau van de dreiging aan te sluiten bij het kenmerk en het soort verandering. Omdat het in dit proefschrift gaat om een eerste verkenning, vindt geen verdieping plaats van de dreigingen naar specifieke functies die Nederland kan vervullen voor illegale groothandelsondernemingen. Die verdieping is bovendien niet zonder haken en ogen. Verder is op voorhand al de afbakening gemaakt dat de illegale groothandelsactiviteiten in of vanuit Nederland moeten plaatsvinden of Nederlandse belangen aantasten.[5]

Uiteindelijk zijn op basis van deze uitgangspunten zeven dreigingen geïdentificeerd. Hierna volgt een toelichting.

[3] Zie paragraaf 5.3.
[4] Zie paragraaf 4.6 voor de uitgangspunten met betrekking tot de samenhang tussen soorten veranderingen.
[5] Zie paragraaf 1.3 en 4.6.

ICT is een belangrijk consumptie- en kapitaalgoed. Het reguliere bedrijfsleven kan ICT in voldoende mate leveren aan hen die daarvoor de marktprijs willen betalen. Toch is er vraag naar bijvoorbeeld gestolen ICT en ICT leent zich om mee te frauderen. ICT kan daarom fungeren als nieuwe groothandelswaar en vormt een dreiging (*dreiging 1*). Net als legale organisaties kan ook een illegale groothandelsonderneming ICT inzetten in de bedrijfsvoering (*dreiging 2*). Wanneer ICT illegale groothandelswaar vormt en/of illegale groothandelsondernemingen ICT inzetten in de bedrijfsvoering, dan kan dat leiden tot een nieuw soort onderneming: een illegale ICT-handelsonderneming. Die verandering is echter een gevolg van de twee andere veranderingen. Bovendien gaat het hier niet om een verandering in de aard, samenstelling of structuur van ondernemingen. Daarom vormt een illegale ICT-handelsonderneming geen aparte verandering en dus geen aparte dreiging.[6]

Kenmerken ICT-ontwikkelingen:	**Verandering in:**		
	Illegale groothandelswaar	*Illegale groothandels-ondernemingen*	*Illegale bedrijfsvoering*
ICT als consumptie- en kapitaalgoed	1) Illegale ICT als groothandelswaar		2) Inzet ICT in illegale bedrijfsvoering
Informatie als consumptiegoed en productiefactor	3) Illegale informatie als groothandelswaar		4) Vergroting inzet informatie in illegale bedrijfsvoering
Virtuele ruimte		5) Virtuele illegale groothandelsonderne-mingen	6) Omzetting van gewone naar virtuele illegale bedrijfsvoering
ICT-sector en -deskundigen			7) Misbruik van ICT-sector en -deskundigen voor illegale bedrijfs-voering

Figuur 6.1 Overzicht dreigingen georganiseerde criminaliteit als gevolg van ICT-ontwikkelingen

Informatie is een belangrijk consumptiegoed en een belangrijke productiefactor. Het reguliere bedrijfsleven kan deze informatie in voldoende mate leveren aan hen die daarvoor de marktprijs willen betalen. Toch kan gestolen, illegaal gekopieerde en gemanipuleerde informatie als groothandelswaar dienen. 'Illegale informatie als groothandelswaar' is dus een dreiging (*dreiging 3*). Informatie is tevens een belangrijke productiefactor voor legale organisaties. Aan de ene kant kan het bedrijfsleven, andere criminelen, terroristische groepen of staten er veel aan gelegen zijn om over dergelijke informatie te beschikken. Illegaal verkregen informatie kan daardoor interessante handelswaar vormen (dreiging 3). Aan de andere kant kan die informatie dienen als productiefactor. Opsporingsinformatie kan bijvoorbeeld bijdragen aan afscherming. De inzet van dergelijke informatie is niet nieuw. Maar, als gevolg van de ICT-ontwikkelingen zijn de beschikbaarheid van informatie en de mogelijkheden om daar aan te komen, aanzienlijk toegenomen. Illegale groothandelsondernemingen zouden de inzet van informatie in de illegale bedrijfsvoering daarom kunnen vergroten (*dreiging 4*). Wanneer informatie illegale groothandelswaar zou vormen, dan zou dat kunnen leiden tot een nieuw soort onderneming: een illegale informatiehandelsonderneming. Die verandering is echter

[6] Zie ook de uitleg aan het begin van deze paragraaf en paragraaf 4.6 voor de specificatie van 'veranderingen in illegale groothandelsondernemingen'.

een gevolg van de andere verandering en betreft niet de aard, samenstelling of structuur van de ondernemingen.[7] Daarom is dit niet als dreiging benoemd.

De virtuele ruimte speelt nu een cruciale rol. Net als legale ondernemingen kunnen illegale groothandelsondernemingen daarvan gebruikmaken. Zij kunnen handelen in virtuele illegale producten. Dat zijn producten waarvan de koop, verkoop en de distributie volledig in de virtuele ruimte plaatsvinden. Voorbeelden daarvan zijn illegale software en informatie (zonder dozen en fysieke gegevensdragers). Tevens kunnen naast 'gewone' ook virtuele illegale groothandelsondernemingen hun opwachting maken (*dreiging 5*). Dat zijn ondernemingen die de koop, verkoop, en/of de distributie in de virtuele ruimte hebben vormgegeven. Dit type onderneming zou ook bestaansrecht kunnen hebben zonder virtuele handelswaar. De virtuele ruimte leent zich immers in potentie ook voor het aangaan van transacties voor fysieke goederen zoals drugs. Bestaande groothandelsondernemingen kunnen daardoor eveneens de virtuele ruimte benutten voor de bedrijfsvoering door een deel van de gewone bedrijfsvoering om te zetten naar een virtuele (*dreiging 6*). De dreiging 'virtuele illegale groothandelsonderneming' is breder dan die van 'virtuele handelswaar', maar omvat dat laatste wel. Omgekeerd heeft virtuele handelswaar geen zelfstandige betekenis zonder virtuele ondernemingen en een virtuele bedrijfsvoering. Daarom is 'virtuele illegale groothandelswaar' niet als afzonderlijke dreiging beschouwd.

Een ander kenmerk van de ICT-ontwikkelingen is de opkomst van de ICT-sector en ICT-deskundigen. ICT-dienstverlening zou illegale groothandelswaar kunnen vormen. Wanneer de ICT-dienstverlening dient als dekmantel voor facilitering van andere activiteiten, voor witwassen of als investering, dan wordt dat beschouwd als een aspect van de bedrijfsvoering (zie dreiging 7). Daarnaast kan een illegale groothandelsonderneming die diensten verlenen aan andere misdaadondernemingen. Als er behoefte zou zijn aan deze vorm van dienstverlening, hangt dat nauw samen met de andere dreigingen, namelijk 2, 4, 6 en 7. De levering daarvan aan andere misdaadondernemingen is dus een gevolg van die dreigingen en heeft geen zelfstandig bestaansrecht. Een extra argument is dat 'dienstverlening door criminelen aan criminelen' ongeschikt is voor de illegale groothandel. Extra schakels tussen producent en eindconsument hebben geen toegevoegde waarde omdat het gaat om specifieke dienstverlening met een maatwerkkarakter. Deze argumenten gelden ook voor ICT-dienstverlening.[8] Daarom is 'illegale ICT-dienstverlening als groothandelswaar' niet als dreiging benoemd en evenmin 'illegale ICT-dienstenonderneming'. Misbruik van de ICT-sector en -deskundigen ten behoeve van de illegale bedrijfsvoering vormt wel een aparte dreiging (*dreiging 7*). De illegale groothandelsonderneming kan ze gebruiken als dekmantel, voor facilitering van andere activiteiten, voor witwassen of als investering.

Niet alle vormen van criminaliteit die zijn te relateren aan de ICT-ontwikkelingen en die men rekent tot computer-, computergerelateerde, IC(T)-, cyber- of internetcriminaliteit (et cetera) komen in dit hoofdstuk aan bod. Niet deze domeinen vormen het vertrekpunt, maar de combinatie van kenmerken van de ICT-ontwikkelingen en de soorten veranderingen (zie figuur 6.1). Verder geldt als afbakening de in dit proefschrift gehanteerde definitie van

[7] Idem.

[8] Zie hiervoor paragraaf 4.2. Strikt genomen hoort dit argument pas aan de orde te komen bij de beoordeling van de waarschijnlijkheid. In dit geval is hier toch afzonderlijk naar gekeken. Indien in het algemeen deze misdaadmarkt wel geschikt zou zijn, zou ondanks het eerdere argument te overwegen zijn geweest om dit toch als afzonderlijke dreiging te benoemen.

georganiseerde criminaliteit. Het moet gaan om het uitvoeren van illegale groothandels-activiteiten in één of meer misdaadmarkten door een illegale groothandelsonderneming. Vormen van criminaliteit waarbij géén sprake is van handel in illegale producten evenals criminaliteit die níét is gericht op het verdienen van geld, komen dus niet aan bod. Daardoor vallen vele illegale en/of ongewenste activiteiten die een relatie hebben met de ICT-ontwikkelingen buiten de boot. Voorbeelden daarvan zijn: digitale pesterijen, uitings- en verspreidingsdelicten, stalking, het verspreiden van spam, allerlei oplichtings- en afpersingsvormen, cyberterrorisme en information warfare. Het gaat bij deze activiteiten niet om de (groot)handel in illegale producten. Hacken, het verspreiden van virussen, skimming, phishing,[9] distributed denial of service-aanval (dDoS-aanval) (et cetera) zijn instrumenteel voor het realiseren van bepaalde doelen. Dat zijn onder andere het afhandig maken van geld van personen en bedrijven en het verkrijgen van goederen op illegale wijze. Deze activiteiten zijn om dezelfde redenen niet apart genoemd, maar kunnen wel instrumenteel zijn voor de in dit hoofdstuk geïdentificeerde dreigingen. Een delict als 'inbreuk op intellectueel eigendom', ook wel genoemd als ordening bij cybercriminaliteit (et cetera), is het gevolg van bijvoorbeeld aanbod van illegale video's en is daarom evenmin afzonderlijk genoemd.[10]

Als logisch afgeleide van de gehanteerde uitgangspunten voor het beoordelen van de ongewenste effecten, passeren niet alle denkbare effecten de revue. De inzet van ICT en informatie in de illegale bedrijfsvoering of het gebruik van de virtuele ruimte kunnen bijvoorbeeld resulteren in een verbetering van de bedrijfsvoering. Dat kan leiden tot onder andere meer winst, lagere risico's of bewijsvoeringsproblemen voor opsporingsinstanties. Aan de andere kant kunnen juist de risico's toenemen voor de illegale groothandelsonder-neming en dus de inzet leiden tot een verslechtering. Analytisch gaat het hierbij niet om ongewenste effecten.[11]

6.3. Mogelijke gevolgen voor misdaadmarkten en -ondernemingen

Net als legale kunnen ook misdaadondernemingen gaan handelen in ICT of informatie en dat inzetten voor de bedrijfsvoering. Ook zij kunnen de virtuele ruimte benutten voor de handel en/of de bedrijfsvoering. Tevens kunnen zij de ICT-sector en -deskundigen betrekken bij de bedrijfsvoering. Net als in legale markten zou dit in misdaadmarkten kunnen leiden tot innovatie, flexibiliteit en verlaging van de transactiekosten. Misdaad-markten hebben daarentegen enkele bijzondere kenmerken. De vraag doet zich daarom voor in hoeverre deze een stimulans of juist een belemmering vormen voor veranderingen. Ook is het de vraag in hoeverre aan de randvoorwaarden is voldaan om de ICT-ontwikke-lingen daadwerkelijk te benutten. In het vervolg van deze paragraaf komen deze vraagstukken aan bod.

[9] Skimming betreft het kopiëren van pinpasgegevens. Bij phishing gaat het om het achterhalen van andermans gegevens op een slimme wijze (vissen), zoals wachtwoorden, pincodes en dergelijke. Dat kan bijvoorbeeld door een website te exploiteren die veel gelijkenis heeft met die van een echt bedrijf zoals een bank {DNRI, 2004, 76-77, 93-94}.

[10] De volgende auteurs gaan in op de vele varianten van criminaliteit die zijn gerelateerd aan de ICT-ontwikkelingen {Boni & Kovacich, 1999}, {Galeotti, 2000B}, {Hoogenboom, 2001}, {NCIS, 1999}, {O'Brien, 2000}, {Power, 2000A}, {Power, 2000B}, {Robinson, 2000}, {Stol e.a., 1999A}, {Stol e.a., 1999B}, {Vriesde e.a., 1999}, {Williams, 1999}.

[11] Zie paragraaf 4.8.

In het legale bedrijfsleven doet zich voortdurend innovatie voor als gevolg van de ICT-ontwikkelingen. In tegenstelling tot in legale markten is er echter in misdaadmarkten geen aanleiding om te innoveren. *Allereerst* ontbreekt daarvoor een commerciële noodzaak. Er is geen sprake van open concurrentie. Eindconsumenten bundelen de krachten niet en kunnen geen vuist maken. Er is geen consumentenbond die aan kwaliteits- en prijsvergelijking doet. Aandeelhouders zijn er niet. De macht van afnemers en leveranciers is bovendien beperkt, omdat ze afhankelijk zijn van netwerken. Vertrouwen in de zakenpartners speelt een belangrijkere rol dan aspecten als stipte levering. Bovendien zijn de marktpartijen niet in een grote concurrentiestrijd met elkaar gewikkeld om prijs of kwaliteit. Een *tweede reden* is dat er vanuit de aard van de processen geen reden is tot innovatie. Het gaat om eenvoudige logistieke processen. Vanwege de imperfecte marktwerking en de noodzaak van vertrouwen, hoeft een misdaadonderneming geen goederen te betrekken van tientallen producenten en enkele keren per dag aan tientallen afnemers te leveren. Dit in tegenstelling tot bijvoorbeeld de legale supermarktconcerns. Navenant zijn de informatieprocessen eveneens eenvoudiger dan van de legale tegenhangers. Vanuit de processen is er dus geen directe noodzaak om over te gaan tot vernieuwing.

Een *derde reden* waarom er geen aanleiding is om te innoveren is dat de huidige illegale producten zich niet lenen voor digitalisering. Het gaat immers overwegend om fysieke goederen en fysieke vormen van dienstverlening die bovendien eenvoudig van aard zijn.[12] Natuurlijk zouden de misdaadondernemingen kunnen overgaan tot productinnovatie. Maar, dan moet wel aan de randvoorwaarden voor innovatie zijn voldaan (zie hierna). Kinderporno-afbeeldingen en illegaal gokken zijn uitzonderingen die zich wel lenen voor digitalisering en daar kan wel worden gesproken van innovatie van de producten en de processen. Bestaand kinderpornomateriaal wordt bijvoorbeeld op allerlei manieren veranderd en als nieuw aangeboden. Verder heeft de virtuele ruimte een belangrijke rol ingenomen voor de distributie van dat materiaal. Maar, eerder is beargumenteerd dat kinderporno-afbeeldingen juist (mede) als gevolg van de ICT-ontwikkelingen niet geschikt zijn als illegale groothandelswaar.[13] Illegaal gokken is eveneens vernieuwd: dat vindt nu tevens in de virtuele ruimte plaats. Volgens NCIS waren er aan het einde van 1998 naar schatting 1000 goksites toegankelijk via het internet. Door technische verbeteringen en een grotere bandbreedte zal dit aantal sindsdien alleen maar zijn toegenomen. In augustus 1998 waren er ongeveer 160 virtuele casino's toegankelijk via het internet, waarvan ongeveer 70% zich bevonden in het Caraïbisch gebied.[14] Het aanbieden van gokdiensten via het internet hoeft niet altijd illegaal te zijn. De wetgeving verschilt tussen landen. Voor een Nederlandse misdaadonderneming is het mogelijk om vanuit Nederland een virtueel casino te exploiteren in het Caraïbisch gebied of juist omgekeerd. Naast criminelen kunnen ook legale ondernemers gokdiensten aanbieden vanuit vele landen. Criminelen moeten dus niet alleen concurreren met andere criminelen, maar tevens met legale ondernemingen. Er bestaat weliswaar veel vraag naar gokdiensten, maar het aantal aanbieders is eveneens groot. Zowel aan de vraag- als de aanbodzijde is de markt versnipperd. Het is twijfelachtig of een individuele digitale gokonderneming op grote schaal klanten kan aantrekken en behouden. Succes laat zich snel kopiëren en klanten kunnen snel wisselen van digitaal casino. Een ander probleem is dat het betalingsverkeer op klassieke wijze moet verlopen, waardoor bewijssporen ontstaan. Door zich virtueel te vestigen in een land waar gokken

[12] Zie subparagraaf 3.6.3.
[13] Zie paragraaf 4.2.
[14] {NCIS, 1999, 12}.

legaal is, speelt dit probleem niet. In feite is dan geen sprake meer van illegaal gokken. Bovendien kunnen vragers en aanbieders elkaar vinden via zoekmachines. Daardoor is er geen rol voor een illegale groothandel. Al met al is het dus niet aannemelijk dat digitaal gokken op groothandelsniveau geschikt is als illegale dienstverlening. Kortom, de illegale producten die zich wel lenen voor digitalisering, zijn in elk geval niet geschikt als illegale groothandelswaar.

Een *vierde reden* waarom er geen aanleiding is om te innoveren is dat een (misdaad)onderneming zonder (grootschalig) gebruik van ICT voorlopig nog prima kan functioneren. Maar, naarmate legale organisaties op steeds grotere schaal ICT gebruiken, ontkomt ook de misdaadonderneming er op enig moment niet aan om mee te doen. Een importeur van drugs heeft vrachtbrieven nodig van de lading waarin de drugs zijn verstopt. Documenten zoals vrachtbrieven komen steeds vaker tot stand met behulp van ICT-toepassingen. Wanneer legale bedrijven in toenemende mate met de fiscus en douane digitale transacties afsluiten en op digitale wijze communiceren, moet ook de misdaadonderneming de werkwijze veranderen. Op de korte termijn speelt dit nog niet, ondanks dat ICT in alle haarvaten van onze samenleving is doorgedrongen. Een misdaadonderneming kan natuurlijk wel proberen om aan bijvoorbeeld vrachtbrieven te komen door middel van misbruik van ICT-toepassingen. Zie hiervoor paragraaf 6.7.

Wanneer de knelpunten van het opereren in de illegaliteit zouden kunnen verminderen, dan zou wel een prikkel bestaan voor veranderingen. Het krijgen van betrouwbaar en deskundig personeel blijft echter een probleem. Het plaatsen van personeelsadvertenties via het internet is bijvoorbeeld even riskant als in de krant. Wel kan een misdaadonderneming een beroep doen op medewerkers of deskundigen aan de andere kant van de wereld. Randvoorwaardelijk blijft dan nog steeds dat de identiteit bekend is en iemand is te vertrouwen. Er bestaat dan geen principieel verschil tussen het communiceren via de telefoon of fax en het communiceren in de virtuele ruimte. Het personeelsprobleem wordt wellicht zelfs nog nijpender. Om te profiteren van de mogelijkheden moet de misdaadonderneming immers een beroep doen op ICT-deskundigen. Deze zijn schaars en het is maar de vraag of zij beschikbaar zijn in de netwerken van de misdaadondernemingen.

Ook beheersing van informatie is een probleem voor een misdaadonderneming. Communicatie en administratie zijn immers riskant, maar wel cruciaal voor het functioneren. De communicatiemiddelen en -media zijn als gevolg van de ICT-ontwikkelingen aanzienlijk verbeterd. Criminelen spelen daar op in. Zo gebruiken zij volop mobiele telefoons en wisselen ze regelmatig van nummer. Het afluisteren van mobiele telefoons is niet onmogelijk, maar is lastiger dan van een vast toestel. Volgens NCIS en Aalbersberg gebruiken criminele groepen het internet om te communiceren via e-mail en om hun activiteiten te organiseren. In de virtuele ruimte kan een misdaadonderneming relatief anoniem communiceren in de massaliteit van informatie. In combinatie met encryptie is de bewijsvoering voor opsporingsinstanties niet eenvoudig. Soms hebben opsporingsinstanties (tijdelijk) moeite om dergelijke middelen en media af te luisteren en de bewijsvoering rond te krijgen. Toch bestaat er geen garantie dat opsporingsinstanties de communicatie niet afluisteren. Bovendien blijft in misdaadmarkten oog-in-oog-communicatie noodzakelijk, zeker bij conflicten.[15] ICT kan verder de administratieve processen ondersteunen. De

[15] {NCIS, 1999, 18} interview met Aalbersberg (bijlage 4), paragraaf 5.6 en {DNRI, 2004, 44}. Kleemans e.a. gaan uitvoerig in op communicatiemanieren en de problemen daarvan {Kleemans e.a., 2002}.

misdaadonderneming kan via het internet bijvoorbeeld de administratie spreiden over diverse landen en diverse bestanden. Zij kan de administratie in een zakcomputer met behulp van encryptie bijhouden in plaats van in het kwetsbare zakboekje of in het geheugen. Toch vormen versleutelde of verspreide administraties geen waarborg voor geheimhouding. Privacybescherming en beveiliging van gegevensopslag en -transport kennen ook voor de misdaadonderneming beperkingen.[16] Misdaadondernemingen kunnen dus (slechts) tot op zekere hoogte profiteren van de ICT-ontwikkelingen voor de communicatie en de administratie.

Beheersing van geld is evenzeer een probleem voor een misdaadonderneming. De ICT-ontwikkelingen hebben fundamentele wijzigingen tot stand gebracht in legale financiële markten. Banken zijn volop actief in de virtuele ruimte. Toch laat een echte doorbraak van nieuwe betalingsmethoden nog op zich wachten. Voorzover je al kunt betalen in de virtuele ruimte, is de betaling gekoppeld aan de reguliere betalingssystemen. Daardoor leveren digitale geldtransacties nog steeds bewijssporen op. Daarom is het betalingsverkeer in de virtuele ruimte niet geschikt voor directe betalingen tussen misdaadondernemingen, leveranciers en afnemers. Dit geldt in het bijzonder voor betalingen met vele onbekenden. Tevens blijft het basisprobleem bestaan, namelijk het verantwoorden van het geld en de bezittingen tegenover de overheid en het vermijden van bewijssporen. De ICT-ontwikkelingen bieden hiervoor niet tot nauwelijks soelaas.

Een ander knelpunt is dat de misdaadonderneming voortdurend de criminele handel en wandel moet afschermen. Aalbersberg nam in 2000 een lichte tendens waar dat Turkse criminelen ICT gebruikten voor afscherming. Hij constateerde toen bijvoorbeeld een lichte groei in het gebruik van ICT voor beveiliging van het eigen huis.[17]

Er komen dus in het algemeen geen prikkels tot innovatie vanuit misdaadmarkten, de processen of de producten. De ICT-ontwikkelingen kunnen evenmin de knelpunten structureel verminderen, met uitzondering van het informatiebeheer en de afscherming. Wanneer er wel prikkels zouden bestaan, is het nog maar de vraag of de randvoorwaarden voor innovatie wel aanwezig zijn. De netwerken waarin misdaadondernemingen samenwerken, lenen zich in beginsel voor innovatie.[18] Maar, zelfstandig werkende medewerkers, intensieve samenwerking met medewerkers van andere misdaadondernemingen, integratie van processen en open samenwerking tussen producenten en consumenten, passen niet bij het vijandige en ongereguleerde karakter van misdaadmarkten. En eerder is al aangegeven dat misdaadondernemingen vooral (en slechts) flexibel zijn, wanneer zij in hun voortbestaan worden bedreigd. Dat is niet het geval op basis van de ICT-ontwikkelingen. En ruimte en prikkels om voor de lange termijn te investeren, zijn er evenmin.[19] Kortom, aan de randvoorwaarden voor innovatie is niet voldaan.

De ICT-ontwikkelingen resulteren in het legale bedrijfsleven in een daling van de transactiekosten tussen en binnen organisaties. Dit geldt zowel binnen als buiten de virtuele ruimte. ICT kan in de virtuele ruimte de vergaring van informatie over de markt, de ondernemingen en de producten verregaand vereenvoudigen. Dat draagt bij aan een

[16] Zie paragraaf 5.7.
[17] Zij bijlage 4.
[18] Zie paragraaf 5.5.
[19] Zie subparagraaf 3.7 en 4.3.3.

verlaging van de transactiekosten. Maar, dan moeten de marktdeelnemers die informatie wel beschikbaar stellen. Binnen misdaadmarkten is dit absoluut niet te verwachten. Transparantie voor elkaar betekent ook transparantie voor opsporingsinstanties. Bovendien bepaalt niet de informatie over de producten en de onderneming de keuze met wie men zakendoet, maar het vertrouwen in de partner. En, een commerciële noodzaak tot veranderingen die zouden kunnen leiden tot een daling van de transactiekosten ontbreekt. Kortom, transparantie valt niet te verwachten en daar komt in elk geval geen verlaging van de transactiekosten uit voort.

De transactiekosten kunnen ook dalen door integratie van processen. Dat vraagt echter nogal wat van het vertrouwen in de samenwerkingspartners. Integratie betekent immers meer afstemming, meer informatie-uitwisseling en grotere transparantie van de bedrijfsvoering. Niet alleen kunnen kwaadwillende criminelen hiervan profiteren, maar ook opsporingsinstanties. Bovendien neemt door integratie de complexiteit van de bedrijfsvoering toe en is een ander concept van bedrijfsvoering nodig. Dit vereist een mentale omslag. Zelfs in het legale bedrijfsleven maakt niet iedere ondernemer die stap (al). En al eerder is gezegd dat een commerciële noodzaak daartoe ontbreekt en dat evenmin aan de randvoorwaarden voor innovatie is voldaan. Doordat men in misdaadmarkten dus niet zal overgaan tot integratie van processen, zullen de transactiekosten niet dalen.

Ook het verdwijnen van marktschijven kan bijdragen aan een verlaging van de transactiekosten. Misdaadmarkten hebben te kampen met relatief veel marktschijven. Deze vloeien voort uit de barrières voor schaalgrootte en de wens tot risicobeperking. En hoewel eerder is aangegeven dat met de inzet van ICT het informatieknelpunt iets minder nijpend is, blijven de (andere) beperkingen bestaan. De spanningsvelden tussen zakendoen en geheimhouding en tussen vertrouwen en geweld blijven onverkort van toepassing. Wel biedt de virtuele ruimte enige kansen om op wereldwijde schaal anoniem te opereren en de bewijsvoering is ingewikkeld en arbeidsintensief.[20] Die anonimiteit werkt echter twee kanten op. Niet alleen de misdaadondernemer blijft in zeker mate anoniem, maar ook de zakenpartner die plotsklaps opsporingsambtenaar kan blijken te zijn. Doordat de locatie van de zakenpartner niet vaststaat, is ook niet helder waar men moet zijn om geweld toe te passen. Zakendoen met onbekenden is daarom riskant en onverstandig. Naast deze redenen, zijn er ook nog andere waarom vertrouwen zo belangrijk is. In de virtuele ruimte ontbreken garanties die er wel zijn in de fysieke wereld. De bestelling, de levering en de betaling vinden niet gelijktijdig plaats. Dit levert bij het legaal zakendoen al complicaties op[21] en al helemaal bij het zakendoen in misdaadmarkten. Creditcardmaatschappijen compenseren het financiële risico voor een legale leverancier en consument, maar niet voor een ondernemer of consument in misdaadmarkten. Legale leveranciers kunnen ofwel gebruikmaken van de goede naam die ze hebben of investeren in naamsbekendheid. De consument weet dan met wie hij zaken doet. Bij misbruik kan hij de betaling proberen terug te draaien en aangifte doen bij de politie. Een consument die zaken doet met een misdaadonderneming, kan deze voorzieningen niet gebruiken. Vertrouwen in elkaar is in virtuele misdaadmarkten daarom nog belangrijker dan in fysieke misdaadmarkten. Zakendoen met weinigen in netwerken blijft dus noodzakelijk om de risico's binnen de perken te houden. Daardoor is de virtuele ruimte niet geschikt als marktplaats voor illegale producten, tenzij men de ander kent. In dat geval is er geen fundamenteel verschil tussen

[20] Zie paragraaf 5.6.
[21] Zie paragraaf 5.7.

telefoneren of het gebruik van e-mail. Op grond van dit betoog is het niet waarschijnlijk dat het aantal marktschijven in misdaadmarkten zal afnemen. Daardoor zal dus ook geen verlaging van transactiekosten optreden.

Innovatie van processen en de daling van transactiekosten in het legale bedrijfsleven hebben geleid tot nieuwe vormen van flexibiliteit. Daarnaast heeft de slimme inzet van ICT de nadelen van samenwerking in netwerken gereduceerd. Daardoor kan eveneens de flexibiliteit toenemen. Grotere flexibiliteit versterkt de concurrentiepositie van bedrijven, terwijl omgekeerd bedrijven dat wel moeten nastreven vanwege de concurrentie. Zoals eerder is aangegeven, ontbreekt in misdaadmarkten een commerciële noodzaak om veranderingen door te voeren. Dat geldt ook voor flexibeler werken om de klanten te behagen. Verder is aangenomen dat innovatie van processen en een daling van transactiekosten niet te verwachten vallen. In misdaadmarkten werkt(e) men wel al samen in netwerken. Maar, als gevolg van de spanningsvelden van het opereren in de illegaliteit, kan de inzet van ICT niet alle nadelen van netwerken verminderen. Wel reageren misdaadondernemingen flexibel op de activiteiten van toezichthoudende en opsporingsinstanties. Hoewel deze instanties zeker ICT inzetten, lopen zij daarin niet voorop. In elk geval is er geen reden om aan te nemen dat daardoor misdaadondernemingen een grotere flexibiliteit moeten betrachten. En zelfs dan is het maar de vraag of zij die extra flexibiliteit zouden kunnen realiseren. De randvoorwaarden voor innovatie zijn immers niet gunstig.

Op basis van deze redenering is de aanname dat innovatie, verlaging van transactiekosten en vergroting van de flexibiliteit zich niet zullen voordoen. Evenmin zal sprake zijn van de daaruit resulterende productiviteitsverhoging en vergroting van het concurrentievermogen. Los van bovenstaande argumenten, is het ook nog maar de vraag of benutting van de ICT-ontwikkelingen wel past bij het profiel, de intentie en de bekwaamheden van de huidige populatie van misdaadondernemers. Er bestaan immers niet alleen grenzen aan wat iemand kan, maar ook aan wat iemand wil. Zij zullen op zijn minst van het bestaan van pc's, het internet en e-commerce op de hoogte zijn. In het gewone functioneren als burger komen zij daarmee in contact. Bij criminelen zijn bijvoorbeeld zakcomputers, personal computers en satelliettelefoons aangetroffen. Maar, zakendoen en communiceren achter de pc en de handel in informatie en ICT zijn niet echt avontuurlijk te noemen. Zelfs legale ondernemers hebben de ICT-ontwikkelingen nog lang niet altijd benut, ondanks de commerciële noodzaak daartoe. Volgens DNRI lijkt het gros van de criminelen (nog) weinig kennis te hebben van ICT.[22]

Maar, wat nu als de huidige populatie van illegale groothandelaren en groothandelsondernemingen gaat veranderen? Stel dat bijvoorbeeld hackers op het criminele pad gaan. Volgens Galeotti zijn de meeste cybercriminelen 16- tot 24-jarigen wier computervaardigheden excellent zijn, maar die nog weinig idee hebben hoe ze hun kennis kunnen benutten om winst te maken. Van elke hack leren zij. Wanneer zij in de gevangenis belanden en in contact komen met criminelen, kan een verbinding ontstaan tussen criminelen en hackers.[23] Zij zouden zich ook kunnen richten op de handel in illegale producten. Daardoor zouden zich geleidelijk wel degelijk veranderingen kunnen voordoen in misdaadmarkten en -ondernemingen. Toch is dat niet aannemelijk. De beperkingen van de misdaadmarkten en het misdaadondernemerschap gelden immers eveneens voor hen. Ook voor hen geldt dat

[22] {DNRI, 2004, 44}.
[23] {Galeotti, 2000A}.

niet alle producten zich lenen als illegale groothandelswaar en dat zij niet zomaar de rol van illegale groothandel op zich kunnen nemen. En vanwege de kenmerken van misdaadmarkten zal de behoefte aan illegale groothandelsondernemingen ook in de toekomst blijven bestaan.[24] Zij vervullen immers een waardevolle rol voor de marktpartijen. Illegale groothandelsondernemingen zullen dus niet verdwijnen en de persoonlijke drempels voor nieuwkomers zijn hoog.

Alles overziend lijkt het er op dat misdaadondernemingen, waaronder de illegale groothandelsondernemingen, slechts beperkt (kunnen) profiteren van de ICT-ontwikkelingen. Deze constatering sluit aan bij de bevindingen van de onderzoekers van het Nationaal Dreigingsbeeld.[25] De misdaadondernemingen zullen vooral kleinschalig en geleidelijk inspelen op de nieuwe mogelijkheden. Aannemelijk is dat zij eerst ICT gebruiken voor communicatie, de administratie en afscherming. Dit zijn immers belangrijke knelpunten voor een misdaadonderneming en ICT kan deze enigszins verminderen. Geleidelijk zullen zij andere opties verkennen en benutten. De mate waarin is mede afhankelijk van de druk vanuit misdaadmarkten zelf, de samenleving en toezichthoudende en opsporingsinstanties.

6.4. Illegale ICT als groothandelswaar

6.4.1. Omschrijving

ICT is een legaal product waarvoor een legale markt bestaat. Desondanks kan ICT illegale handelswaar vormen. Onder ICT valt zowel hardware als software waaronder besturingssoftware (bijvoorbeeld Windows) en applicatiesoftware (bijvoorbeeld Microsoft Word). Onder hardware vallen zowel complete computers, computeronderdelen (bijvoorbeeld chips) als telefoongerelateerde hardware zoals een mobiele telefoon.

Vanwege de ruime beschikbaarheid van ICT bestaan er vele mogelijkheden voor diefstal van een individueel exemplaar tot en met complete containers. Net als bij andere gestolen goederen kan de illegale groothandel de gestolen waar opkopen van helers en doorverkopen aan anderen.

ICT leent zich ook als instrument voor overtreding van fiscale en douanewetgeving. ICT is hiervoor aantrekkelijk omdat het gaat om relatief kleine goederen met een hoge waarde. Zo spelen in zogenaamde BTW-carrousels geheugenchips een belangrijke rol. De chips maken vele grensoverschrijdende bewegingen als gevolg van de fictieve handel. Dit leidt elke keer tot compensatie van de betaalde BTW. Wanneer de overheid uiteindelijk de BTW in het land van bestemming wil heffen, heeft zij het nakijken. De fraude als gevolg van de handel is een feit. Hoewel het van dit type ondernemingen eigenlijk helemaal niet de bedoeling is om de handelswaar echt te verkopen, doen zij zich wel voor als groothandel. Zij handelen immers in het groot, omdat dat meer geld oplevert. Zij verkopen niet aan eindconsumenten, maar (zogenaamd) aan andere BTW-plichtigen (detail- of groothandel). De verdiensten zitten in de gefingeerde verkopen en de daaraan gerelateerde fraude ten koste van één of meer van de Europese lidstaten. Ondanks het feit dat deze illegale

[24] Zie de paragrafen 3.5, 3.7 en 3.8 voor de rol van illegale groothandelsondernemingen in misdaadmarkten en paragraaf 3.6 voor de kenmerken van misdaadmarkten.
[25] {DNRI, 2004, 44}.

groothandelsondernemingen feitelijk geen illegale goederen verkopen, is toch aangenomen dat deze goederen zich lenen als illegale groothandelswaar.

Software leent zich voor illegaal kopiëren (vervalsing). De kosten om software te kopiëren vormen een fractie van de investeringskosten. Dit creëert een aanzienlijke prijswig. Onderscheid moet daarbij worden gemaakt tussen illegaal kopiëren zoals dat op elke pc kan plaatsvinden zonder professionele kennis (illegale kopieën van software) en professionele vervalsingen, inclusief de bijbehorende certificaten, verpakkingsmateriaal en handleidingen (vervalste fysieke software). Hardware leent zich eveneens voor vervalsen. Een bijzondere vorm is het manipuleren van de sim-kaart van een mobiele telefoon. Telecom-bedrijven verkopen de gsm's onder de marktprijs en hopen het geld terug te verdienen met het gebruik van het toestel. Door de sim-kaart te manipuleren, kan de crimineel het toestel verkopen tegen een hogere prijs, zonder de beperkingen van de leverancier. Men duidt dit wel aan als telecomfraude. In de kern gaat het daarbij om oplichting. Hoewel het illegaal kopiëren en vervalsen zelf níét worden gerekend tot de illegale groothandel, valt het handelen in die producten daar wel onder.

6.4.2. Beoordeling waarschijnlijkheid

ICT verschilt niet fundamenteel van andere goederen met een (fiscale) prijswig, gestolen goederen en goederen waarbij inbreuk is gemaakt op (intellectuele) eigendomsrechten. In het algemeen zijn soortgelijke goederen geschikt voor de illegale groothandel. Een bijzonder aspect is wel dat ICT veelal klein is en een hoge waarde vertegenwoordigt. Vanwege de relatief hoge prijzen en de snelle technische veroudering zullen er altijd mensen zijn die graag voor minder geld de beschikking krijgen over ICT. Dit geldt vooral voor de nieuwste snufjes. ICT kan verder in ontwikkelingslanden een schaars goed zijn. Er is dus een misdaadmarkt voor illegale ICT. Net als bij soortgelijke illegale goederen hebben de groot- en detailhandel een toegevoegde waarde. Er zijn vele dieven, oplichters en dergelijke en vele eindconsumenten die niet rechtstreeks zaken met elkaar kunnen doen. Het potentiële handelsvolume is groot genoeg voor extra schakels. Wel zouden vraag en aanbod in de virtuele ruimte bij elkaar kunnen komen. Het aanbod van illegale hard- en software valt niet noodzakelijkerwijze op, omdat er veel handel plaatsvindt in hard- en software. Illegale ICT is dus geschikt als illegale groothandelswaar, maar een deel van de handel zou ook zonder tussenkomst van de groothandel kunnen verlopen.[26]

In het Nationaal Dreigingsbeeld stelt men dat piraterij van software (en audio en video) zich niet alleen leent voor particulieren, maar ook voor georganiseerde criminaliteit. Groepen die zich daar mee bezighouden, zijn vooral uit het buitenland bekend. Men wijt dit mede aan de geringe opsporingsprioriteit in Nederland waardoor sprake is van een groot dark number. Piraterij van software, audio en video wordt beschouwd als dreiging.[27] Er wordt echter geen onderscheid gemaakt tussen fysieke vervalsingen, inclusief de dozen, certificaten van echtheid et cetera, en digitale kopieën zoals deze op vrijwel elke nieuwe pc kunnen worden aangemaakt. Evenmin specificeert men of de particuliere hobbyisten en georganiseerde criminaliteit zich met dezelfde vormen van piraterij bezighouden. Het illegaal kopiëren van software is eenvoudig en de kopieën zijn gemakkelijk te distribueren via cd's of het internet. Eindconsumenten en producenten kunnen daardoor eenvoudig met

[26] Zie paragraaf 4.2 voor de factoren die hierop van invloed zijn.
[27] {DNRI, 2004, 75-76}.

elkaar in contact komen en de morele drempel om illegaal gekopieerde software te produceren en aan te schaffen, ligt laag.[28] En hoewel strikt genomen gestolen of vervalste fysieke en illegaal gekopieerde software tot dezelfde misdaadmarkt behoren, bestaat toch een verschil. Er zijn immers minder partijen die kunnen beschikken over gestolen fysieke software of in staat zijn om de verpakking (et cetera) van fysieke software te vervalsen. Evenmin kunnen eindconsumenten en producenten eenvoudig met elkaar in contact komen. Het ligt immers minder voor de hand om op bijvoorbeeld een verjaardagspartij of het schoolplein (gestolen) originele dozen met software aan te bieden. De drempel ligt daarvoor hoger dan voor illegaal gekopieerde software. Daarom is de aanname dat er wel een rol is weg gelegd voor de illegale groothandel voor gestolen of vervalste fysieke software, maar niet voor illegaal gekopieerde.[29]

Er zullen zeker misdaadondernemingen zijn die de functies van de groothandel voor hun rekening willen en kunnen nemen. De handel in illegale ICT kan winst genereren. In relatie tot andere goederen is ICT klein ten opzichte van de waarde. Daardoor zijn de risico's voor de misdaadonderneming kleiner dan bij andere goederen zoals auto's, of lage-waarde-goederen zoals sigaretten of vlees. ICT spreekt wellicht niet tot de verbeelding van een illegale groothandelaar[30], maar kan wel winstgevend zijn. De handel in ICT stelt geen bijzondere eisen aan de bedrijfsvoering. Hooguit is voor de handel in vervalsingen en kopieën enige materiekennis vereist om zelf niet opgezadeld te worden met al te opzichtige vervalsingen of slechte kopieën.

Sociale controle is tot op zekere hoogte mogelijk. Net zo goed als slachtoffers van andere gestolen goederen, kunnen de slachtoffers van gestolen ICT toezien op hun goederen en een beroep doen op opsporingsinstanties wanneer ze zijn gestolen. Wanneer de goederen worden aangeboden in de virtuele ruimte, zijn er mogelijkheden om hiernaar te zoeken. Voor de overheid en opsporingsinstanties maakt het geen verschil uit of het gaat om ICT of andere gestolen goederen. Bij fraude is de overheid het slachtoffer en heeft ze, net als bij andere vormen van fraude, mogelijkheden om dit te voorkomen of aangifte te doen bij opsporingsinstanties. Voor vervalsingen en illegale kopieën heeft de ICT-branche een groot belang bij sociale controle. Ook hier kan de branche gericht naar zoeken wanneer ze worden aangeboden in de virtuele ruimte. Voor de anderen, waaronder de overheid en opsporingsinstanties, maakt deze vorm van vervalsing geen verschil ten opzichte van andere vormen. Lastig is wel dat voor illegale kopieën van software er vele aanbieders en vragende partijen zijn en het min of meer sociaal geaccepteerd lijkt te zijn. Dit beperkt de mogelijkheden voor sociale controle. Al met al verschilt ICT voor sociale controle niet fundamenteel van andere gestolen waar, goederen met een fiscale prijswig en vervalsingen en is sociale controle niet onmogelijk.

In het algemeen bestaan er in Nederland geschikte mogelijkheden voor de illegale groothandel in soortgelijke goederen. Er is geen argument om aan te nemen dat dit niet geldt voor ICT. Zo is ICT in Nederland in ruime mate voorhanden, er vindt een levendige legale handel plaats, de bevolking van Nederland loopt niet achter in kennis over ICT en de

[28] Het gemak, het grote aanbod en de grote vraag in de virtuele ruimte, evenals de acceptatie van illegaal kopiëren blijken nadrukkelijk uit het onderzoek van Svensson en Van Wijk. Tevens noemen zij geschatte percentages van illegale software in Europa en Nederland. Deze liggen hoog {Svensson & Van Wijk, 2004, 29-40, 45-50, 77}.
[29] Zie verder ook de argumentatie voor illegaal gekopieerde audio en video (subparagraaf 6.6.2).
[30] Zie subparagraaf 4.3.2 voor het profiel van illegale groothandelaren.

productie en handel zijn niet voorbehouden aan specifieke landen of etnische groepen. Omgekeerd is Nederland niet extra aantrekkelijk ten opzichte van andere landen. Nederland wijkt immers op deze kenmerken niet substantieel af van andere ontwikkelde landen.

Alles overziend is de waarschijnlijkheid van 'illegale ICT als groothandelswaar' hoog vanwege vooral de geschiktheid van illegale ICT als groothandelswaar. Een uitzondering daarop is de deeldreiging 'illegale kopieën van software als groothandelswaar'. De waarschijnlijkheid daarvan is laag.

6.4.3. Beoordeling ongewenste effecten

ICT is een legaal product en gaat op zichzelf niet gepaard met ongewenste effecten. De handel in illegale ICT resulteert wel in ongewenste effecten doordat anderen in de misdaadmarkt worden gestimuleerd om criminaliteit te plegen. Dit leidt tot een aantasting van de veiligheid bij gestolen ICT en een financieel verlies bij de slachtoffers van diefstal en/of de producenten en/of de kopers. De handel in ICT als instrument voor fraude resulteert in financieel verlies voor één van de Europese overheden. Doordat ICT een hoge waarde vertegenwoordigt, leidt fiscale fraude met ICT (wellicht) tot een hogere dan gemiddelde schadepost. Wanneer Nederlandse illegale groothandelsondernemingen hun activiteiten ook richten op het buitenland, kan dat leiden tot schade aan de buitenlandse betrekkingen. De handel in illegale ICT stelt in beginsel geen bijzondere eisen aan de onderneming of aan de bedrijfsvoering ten opzichte van vergelijkbare illegale goederen. Daar komen dus geen bijzondere effecten uit voort.

6.5. Inzet ICT in illegale bedrijfsvoering

6.5.1. Omschrijving

Net als een legale onderneming kan ook een illegale groothandelsonderneming ICT gebruiken als kapitaalgoed ten behoeve van bijvoorbeeld de communicatie, administratie, afscherming of logistieke afhandeling van goederenstromen. Zo vergt de drugshandel een logistiek proces dat zij met behulp van ICT kan proberen te verbeteren. De inzet kan op zichzelf staan, maar kan ook voortkomen uit één of meer van de andere genoemde veranderingen.[31] Wanneer groothandelsondernemingen bijvoorbeeld gaan handelen in illegale informatie, kan het noodzakelijk zijn om ICT in te zetten in de bedrijfsvoering. De inzet van ICT met uitsluitend als doel om een virtuele bedrijfsvoering op te zetten, valt onder 'omzetting van gewone naar virtuele illegale bedrijfsvoering'.

6.5.2. Beoordeling waarschijnlijkheid

Eerder is aangegeven dat de voordelen van de inzet van ICT beperkt zijn. En zelfs in die gevallen dat er voordelen zijn te behalen, kleven er ook risico's aan. Tevens is aangegeven dat aan de randvoorwaarden voor veranderingen niet is voldaan. Verder sluit de inzet van ICT niet aan bij de bestaande werkwijze en het profiel van de illegale groothandelaar.[32, 33]

[31] In bijlage 2 zijn de relaties tussen deze en andere dreigingen gespecificeerd.
[32] Zie paragraaf 6.3.

Op basis van bovenstaande redenering is niet te verwachten dat illegale groothandelsondernemingen op grote schaal en structureel ICT gaan inzetten als kapitaalgoed. De inzet van ICT voor communicatieve, administratieve en afschermingsdoeleinden vormt daarop een uitzondering.[34] De mogelijkheden om met behulp van ICT de communicatie af te schermen, zijn fors toegenomen. "Het is bekend dat grotere groeperingen ICT-methoden toepassen bij contrastrategieën, zij het vooralsnog op beperkte schaal [….]". Maar, het gebruik van de nieuwe mogelijkheden is nu nog beperkt.[35] Wanneer de inzet randvoorwaardelijk is voor één van de andere veranderingen, bijvoorbeeld voor de handel in illegale informatie, dan zouden groothandelsondernemingen wel kunnen overgaan tot de inzet van ICT. Die veranderingen zijn in de overige paragrafen als niet waarschijnlijk gekwalificeerd en daardoor is de randvoorwaardelijke inzet van ICT evenmin waarschijnlijk.

De illegale groothandelsonderneming kan op uiteenlopende wijzen aan ICT komen zoals door diefstal of gewone aanschaf. Gezien het karakter van de groothandelsonderneming ligt gewone aanschaf meer voor de hand dan diefstal. Waarom extra risico's lopen door met een boodschappenlijstje in de hand in het criminele circuit op zoek te gaan naar ICT of dat zelf te stelen? Verkopers kunnen immers niet beoordelen waarom iemand ICT aanschaft en bovendien zijn er vele legale verkopers actief in de markt. De verkopers kunnen daardoor onbewust zakendoen met criminelen. Sociale controle op de aanschaf is moeilijk uitvoerbaar en bovendien is het voor de verkopers ook nog eens profijtelijk. Verder hebben zij geen direct belang om controle uit te oefenen. Maar, net zo goed als dat ICT legale ondernemingen kwetsbaar maakt voor misbruik, maakt de inzet ervan misdaadondernemingen kwetsbaar. Daar waar bijvoorbeeld hackers binnen legale ondernemingen op zoek kunnen gaan naar informatie, kunnen opsporingsinstanties dat bij misdaadondernemingen. Wel kunnen nieuwe vraagstukken ontstaan en zijn nog niet op alle terreinen daarvoor oplossingen bedacht of geïmplementeerd.[36] Sociale controle is dus tot op zekere hoogte uitvoerbaar.

Alles overziend is de waarschijnlijkheid van 'inzet van ICT in illegale bedrijfsvoering' laag doordat de voordelen niet substantieel opwegen tegen de nadelen, er geen aanleiding is en de randvoorwaarden niet optimaal zijn. Een uitzondering daarop is de inzet voor communicatie, administratie en afscherming. De waarschijnlijkheid daarvan is hoog.

6.5.3. Beoordeling ongewenste effecten

De inzet van ICT voor de bedrijfsvoering tast niet direct belangen aan. Strikt genomen maakt het niet uit of men in de bedrijfsvoering gebruikmaakt van de ganzenveer, een typemachine, een schoenendoos of de postduif. Dit laat onverlet dat de illegale bedrijfsvoering op zich wel kan resulteren in ongewenste effecten, maar die specificatie is niet het doel van deze beoordeling. Wel zou de inzet van ICT gepaard kunnen gaan met misbruik van de ICT-sector en -deskundigen. Dit kan leiden tot dezelfde ongewenste effecten als van die dreiging zelf.[37]

---

[33] Paoli beschrijft eveneens dat de beperkingen van de illegaliteit benutting van de nieuwe ICT-mogelijkheden in de weg staan. Overigens hanteert zij een heel ander vertrekpunt en is haar argumentatie summier {Paoli, 2002, 69-70}.
[34] Zie voor dat laatste paragraaf 6.3.
[35] {DNRI, 2004, 45, 120-121}.
[36] Zie de paragrafen 5.6 en 5.7.
[37] Zie subparagraaf 6.10.3.

6.6. Illegale informatie als groothandelswaar

6.6.1. Omschrijving

Informatie omvat tekstuele informatie zoals kranten, audio, foto's en video. Informatie kan zijn vastgelegd op uiteenlopende media, zoals papier, cd-rom, dvd, USB-key, diskette of videoband. Het gaat dan om papieren, magnetische of digitale gegevensdragers. Informatie als consumptiegoed is een legaal product waarvoor een legale markt bestaat. Voorbeelden zijn kranten en muziek-cd's. Legale organisaties gebruiken daarnaast informatie als productiefactor. Veelal heeft die informatie een strategische betekenis voor de organisatie en leidt die informatie in andermans handen tot schade. Voorbeelden zijn researchgegevens, verslagen van fusiebesprekingen en financiële gegevens. De informatie kan daarentegen ook juist bewust aan andere organisaties worden verkocht. Dit is bijvoorbeeld het geval met telefoon- en adresgegevens van KPN en TPG. Mengvormen bestaan ook. Een analyserapport van een bank vormt aan de ene kant een productiefactor om investeringen op te baseren. Aan de andere kant kan een bank dit rapport ter beschikking stellen aan klanten ter ondersteuning van hun beleggingsbeslissingen (consumptiegoed).

Type handelswaar	Onderverdeling	Voorbeelden
Gestolen informatie	Gestolen informatie (consumptiegoed) Gestolen informatie (productiefactor met waarde voor enkelen)	Gestolen (fysieke vormen van) audio en video Researchgegevens Klantenbestanden
Gestolen en/of gemanipuleerde informatie	Gestolen en gemanipuleerde informatie Illegaal gegenereerde informatie	Creditcard- en identiteitsinformatie Creditcardinformatie
Illegaal gekopieerde informatie	Illegaal gekopieerde audio Illegaal gekopieerde video	Illegaal gekopieerde cd Illegaal gekopieerde film
Vervalste fysieke vormen van audio en video		Illegaal gekopieerde cd of film
Kinderporno-afbeeldingen		Foto's en video

Figuur 6.2 Typologie informatie als illegale handelswaar

Informatie kan illegale handelswaar vormen. Een *eerste* vorm betreft gestolen informatie. Informatie is immers op ruime schaal voorhanden. Er bestaan bovendien vele mogelijkheden om daar op illegale wijze aan te komen. Bij diefstal van informatie die fungeert als productiefactor spreekt men over industriële, economische of bedrijfsspionage.[38] Een *tweede* vorm van handelswaar is de combinatie van gestolen en gemanipuleerde informatie. Er bestaan vele mogelijkheden daartoe. Het illegaal genereren van creditcard- en identiteitsinformatie zijn daarvan voorbeelden.[39] Een *derde* vorm betreft de handel in illegale kopieën. Voorbeelden zijn illegale kopieën van audio en video.[40] Een *vierde* vorm

[38] Deze vormen van criminaliteit zijn genoemd in/door: {Power, 2000B}, interview Aalbersberg en ICT-bedrijf (bijlage 4). Het gaat hier niet om de spionage zelf, maar om de handel in de gestolen informatie.

[39] Deze vormen van criminaliteit zijn genoemd in/ door: {NCIS, 1999}, {Stol e.a., 1999A}, {Vriesde e.a., 1999}, {Power, 2000B}, {Boni & Kovacich, 1999}, {Williams, 1999}, {O'Brien, 2000}, {Robinson, 2000}, {Van Duyne e.a., 2001, 36}, interview Vriesde, Aalbersberg en ICT-bedrijf (bijlage 4). Het gaat hier niet om de manipulatie zelf, maar om de handel in de betreffende informatie.

[40] Het illegaal kopiëren en de handel daarin (piraterij) zijn genoemd in: {NCIS, 1999}, {Vriesde e.a., 1999} en {Power,

zijn fysieke vervalsingen van vormen van audio en video, inclusief het verpakkingsmateriaal en de labels. Een *vijfde* en tevens veelgenoemd voorbeeld van een illegaal product waarbij sprake is van manipulatie en/of kopiëren, zijn kinderporno-afbeeldingen. Figuur 6.2 specificeert de uiteenlopende vormen van handelswaar en schetst voorbeelden daarvan.

6.6.2. Beoordeling waarschijnlijkheid

De mate waarin informatie geschikt is voor de illegale groothandel, is afhankelijk van het type informatie. Voor illegale informatie die het karakter heeft van een consumptiegoed moeten we een onderscheid maken tussen maatwerk en massagoederen. In het geval van maatwerk, zoals bij privé-foto's en een video van de eigen vakantie, bestaat er nauwelijks een afzetmarkt. Deze goederen lenen zich daarom niet voor de illegale groothandel. In het geval van massagoederen, zoals cd's en dvd's van een populaire artiest, ligt dat anders. Daarvoor bestaat wel een omvangrijke markt.

Vervalste fysieke evenals illegaal gekopieerde audio en video vormen potentiële illegale groothandelswaar. Het maken van illegale kopieën is eenvoudig uitvoerbaar. Vrijwel elke nieuwe pc beschikt tegenwoordig over een cd- of dvd-brander. In bibliotheken en videotheken kun je audio of video lenen en vervolgens kopiëren. Er bestaan honderden, zo niet duizenden websites van waaruit het mogelijk is om muziek- en filmbestanden te downloaden. Distributie kan in digitale vorm plaatsvinden via zowel dvd als via het internet. De handel in illegaal gekopieerde audio en video vereist dus geen hoogstandjes of forse investeringen. De morele drempel om audio te kopiëren en te verkopen ligt laag. Het aantal illegale kopieerders en dus leveranciers is potentieel zeer groot. Op het schoolplein en in de virtuele ruimte spreekt men ongegeneerd over illegale kopieën. Velen kunnen en willen het uitvoeren en de resultaten verkopen al dan niet tegen kostprijs. Voor eindconsumenten ligt de morele drempel voor de aanschaf ervan eveneens laag.[41] Kopers kunnen rechtstreeks zakendoen met de producenten en vice versa. Illegaal gekopieerde audio en video zijn dus geen geschikte handelswaar voor de illegale groothandel. De extra schakels van de groot- en detailhandel hebben geen toegevoegde waarde en er is geen bestaansrecht voor handelaren in het groot als gevolg van de grote hoeveelheid kleine handelaren. Hoewel strikt genomen gestolen of vervalste fysieke en illegaal gekopieerde audio en video tot dezelfde misdaadmarkt behoren, bestaat toch een verschil. Er zijn immers minder partijen die kunnen beschikken over gestolen fysieke audio en video of in staat zijn om de verpakking (et cetera) daarvan te vervalsen. Evenmin kunnen eindconsumenten en producenten eenvoudig met elkaar in contact komen. Het ligt immers niet voor de hand om op bijvoorbeeld een verjaardagspartij of het schoolplein (gestolen) originele audio en video aan te bieden. De drempel ligt daarvoor hoger dan voor illegaal gekopieerde audio en video. Daardoor is er een rol weg gelegd voor de illegale groothandel en is die handelswaar wel degelijk geschikt. Zoals eerder is opgemerkt, beschouwt het Nationaal Dreigingsbeeld piraterij van audio en video als waarschijnlijk, benoemt dit als dreiging en ziet een rol weg gelegd voor georganiseerde criminaliteit.[42] Vanwege de eerder gemaakte kanttekening en op grond van bovenstaande argumenten, is hier het uitgangspunt dat illegale digitale

---

2000B}.

[41] Zie voor de acceptatie van het illegaal downloaden en kopiëren, het grote aanbod en de grote vraag in de virtuele ruimte het onderzoek van {Svensson & Van Wijk, 2004, 29-40, 45-55}.

[42] Zie paragraaf 6.4.2.

kopieën geen geschikte groothandelswaar vormen en gestolen of vervalste fysieke vormen van audio en video wel.

Andere potentiële handelswaar vormt 'spionage-informatie'. Er is een misdaadmarkt voor dergelijke informatie. De internationale competitie is sterk toegenomen. Zowel overheden als het bedrijfsleven kunnen strategische voordelen behalen met behulp van informatie van anderen. Het gaat daarbij om grote belangen. In toenemende mate is gevoelige informatie opgeslagen in computersystemen. Daardoor verschuift spionage van fysieke naar digitale diefstal. Het is overigens lang niet altijd noodzakelijk om zelf toegang te hebben tot de digitale informatie. Volgens Power verkopen of geven vooral insiders informatie aan de concurrenten. De verschillende overheden, waaronder die van de Verenigde Staten, Frankrijk, Duitsland en China, houden zich actief bezig met economische spionage.[43]

Is spionage-informatie geschikt voor de illegale groothandel? Iemand die op zoek is naar informatie heeft een unieke behoefte. Het gaat daarbij om maatwerk. Dit vereist de nodige specifieke inspanningen van de partij die die informatie wil leveren. Uiteenlopende partijen kunnen voorzien in die informatie. Er bestaat immers een groot schemergebied tussen legaal en illegaal. In dit schemergebied opereren overheden, medewerkers van bedrijven en informatiemakelaars. Ook het aanbod van informatie is maatwerk. De informatie heeft immers slechts waarde voor enkelen. De informatie moet dus specifiek zijn toegesneden op de afnemer. Dezelfde informatie kan daardoor niet aan vele afnemers worden geleverd. Er is dus geen sprake van grootschalige vraag naar dezelfde informatie en grootschalig aanbod daarvan. Er zijn ook geen afnemers of leveranciers die in grote partijen van dezelfde informatie handelen. Verder is er geen toegevoegde waarde om schakels in te bouwen tussen de dief van de informatie en de afnemer ervan. Spionage-informatie is daarom geen geschikte handelswaar voor de illegale groothandel.

Ook identiteits- en creditcardinformatie vormen potentiële handelswaar. Identiteits-informatie wordt in de Verenigde Staten op grote schaal misbruikt, zeker het 'Social Security Number'.[44] Het achterhalen en misbruiken van andermans identiteit via het internet is een snel toenemende vorm van misdaad[45], maar lijkt zich nog niet te hebben voorgedaan in Nederland. Toch beschouwt het Nationaal Dreigingsbeeld identiteitsdiefstal als een potentiële dreiging.[46] Geldt dat ook voor de handel er in? Degene die een ander de identiteitsinformatie ontfutselt, kan er natuurlijk zelf allerlei vormen van criminaliteit mee plegen. Voorbeelden daarvan zijn het aanvragen van bankrekeningen en uitkeringen. Stel dat iemand dat niet wil, kan of te riskant vindt. Hij kan die informatie aan anderen verkopen. In die zin is er een misdaadmarkt. Er is echter geen aanleiding om minimaal twee schakels in te bouwen tussen de producent (de dief) en de eindconsument die het misbruik daadwerkelijk pleegt. De koper kan immers pas de waarde van de informatie bepalen op het moment dat hij het misbruikt. Bovendien kan dezelfde informatie ook al

[43] Gebaseerd op interviews met Aalbersberg en een ICT-bedrijf (bijlage 4) alsmede {Power, 2000B, 5, 166-178, 260} en {Boni & Kovacich, 1999, 84, 85, 102}.
[44] {Power, 2000B, 215-221}.
[45] Alleen al in 2000 zijn de persoonsgegevens van ruim 700.000 Amerikanen misbruikt. Het gemak waarmee in de VS persoonlijke gegevens te koop zijn en verhandeld worden, is hiervan een oorzaak evenals de rol die Social Security-nummers spelen in de Verenigde Staten. Schattingen geven aan dat bij meer dan de helft van alle identiteitsvervalsingen het internet een rol speelt. Nederland kent geen Social Security-nummers en de nummers die we wel hebben, zijn minder gemakkelijk te verkrijgen dan in de VS. De constatering is ontleend aan Netkwesties van 27 april 2001 (www.netkwesties.nl/editie13/artikel3.html) {Cops@Cyberspace, 2001}.
[46] {DNRI, 2004, 76-78}.

aan anderen zijn verkocht. Er is evenmin een reden om in grote partijen identiteits-informatie te handelen. Waarom er zelf niet van profiteren? De aanname is daarom dat identiteitsinformatie geen geschikte handelswaar vormt voor de illegale groothandel. Ook creditcardinformatie wordt vooral in de Verenigde Staten op grote schaal ontvreemd en ook in Nederland zijn gevallen bekend. Het Nationaal Dreigingsbeeld classificeert creditcardfraude via het internet als dreiging.[47] Sommigen kunnen creditcardinformatie zelf genereren zonder enige vorm van ontvreemding. Toch is ook de redenering over identiteitsinformatie op deze handelswaar van toepassing. Gestolen en/of gegeneerde creditcardinformatie vormt dus geen illegale groothandelswaar.[48]

Eerder is al aangegeven dat kinderporno niet geschikt is voor de illegale groothandel.[49] Desondanks vermeldt het Nationaal Dreigingsbeeld: "Kinderpornografisch materiaal op het internet zou voor twintig procent te maken hebben met georganiseerde criminaliteit. Het materiaal is veelal afkomstig uit landen met gebrekkige ICT- en zedenwetgeving: Rusland, sommige landen in Oost-Europa en Zuid-Amerika".[50] Hoewel de aanname blijft dat kinderpornomateriaal niet geschikt is als groothandelswaar, is dit wel een element dat nader onderzoek behoeft. Welke aanname klopt niet? Heeft men bijvoorbeeld manieren gevonden om de betalingen te innen zonder risico's te lopen? Of komen nu juist zij die dachten dat deze handelswaar wel degelijk geschikt is, in het zicht van de politie?

Met uitzondering van 'gestolen en vervalste fysieke audio en video', vormen de genoemde soorten illegale informatie dus geen geschikte handelswaar voor de illegale groothandel. Op grond daarvan is het niet aannemelijk dat illegale groothandelsondernemingen de functies van de groothandel voor hun rekening willen nemen. Dit zou overigens geen onoverkomelijke eisen stellen aan de bedrijfsvoering. De reguliere bedrijfsvoering en de daarvoor gebruikelijke ondersteuners zouden kunnen volstaan.

Sociale controle is tot op zekere hoogte mogelijk. Voor spionage-, identiteits- en creditcardinformatie kunnen de eigenaren voldoende beveiligingsmaatregelen treffen. Voorbeelden zijn de installatie van een virusscanner, firewall, installatie van reparaties voor software (patches), organisatorische maatregelen, voorzichtigheid betrachten et cetera. Overigens heeft nog steeds niet iedereen die maatregelen ook daadwerkelijk getroffen. Bovendien is veel van deze informatie tegenwoordig digitaal opgeslagen. Grote hoeveelheden daarvan kunnen met heel kleine hulpmiddelen, bijvoorbeeld een USB-key, worden meegenomen of, zonder dat sprake is van fysieke toegang, worden gehackt. Misbruik van creditcardgegevens valt in elk geval op bij de houder en in sommige gevallen ook bij de banken. Banken nemen ook allerlei veiligheidsmaatregelen en zij drukken gebruikers op het hart om zorgvuldig om te gaan met de creditcard(gegevens). Misbruik van identiteitsinformatie zal ook snel blijken. De betaling met de creditcard en het gebruik van identiteitsinformatie laten verder bewijssporen na. Deze kunnen met enig speurwerk leiden naar de illegale groothandelsonderneming. Wanneer informatie is ontvreemd bij bedrijven, overheden en dergelijke (spionage-informatie) hoeft dat niet boven water te

[47] {DNRI, 2004, 76-78}.
[48] De factoren zoals die zijn verwoord in paragraaf 4.2 zijn in onvoldoende mate aanwezig. Van Duyne e.a. gaan eveneens in op deze handelswaar. Hoewel hun redenering niet eenduidig is, lijken ook zij te concluderen dat er sprake is van een platte marktstructuur met vele participanten {Van Duyne e.a., 2001, 36-37}.
[49] Zie paragraaf 4.2.
[50] {DNRI, 2004, 117}. Dit punt is ontleend aan: NCIS (National Criminal Intelligence Service), *UK Threat assessment. The threat from serious and organised crime 2003*, UK, 2003.

komen, terwijl wel schade kan ontstaan. Voor diefstal of vervalsing van fysieke audio en video geldt dat, net als bij andere gestolen en vervalste goederen, sociale controle mogelijk is. Illegaal gekopieerde audio en video die worden aangeboden in de virtuele ruimte, is op zich eenvoudig te constateren. Het sanctioneren daarvan is echter minder eenvoudig. Aanbod en aanschaf via het schoolplein en dergelijke verlopen minder zichtbaar en de controle daarop is lastiger. Extra handicap is tevens dat het sociaal geaccepteerd lijkt te zijn om audio en video te kopiëren. Desondanks slagen de door de branches opgerichte organisaties zoals BREIN en de specifieke opsporingsinstanties zoals Buma/Stemra er wel degelijk in om kopieerders aan te pakken.[51] Sociale controle op kinderporno is zeker mogelijk. Er zijn nationaal en internationaal meldpunten, de sociale acceptatie ligt laag waardoor mensen aanbod melden[52] en opsporingsinstanties werken internationaal veelvuldig samen om het aanbod te bestrijden.

De algemene beoordeling voor deze dreiging is dat de waarschijnlijkheid laag is vanwege vooral de ongeschiktheid van illegale informatie als groothandelswaar. Een uitzondering daarop is gestolen en vervalste audio en video in fysieke vorm (met dozen et cetera). De waarschijnlijkheid daarvan is als hoog gekwalificeerd.

6.6.3. Beoordeling ongewenste effecten

Informatie is een legaal product en gaat op zich niet gepaard met ongewenste effecten, met uitzondering van kinderporno-afbeeldingen. De wetgever acht die effecten zodanig schadelijk, dat het bezit strafbaar is gesteld. De groothandel in en het gebruik/misbruik van illegale informatie heeft ongewenste effecten. Dat vormt een stimulans voor anderen in misdaadmarkten. De illegale groothandel fungeert aan de ene kant als afzetkanaal voor dieven, hackers, illegale kopieerders, helers en dergelijke. Dit leidt tot een aantasting van de veiligheid en een afname van de leefbaarheid in vooral de virtuele ruimte voor de spionage-informatie, identiteits- en creditcardinformatie. In het geval van diefstal van audio en video resulteert dat ook in financieel verlies bij de slachtoffers. Aan de andere kant fungeert zij als leverancier voor de criminele detailhandel en daarmee voor de gebruikers. Dat leidt tot een financieel verlies voor banken bij misbruik van creditcard- of identiteitsinformatie, bij de bedrijven wier informatie is gestolen of voor de brancheorganisaties bij illegale kopieën van audio en video. Toch is het in het laatste geval nog niet eens zeker dat zij verlies lijden. Wellicht had anders de koper de audio of video toch niet aangeschaft.[53] Het kan ook leiden tot verstoring van de markwerking wanneer bijvoorbeeld spionage-informatie wordt misbruikt. De handel in illegale informatie kan tevens tot schade aan de buitenlandse betrekkingen leiden wanneer Nederlandse misdaadondernemingen zich hiermee bezighouden. Illegale informatie als handelswaar stelt in beginsel geen bijzondere eisen aan de onderneming of aan de bedrijfsvoering ten opzichte van de groothandel in andere soortgelijke goederen. Daar komen dus geen bijzondere ongewenste effecten uit voort. Immers het ontvreemden van de informatie en het kopiëren verricht de groothandel niet zelf. De handel in kinderporno kan resulteren in seksueel misbruik van kinderen door degenen die die afbeeldingen maken. Wel is het als gevolg van de ICT-ontwikkelingen mogelijk om oneindig te variëren in afbeeldingen zonder dat verder

[51] Zie paragraaf 5.6 en {Svensson & Van Wijk, 2004, 64-78}.
[52] Zie hiervoor {Svensson & Van Wijk, 2004, 34, 40, 60}.
[53] Dit is geen normatief oordeel van de auteur.

misbruik van kinderen plaatsvindt. Toch maakt de wetgever geen onderscheid hiernaar, voorzover dit überhaupt te onderscheiden zou zijn.

Hoewel niet noodzakelijk, kan de handel in informatie resulteren in misbruik van de ICT-sector en -deskundigen en de omzetting van een gewone naar een virtuele bedrijfsvoering. De ongewenste effecten daarvan zijn gelijk aan die van de corresponderende dreigingen.[54] Het gaat hier om mogelijke bijkomende ongewenste effecten van deze dreiging.

6.7. Vergroting inzet informatie in illegale bedrijfsvoering

6.7.1. Omschrijving

Als gevolg van de ICT-ontwikkelingen is meer informatie beschikbaar dan vroeger. Tevens zijn de instrumenten om daar op (illegale) wijze aan te komen aanzienlijk toegenomen. In de illegale bedrijfsvoering speelt informatie eveneens een rol. De secundaire criminaliteit is bijvoorbeeld deels gericht op het verkrijgen van identiteits-documenten en officiële documenten, zoals vrachtbrieven. Ook voor afscherming is informatie belangrijk. Verder heeft de misdaadonderneming achtergrondinformatie nodig over bijvoorbeeld de asielprocedures in landen. Deze kan zij verkrijgen via het internet. Net als een legale onderneming kan ook een illegale groothandelsonderneming de inzet van informatie in de bedrijfsvoering vergroten. Specifieke vormen daarvan zijn: een groter gebruik van opsporingsinformatie in de bedrijfsvoering (offensieve afscherming), de inzet van bij anderen ontvreemde informatie of het gebruik van de virtuele ruimte als informatiebron.

6.7.2. Beoordeling waarschijnlijkheid

Eerder is geschetst dat er onvoldoende prikkels zijn om over te gaan tot veranderingen in de bedrijfsvoering. Tevens is aangegeven dat aan de randvoorwaarden voor innovatie niet is voldaan. Bovendien past een grotere inzet van informatie niet bij het profiel van de illegale groothandelaar en de vigerende bedrijfsvoering. Ook toezichthoudende en opsporingsinstanties geven daartoe geen aanleiding. Sterker nog, een toename van informatie vormt een risico voor de geheimhouding en kan bewijssporen opleveren.[55]

Opsporingsinformatie is aantrekkelijk voor een illegale groothandelsonderneming. De groothandelaar kan onder andere op grond van die informatie de afscherming verbeteren. De toenemende digitalisering bij opsporingsinstanties biedt in potentie de gelegenheid om aan opsporingsinformatie te komen. In Amsterdam heeft een criminele groep halverwege de jaren negentig met behulp van technische deskundigen het telefoonverkeer van de Amsterdamse politie afgeluisterd. Power beschrijft een casus waarin criminelen de gegevens van de politie gedurende enige tijd hebben ingezien.[56] Informatie van toezichthouders zoals de douane, beveiligingsbedrijven (et cetera) is eveneens aantrekkelijk. Het kan bijdragen aan afscherming en beperking van de risico's. Om aan de informatie te komen, kan de illegale groothandelsonderneming medewerkers ronselen, handlangers

[54] Zie subparagraaf 6.9.3 en 6.10.3,
[55] Zie paragraaf 6.3.
[56] {Klerks, 2000, 167}, {Enquêtecommissie, 1996A}, {Power, 2000B, 102}.

plaatsen of zelf overgaan tot hacken. Vanwege de specialistische kennis die is vereist, ligt het hacken niet voor de hand.[57] Uit het interview met een ICT-bedrijf blijkt dat criminelen contact zoeken met ICT-bedrijven om aan informatie te komen. Bovendien kan een illegale groothandelsonderneming de virtuele ruimte gebruiken als informatiebron. Ook dat kan voordelen opleveren.

Sociale controle is tot op zekere hoogte mogelijk. Wanneer de illegale groothandelsonderneming de bedrijfsvoering zou innoveren, bestaan er mogelijkheden om de informatie af te schermen met behulp van bijvoorbeeld encryptie. Dat maakt de opsporing lastiger. Aan de andere kant hebben opsporingsinstanties wel degelijk de gelegenheid om afgeschermde informatie boven water te krijgen en dat levert juist bewijssporen op.[58] Ontvreemding van informatie laat eveneens sporen na en aannemelijk is dat opsporingsinstanties ontvreemding van eigen informatie hoog opnemen en daar een onderzoek naar zullen instellen. Datzelfde geldt voor de overige genoemde instanties. Informatie opvragen in de virtuele ruimte laat sporen na en kan achteraf dienen als bewijsmateriaal. Het opvragen van specifieke informatie kan bovendien argwaan opleveren bij de aanbieder ervan en interesse opleveren om de vragensteller te achterhalen.

Alles overziend is de vergroting van de inzet van informatie in de illegale bedrijfsvoering niet waarschijnlijk doordat de voordelen niet substantieel opwegen tegen de nadelen, er geen aanleiding is en de randvoorwaarden niet optimaal zijn. Dit met uitzondering van het gebruik van de virtuele ruimte als informatiebron.

6.7.3. Beoordeling ongewenste effecten

Een vergroting van de inzet van informatie in de bedrijfsvoering tast niet direct belangen aan. Wel zou de inzet ervan gepaard kunnen gaan met ontvreemding van informatie bij opsporingsinstanties of anderen. Dit kan leiden tot een afname van het vertrouwen in de instanties.

Een vergroting van de inzet van informatie kan leiden tot de inzet van ICT in de bedrijfsvoering en tot misbruik van de ICT-sector en -deskundigen. De ongewenste effecten daarvan vormen ook de ongewenste effecten van deze dreiging. Deze effecten zijn elders in dit hoofdstuk gespecificeerd bij de corresponderende dreigingen.

6.8. Virtuele illegale groothandelsondernemingen

6.8.1. Omschrijving

Net als legale ondernemingen kunnen misdaadondernemingen de virtuele ruimte gebruiken om producten te kopen, te verkopen en/of te distribueren. Er is sprake van een virtuele illegale groothandelsonderneming wanneer deze de koop, verkoop, en/of de distributie in de virtuele ruimte heeft vormgegeven. Wanneer een virtuele organisatie uitsluitend dient als dekmantel, facilitering, investeringsbron of witwasgelegenheid, dan valt die organisatie onder de illegale bedrijfsvoering (zie hiervoor paragraaf 6.9).

[57] Dat laatste veronderstelt men ook in het Nationaal Dreigingsbeeld {DNRI, 2004, 45, 114-116}.
[58] Zie paragraaf 5.6 en 5.7.

Buitenlandse virtuele illegale groothandelsondernemingen zouden zich op Nederland kunnen richten om handel te drijven. De plaats waar iemand verblijft, maakt immers in de virtuele ruimte niet uit. Omgekeerd kunnen juist Nederlandse illegale groothandelsondernemingen een virtuele gedaante aannemen en hun activiteiten verplaatsen of uitbreiden naar het buitenland.

6.8.2. Beoordeling waarschijnlijkheid

Eerder is verwoord dat de virtuele ruimte niet aantrekkelijk is als marktplaats voor het afsluiten van illegale transacties. Vertrouwen in de leveranciers en afnemers is bij handel in de virtuele ruimte randvoorwaardelijk. Daar past het niet bij om met vele en onbekende partijen zaken te doen, terwijl dat nu juist één van de voordelen is van de handel in de virtuele ruimte. Het verstrekken van informatie over de producten ligt evenmin voor de hand en daarmee verdwijnt nog een voordeel van de virtuele ruimte. Verder zijn de illegale producten overwegend fysiek, waardoor ze niet kunnen worden gedistribueerd in de virtuele ruimte. Uitzonderingen daarop vormen kinderporno-afbeeldingen, illegaal gokken, illegale digitale informatie en illegaal gekopieerde software. Deze producten zijn echter alle als ongeschikt gekwalificeerd voor de illegale groothandel.[59] Verder bestaan geen prikkels om juist handel te drijven in de virtuele ruimte en ontbreken de randvoorwaarden voor de daarvoor vereiste veranderingen en voor productinnovatie.[60] Toch noemt NCIS de handel in medicijnen als voorbeeld waarbij criminelen e-commerce bedrijven.[61] In de Verenigde Staten zijn enkele medicijnen immers legaal en zonder recept verkrijgbaar en niet in Nederland. In potentie zou echter elke apotheek in de Verenigde Staten deze medicijnen kunnen leveren aan iedere Nederlander. Er is daarom geen meerwaarde voor een illegale groothandel. De virtuele ruimte heeft wel enkele kenmerken die sociale controle bemoeilijken. Toch biedt de virtuele ruimte naast beperkingen, ook enkele voorzieningen die sociale controle juist eenvoudiger maken.[62] De virtuele ruimte is al met al niet geschikt als marktplaats voor fysieke illegale producten en geschikte virtuele illegale handelswaar is niet voorhanden. Daarom zullen zowel Nederlandse als buitenlandse illegale groothandelsondernemingen geen handel willen en kunnen drijven in de virtuele ruimte. Het Nationaal Dreigingsbeeld constateert eveneens dat het internet (nog) nauwelijks wordt gebruikt voor het aanbieden van illegale goederen en classificeert ‘het gebruik van het internet als marktplaats’ als geen dreiging.[63]

Op grond van het ontbreken van geschikte handelswaar, de ongeschiktheid van de virtuele ruimte, het ontbreken van een noodzaak en het niet ingevuld zijn van de randvoorwaarden, is de waarschijnlijkheid van virtuele illegale groothandelsondernemingen als laag gekwalificeerd.

[59] Zie paragraaf 4.2, 6.3, subparagraaf 6.4.2 en 6.6.2.
[60] Zie paragraaf 6.3.
[61] {NCIS, 1999}.
[62] Zie paragraaf 5.6 voor de beperkingen van en de mogelijkheden voor sociale controle.
[63] {DNRI, 2004, 44, 116-117}.

6.8.3. Beoordeling ongewenste effecten

In de kern bestaan er geen verschillen tussen de ongewenste effecten van een virtuele of een gewone illegale groothandelsonderneming. Beide soorten ondernemingen drijven handel in soortgelijke illegale producten en moeten daarvoor een bedrijfsvoering opzetten. De aard van de bedrijfsvoering verschilt natuurlijk wel. Bij een virtuele onderneming is die (grotendeels) virtueel en gestoeld op ICT. Tevens kan een virtuele onderneming ondersteuning zoeken van de ICT-sector en -deskundigen. Daaruit komen enkele ongewenste effecten voort. Deze zijn beschreven bij de corresponderende dreigingen.[64]

Indien buitenlandse ondernemingen (een deel van) hun activiteiten virtueel in Nederland gaan uitvoeren, kan dat leiden tot nieuwe of meer illegale producten op de Nederlandse markt. Daardoor zouden deze uiteindelijk voor meer eindconsumenten en tussenhandelaren bereikbaar worden en/of de prijs zou kunnen dalen. Er zou meer concurrentie kunnen komen, waardoor Nederlandse misdaadondernemingen minder winst kunnen maken of meer geweld ontstaat. Volstaan wordt hier met de voorzichtige aanname dat virtuele groothandelsondernemingen zouden kunnen resulteren in een grotere beschikbaarheid van illegale producten voor zowel de levering aan als de afname van Nederlandse ondernemingen. Dit kan resulteren in een aantasting van de veiligheid en een afname van de leefbaarheid. Wanneer Nederlandse illegale groothandelsondernemingen meer handel zouden gaan drijven in het buitenland, dan kan dat leiden tot schade aan de buitenlandse betrekkingen.

6.9. Omzetting van gewone naar virtuele illegale bedrijfsvoering

6.9.1. Omschrijving

De virtuele ruimte speelt een cruciale rol in de samenleving. Informatieverwerking en communicatie zijn daarin nauwelijks aan tijd, plaats en omvang gebonden. De virtuele ruimte en de fysieke wereld integreren steeds verder. Net als legale ondernemingen kunnen illegale groothandelsondernemingen de virtuele ruimte gebruiken voor de bedrijfsvoering, bijvoorbeeld om te communiceren. Eerder is een groothandelsonderneming die de koop, verkoop en/of de distributie in de virtuele ruimte heeft georganiseerd, benoemd als virtuele illegale groothandelsonderneming. Het gebruik van de virtuele ruimte voor deze activiteiten is al apart beschouwd en gedefinieerd en valt daarom in dit kader buiten de illegale bedrijfsvoering. Het gaat dus om de omzetting ten behoeve van de overige primaire, de secundaire en de ondersteunende (criminele) activiteiten van een illegale groothandelsonderneming.

In paragraaf 6.3 is aangenomen dat illegale groothandelsondernemingen de ICT-ontwikkelingen geleidelijk en kleinschalig gaan gebruiken voor communicatie, administratie en afscherming. In paragraaf 6.7 is, vanuit de invalshoek van de rol van informatie in de bedrijfsvoering, al gekeken naar dat gebruik. In elk geval is daar genoemd dat de virtuele ruimte kan worden gebruikt als informatiebron. Zeker de virtuele ruimte kan zich lenen voor communicatie en administratie vanwege de karakteristieken ervan en de kenmerken die sociale controle bemoeilijken.[65] Dat kan tevens bijdragen aan een betere

[64] Zie subparagraaf 6.5.3, 6.9.3 en 6.10.3.
[65] Zie paragraaf 5.6.

afscherming evenals het gebruik van virtuele organisaties. Ook voor andere doeleinden zouden virtuele organisaties aantrekkelijk kunnen zijn, namelijk voor legitimering (dekmantel), facilitering, witwassen of als investering. Wanneer die virtuele organisaties ICT-diensten of -producten aanbieden, dan worden deze gerekend tot de ICT-sector (zie de volgende paragraaf).

6.9.2. Beoordeling waarschijnlijkheid

Eerder is al geschetst dat er onvoldoende prikkels zijn om over te gaan tot veranderingen in de bedrijfsvoering en tot de vorming van een virtuele onderneming. Er zijn wel voordelen te behalen door te communiceren in de virtuele ruimte. Toch is aangegeven dat daar ook risico's aan kleven en dat aan de randvoorwaarden voor innovatie niet is voldaan.[66] Van volledige omzetting van de communicatie zal daarom geen sprake zijn. Voor administratieve doeleinden gelden nog meer risico's. Daarvoor is het nog belangrijker om te weten met wie je zakendoet en moet je er op kunnen vertrouwen dat de administratie niet in verkeerde handen valt. Vanwege de beperkingen van de virtuele ruimte[67], is aan die voorwaarden niet voldaan.

De illegale groothandelsondernemingen zouden ook virtuele organisaties kunnen misbruiken voor de illegale bedrijfsvoering. Als dekmantel zijn ze niet nodig, omdat het niet aannemelijk is dat illegale groothandelsondernemingen handelen in de virtuele ruimte. Zij kunnen wel faciliteren bij de administratie, het verkrijgen van goederen of het opzetten van juridische constructies. Via het internet kan in de Verenigde Staten bijvoorbeeld binnen acht minuten een Delaware corporation worden opgericht. Deze rechtsvorm is wereldwijd te gebruiken. Ook is het zeer eenvoudig om binnen korte tijd een trustmaatschappij op te richten met behulp van het internet. Tevens is het kopen van een paspoort relatief eenvoudig.[68] Naast de aantrekkelijke kanten bestaan er echter eveneens de eerdergenoemde risico's.[69]

Verder kunnen virtuele organisaties dienen voor witwassen. Door goederenstromen of dienstverlening te fingeren tussen virtuele organisaties kan de illegale groothandelsonderneming een legale omzet voorwenden voor de illegale inkomsten. Op basis van de eerdere redeneringen over de bruikbaarheid van de virtuele ruimte voor criminele activiteiten is het overigens nog maar de vraag of witwassen in de virtuele ruimte wel reëel is. Ook witwassen in de virtuele ruimte laat bijvoorbeeld sporen na. Ook volgens het Nationaal Dreigingsbeeld is onduidelijk of dit voorkomt.[70] Hoewel nader onderzoek hierover uitsluitsel moet geven, is hier de aanname dat witwassen via virtuele organisaties niet aantrekkelijk is. De redenen daarvoor zijn de beperkingen van de virtuele ruimte voor misdaadmarkten.[71]

Tot slot kunnen virtuele organisaties dienen als investering. De oprichting van een virtuele organisatie is namelijk veel eenvoudiger dan van een gewoon bedrijf en er worden geen hoge eisen gesteld. Bovendien valt het niet op wanneer iemand een bedrijf start via het

[66] Zie paragraaf 6.3 en 5.6.
[67] Zie paragraaf 5.7 en 6.8.2.
[68] De voorbeelden zijn ontleend aan {Kerstens, 1995}, {Robinson, 2000, 244}, {Westerman, 1999}.
[69] Zie paragraaf 6.3 en 6.8.2.
[70] Bevinding vanuit {DNRI, 2004, 46, 104-106}.
[71] Zie paragraaf 6.3 en 6.8.2.

internet. Een virtuele organisatie kan ook eenvoudig verdwijnen. Afstanden spelen bovendien geen rol. Vanuit een Amsterdamse zolderkamer kan iemand een bloeiend virtueel bedrijf op de Antillen exploiteren. Via het internet kan het bedrijf ook nog eens een (dubieuze) juridische status verkrijgen. Een ander aantrekkelijk element is dat sociale controle op virtuele organisaties lastiger is dan voor gewone bedrijven. Dit in verband met het internationale karakter, de beperkte oprichtingseisen en dergelijke. Aan de andere kant zal de organisatie toch ook ergens moeten zijn geregistreerd bij providers en is de kans aanwezig dat deze wordt opgemerkt door zoekmachines. Een minpunt is verder dat een virtuele organisatie niet echt tot de verbeelding spreekt. Het eigendom van bijvoorbeeld een horecagelegenheid past beter bij de levensstijl en het profiel van een illegale groothandelaar dan een virtuele organisatie. De reden om te investeren is ook niet gelegen in de noodzaak om te beschikken over een dekmantel in de virtuele ruimte of voor het witwassen.[72] Een bijzonder soort virtuele organisatie is een cyberbank. Een cyberbank biedt interessante voorzieningen voor witwassen. De drempels om bankdiensten aan te bieden zijn gewoonlijk hoog. Voor off-shore-banken liggen de drempels weliswaar minder hoog, maar dan vormt de afstand een beperking. De toetredingsdrempels op het internet liggen lager en de beperkingen van afstand gelden niet. Het eigendom van cyberbanken kan daarom interessant zijn,[73] maar vergt wel specifieke financiële kennis. Het is maar de vraag of de illegale groothandelsondernemingen in hun netwerken in voldoende mate kunnen beschikken over deze kennis en of men een cyberbank wel zelfstandig kan exploiteren. Ook de exploitatie vergt immers veel kennis van zaken en dat staat ver af van de gemiddelde belevingswereld van de illegale groothandelaren. Voor facilitaire doeleinden is evenmin een virtuele organisatie nodig. Als men al gebruik wil maken van de faciliteiten die verkrijgbaar zijn in de virtuele ruimte, dan kan dat ook zonder over een virtuele organisatie te beschikken. Het eigendom van virtuele organisaties heeft dus enkele aantrekkelijke kanten, maar ook duidelijke minpunten.

Het algemene beeld op basis van deze redenering is dat het niet waarschijnlijk is dat illegale groothandelsondernemingen de illegale bedrijfsvoering gaan omzetten naar een virtuele bedrijfsvoering. Belangrijke redenen zijn dat de voordelen niet opwegen tegen de nadelen, er geen aanleiding is en de randvoorwaarden niet optimaal zijn. Wel is het waarschijnlijk dat zij de communicatie (deels) in de virtuele ruimte vormgeven.

6.9.3. Beoordeling ongewenste effecten

In de kern verschilt een virtuele bedrijfsvoering niet van een gewone bedrijfsvoering. Of men nu via de telefoon communiceert, of via het gewone criminele circuit aan een paspoort komt of via het internet, maakt niet uit. Evenmin maakt het uit of men de administratie bijhoudt in een schoenendoos op een Nederlandse zolder of op een computer die zich fysiek op Curaçao bevindt. Hooguit zou men kunnen zeggen dat er wel verschil bestaat voor het witwassen met en het investeren in een virtuele organisatie. Het witwassen via een horecagelegenheid of de investering daarin kan de normale concurrentieverhoudingen verstoren en het bonafide ondernemers moeilijker maken. Voor witwassen en investeren in virtuele organisaties geldt dat niet, omdat dergelijke illegale organisaties feitelijk niet aan de legale economie hoeven deel te nemen. Wel kunnen we spreken van een aantasting van het vertrouwen in virtuele organisaties wanneer deze op grote schaal worden misbruikt

[72] Zie hiervoor de eerdergenoemde argumenten.
[73] {NCIS, 1999}, {NCIS, 2000B, 11}, {Galeotti, 2000A, 50, 52}, {Williams, 1999, 31}.

voor illegale doeleinden. Dit zou het imago van dergelijke organisaties en de virtuele ruimte niet ten goede komen. Verder resulteert een virtuele bedrijfsvoering in de inzet van ICT en mogelijke misbruik van de ICT-sector en -deskundigen. De ongewenste effecten daarvan vormen tevens ongewenste effecten van deze dreiging.

6.10. Misbruik ICT-sector en -deskundigen voor illegale bedrijfsvoering

6.10.1. Omschrijving

Als gevolg van de ICT-ontwikkelingen is een ICT-sector ontstaan. Ook hebben nieuwe deskundigen hun intrede gedaan zoals website-ontwerpers, beveiligingsdeskundigen en programmeurs. Een illegale groothandelsonderneming zou de sector en deskundigen kunnen gebruiken voor legitimering of facilitering, voor het witwassen of als investering. Vier vormen van betrokkenheid zijn te onderscheiden, al dan niet door tussenkomst van intermediairs: gebruik, afpersing, samenwerking en bezit. De betrokkenheid kan bewust of onbewust zijn en wel of niet profijtelijk.[74] Het voert te ver om in deze paragraaf alle varianten van betrokkenheid uit te werken. Dat past niet bij het verkennende karakter van de risicoanalyse. Een aanvullend onderzoek is dan noodzakelijk. Het accent ligt op onbewuste betrokkenheid van de ICT-sector en -deskundigen, bewuste betrokkenheid en investeringen in de ICT-sector. Daarmee worden als het ware twee uitersten van een continuüm verkend en een tussenvariant. Aan de ene kant van het continuüm bevindt zich dan de onbewuste betrokkenheid, waarvan vooral sprake kan zijn wanneer illegale groothandelsondernemingen de sector en deskundigen misbruiken voor facilitering en witwassen. Daarvan hoeven de betrokkenen zich niet bewust te zijn. Aan de andere kant bevindt zich juist het investeren in ICT-bedrijven, waardoor in beginsel alle functies zouden kunnen worden vervuld.

6.10.2. Beoordeling waarschijnlijkheid

Het misbruik van de ICT-sector en -deskundigen is vooral een afgeleide van de mate waarin illegale groothandelsondernemingen inspelen op de ICT-ontwikkelingen. Doen zij dit niet tot nauwelijks, dan bestaat er ook geen noodzaak om tot misbruik over te gaan. Doen zij dat wel, dan is de noodzaak wel aanwezig. Het investeren in de sector kan daarop een uitzondering zijn. Dat kan een zelfstandig bestaansrecht hebben.

Eerder in dit hoofdstuk is al enkele malen verwoord dat illegale groothandelsondernemingen kleinschalig en geleidelijk inspelen op de ICT-ontwikkelingen. Het merendeel van de (deel)dreigingen is als ‘niet waarschijnlijk’ gekwalificeerd. Uitzonderingen zijn het gebruik van ICT voor communicatie, administratie en afscherming evenals het gebruik van de virtuele ruimte als informatiebron. Daarvoor moeten de illegale groothandelsondernemingen eigenlijk tot op zekere hoogte wel misbruik maken van de ICT-sector en -deskundigen. Daarvoor volstaat veelal (onbewuste, maar profijtelijke) betrokkenheid van hard- en softwareleveranciers, telefoonbedrijven en providers als faciliterende instanties.

[74] Zie de paragrafen 4.3 en 4.4 voor de functies van legale bedrijven voor een misdaadonderneming en de soorten betrokkenheid.

Die onbewuste betrokkenheid is, als afgeleide van de hoge waarschijnlijkheid van de genoemde vormen van ICT-gebruik, aannemelijk. Zo moeten illegale groothandelsondernemingen wel hard- en software betrekken van de ICT-sector, gebruikmaken van de diensten van providers en telecombedrijven en eventueel voor het gebruik ervan een beroep doen op deskundigen. Bewuste betrokkenheid is daar niet voor noodzakelijk. Hard- en software is immers op vele plaatsen verkrijgbaar evenals advies om dat aan de praat te krijgen. Er zijn zo veel abonnees van telecombedrijven en providers, dat het crimineel gebruik van de diensten helemaal niet hoeft op te vallen. Waarom dan iemand corrumperen of er een handlanger plaatsen? Dat levert immers ook risico's op. Als overigens opsporingsinstanties een onderzoek starten, dan kunnen die partijen wel veel gegevens overleggen waardoor het wel een risico vormt voor criminelen.

Wanneer de ICT-sector en -deskundigen *bewust* betrokken zouden zijn, dan past dat niet bij de bestaande werkwijze van illegale groothandelsondernemingen. De affiniteit met ICT is gering en anderen betrekken bij de bedrijfsvoering is riskant. In het Nationaal Dreigingsbeeld veronderstelt men overigens wel dat de druk op de sector zal toenemen vanwege de steeds betere beveiliging van systemen en de ICT die toezichthoudende instanties inzetten. Gesteld wordt dat recente gevallen in ons land niet bekend zijn, hoewel men wel refereert aan een beperkt aantal gevallen die uit opsporingsonderzoeken naar voren zijn gekomen. Mede omdat in het buitenland wel meer gevallen bekend zijn, beschouwt men corruptie van ICT-personeel als potentiële dreiging.[75] Op grond van de beoordeling van de waarschijnlijkheid van de overige dreigingen in dit proefschrift is het overigens voor illegale groothandelsondernemingen nog maar de vraag of de verwachte toename reëel is.

Los van de geïdentificeerde dreigingen zou een illegale groothandelsonderneming kunnen investeren in een ICT-bedrijf. Vóór maart 2000 kon een geringe investering aanzienlijke winsten opleveren door de nieuwe organisatie naar de beurs te brengen. Sinds maart 2000 is daarin een kentering gekomen. Enerzijds kan een illegale groothandelsonderneming daardoor minder snel geld verdienen met een investering. Anderzijds is het voor (goedwillende) ondernemers sindsdien steeds moeilijker geworden om financiers te vinden voor startkapitaal. Een illegale groothandelaar zou deze ondernemers financieel kunnen bijstaan. Geleidelijk kan hij de ondernemer misbruiken. Extra aantrekkelijk kan een investering in een provider zijn. Een provider kan niet alleen legale inkomsten genereren, maar vooral een belangrijke rol spelen in de afscherming. Voor het opsporen van criminaliteit zijn opsporingsinstanties afhankelijk van de (on)vrijwillige medewerking van een provider. Volgens Power start een opsporingsonderzoek naar criminaliteit in de virtuele ruimte veelal op basis van een specifiek internetadres, een datum en een tijdstip.[76] Het kan voor een groothandelsonderneming daarom aantrekkelijk zijn om een provider in eigen bezit te hebben of daar invloed op te hebben. De toetredingsdrempels liggen bovendien vrij laag. Wel is voldoende geld en kennis nodig. Theoretisch gezien kunnen providerdiensten ook dienen voor het witwassen of om aan informatie te komen van bijvoorbeeld opsporingsinstanties. Diverse auteurs wijzen echter op het feit dat een illegale groothandelaar bekend wil zijn met een bepaalde sociale setting of bedrijfstak[77] en dat is niet aannemelijk. Bovendien kost het oprichten van een eigen bedrijf veel doorlooptijd, de

[75] {DNRI, 2004, 45, 100-101}
[76] {Power, 2000B, 257}.
[77] Zie onder andere {Kleemans e.a., 2002}.

opbouw van vertrouwen en investeringsgelden. Doordat er voor illegale groothandelsondernemingen geen aanleiding is om in te spelen op de ICT-ontwikkelingen, is er ook geen directe noodzaak om te investeren in dit type bedrijven. Volgens het Nationaal Dreigingsbeeld zijn er uit opsporingsonderzoeken wel gevallen bekend waarbij er via gefingeerde omzetten geld is witgewassen met behulp van belhuizen en internetcafés.[78] Dit type bedrijf past meer bij de belevingswereld. Bekend is immers dat criminelen investeren in de horeca. Maar om nu te zeggen dat dit specifieke ICT-bedrijven zijn, gaat toch wat te ver.

Sociale controle op misbruik van de ICT-sector en -deskundigen is tot op zekere hoogte uitvoerbaar. De sector en de beroepsgroepen hebben er belang bij om niet betrokken te raken. Hun bestaansrecht is sterk afhankelijk van vertrouwen in de integriteit. Hun werkzaamheden binnen organisaties zijn immers zeer vertrouwelijk van aard. Het Nationaal Dreigingsbeeld constateert dat de kwetsbaarheid van de sector voor betrokkenheid bij georganiseerde criminaliteit nog onvoldoende wordt onderkend.[79] Daar waar andere sectoren en beroepsgroepen reeds een traditie hebben om betrokkenheid bij (georganiseerde) criminaliteit te voorkomen, is dat in deze nieuwe sector en beroepsgroep nog niet te verwachten. Het specifieke karakter van de deskundigheid beperkt tevens de mogelijkheden voor controle op de werkzaamheden. De ICT-sector zal verder lang niet altijd kunnen vermoeden dat de geleverde producten voor illegale doeleinden worden benut. Dit geldt bijvoorbeeld voor telefoonbedrijven en providers. Deze kunnen onbewuste betrokkenheid niet tot nauwelijks vermijden indien ze de privacy en dergelijke van hun klanten willen waarborgen. In sommige gevallen kunnen bedrijven wel degelijk vermoeden dat een relatie bestaat met criminaliteit. In die gevallen is sprake van bewuste betrokkenheid. In elk geval voor 2001 ging het in de sector zodanig goed dat er geen aanleiding was om bewust criminelen te ondersteunen. Als gevolg van het personeelsgebrek was men toen wel kwetsbaar dat handlangers zich als medewerker zouden aanbieden. Na 2001 gaat het veel slechter in de branche. De winstgevendheid staat onder druk, geldschieters zijn moeilijker te vinden en medewerkers worden ontslagen. Die ontslagen medewerkers zijn kwetsbaar voor betrokkenheid. Toch bestaat er geen aanleiding te veronderstellen dat hierdoor de ICT-sector en -deskundigen de illegale groothandel op grote schaal willen en kunnen ondersteunen. In hoeverre de sector zelf malafide ICT-bedrijven of providers zouden kunnen identificeren, is niet apart onderzocht.

Misbruik van de ICT-sector en -deskundigen voor de illegale bedrijfsvoering is al met al niet waarschijnlijk. De voordelen wegen niet op tegen de nadelen, men is niet echt bekend met die bedrijfstak en er is geen aanleiding. Een uitzondering is ‘onbewuste betrokkenheid van de ICT-sector en -deskundigen’ als gevolg van het (gedeeltelijke) gebruik van ICT voor communicatie, administratie en afscherming en het gebruik van de virtuele ruimte als informatiebron.

6.10.3. Beoordeling ongewenste effecten

Als gevolg van de ICT-ontwikkelingen zijn vele organisaties en individuen sterk afhankelijk van de ICT-sector en -deskundigen. Zij komen bij vele organisaties over de vloer, kennen de bedrijfsvoering veelal goed en hebben een vertrouwenspositie. Wanneer

[78] {DNRI, 2004, 105}.
[79] {DNRI, 2004, 46}.

zij betrokken zouden raken bij de illegale groothandel, kan dit hun imago aantasten en daarmee de vertrouwenspositie ondermijnen. Dit kan leiden tot een verlies aan vertrouwen en aantasting van hun integriteit. Dat geldt uiteraard niet voor onbewust betrokken organisaties, zoals telefoonbedrijven of providers die bijvoorbeeld een e-mailadres hebben toegekend. Het geldt wel als via telefoonbedrijven en dergelijke cruciale bedrijfsinformatie zou lekken, ICT-consultants bewust hun diensten aan zouden bieden en zeker als criminelen investeren in ICT-bedrijven. Tevens kan bewuste betrokkenheid van en investeringen in ICT-bedrijven de marktwerking verstoren. Deze bedrijven hebben immers naast de normale ook een andere financieringsbron. Daardoor kan sprake zijn van oneerlijke concurrentie.

6.11. Overzicht beoordeling dreigingen

In dit hoofdstuk zijn zeven dreigingen geïdentificeerd en beoordeeld op waarschijnlijkheid en ongewenste effecten. Slechts één dreiging, 'illegale ICT als groothandelswaar' is als waarschijnlijk beoordeeld (zie figuur 6.3). Het gaat daarbij niet om een wezenlijke verandering. De handel in gestolen of vervalste goederen en goederen met een fiscale prijswig of illegale kopieën, is van alle tijden. En, nieuwe goederen leiden nu eenmaal tot nieuwe objecten voor criminaliteit en daardoor ook tot potentiële groothandelswaar. Daar is niets nieuws onder de zon. Sociale controle is, net als bij de andere handelswaar, tot op zekere hoogte mogelijk. De overige dreigingen zijn als onwaarschijnlijk beoordeeld.

Wanneer de dreigingen zich zouden manifesteren, dan vallen de ongewenste effecten in het algemeen mee (zie figuur 6.3). In de kern verschillen illegale ICT en informatie, twee nieuwe soorten handelswaar, niet zodanig van andere illegale groothandelswaar dat sprake is van vele (extra) ongewenste effecten. Deze beoordeling laat onverlet dat de wetgever elke vorm van illegale handelswaar als ongewenst beschouwt. Evenmin zijn de ongewenste effecten van een virtuele illegale groothandelsonderneming, een nieuw soort, wezenlijk anders dan van een gewone. Hetzelfde geldt voor de nieuwigheden in de bedrijfsvoering. Deze leiden niet tot een substantieel andere bedrijfsvoering en dus niet tot totaal andere ongewenste effecten. Daarmee is niet gezegd dat er geen sprake is van ongewenste effecten.

De dreigingen zijn mede beoordeeld op basis van deeldreigingen op een lager abstractie-niveau (zie figuur 6.4). Enkele daarvan zijn wel als waarschijnlijk beoordeeld in tegenstelling tot de dreiging waartoe zij behoren. Het gaat dan om de deeldreigingen 2A, 3A, 4C, 6A en 7A. Daarentegen is de waarschijnlijkheid van de deeldreiging 'illegale kopieën van software als groothandelswaar' als laag beoordeeld. Dit in tegenstelling tot 'illegale ICT als illegale groothandelswaar' in het algemeen. Enkele deeldreigingen lenen zich om in een aanvullende risicoanalyse verder te onderzoeken. Het gaat dan om: 'kinderporno-afbeeldingen als groothandelswaar', 'witwassen met behulp van virtuele organisaties', 'eigendom van providers door illegale groothandelsondernemingen', 'eigendom van cyberbanken' en specifieke vormen van betrokkenheid van de ICT-sector en -deskundigen. Weliswaar zijn enkele argumenten genoemd die ten grondslag liggen aan de beoordeling, maar enig voorbehoud is op zijn plaats. Er zijn namelijk voorbeelden van deze deeldreigingen bekend en er zijn onduidelijkheden of tegenstrijdigheden die de beoordeling lastig maken.

Nr.	Dreiging	Waarschijnlijkheid	Ongewenste effecten[80]
1	Illegale ICT als groothandelswaar	Waarschijnlijk	Product niet inherent schadelijk Afname veiligheid Financieel verlies, slachtoffers, kopers, producenten en overheden Schade aan buitenlandse betrekkingen
2	Inzet ICT in illegale bedrijfsvoering	Niet waarschijnlijk	Geen ongewenste effecten ten opzichte van een gewone bedrijfsvoering Ongewenste effecten van dreiging 7
3	Illegale informatie als groothandelswaar	Niet waarschijnlijk	Product niet inherent schadelijk, m.u.v. kinderporno-afbeeldingen (seksueel misbruik kinderen) Afname veiligheid en leefbaarheid Financieel verlies slachtoffers, branches, banken, overheden Verstoring marktwerking Schade aan buitenlandse betrekkingen Ongewenste effecten van dreigingen 6 en 7
4	Vergroting inzet informatie in illegale bedrijfsvoering	Niet waarschijnlijk	Geen ongewenste effecten ten opzichte van een gewone bedrijfsvoering Afname van vertrouwen in de overheid of andere instanties Ongewenste effecten dreiging 7
5	Virtuele illegale groothandelsonder-nemingen	Niet waarschijnlijk	Het gaat om dezelfde producten als gewone illegale groothandelsondernemingen Afname veiligheid Schade aan buitenlandse betrekkingen Ongewenste effecten van dreigingen 6 en 7
6	Omzetting van gewone naar virtuele illegale bedrijfs-voering	Niet waarschijnlijk	In het algemeen geen ongewenste effecten ten opzichte van een gewone bedrijfsvoering Aantasting vertrouwen in virtuele organisaties Ongewenste effecten van dreiging 7
7	Misbruik ICT-sector en -deskundigen voor illegale bedrijfs-voering	Niet waarschijnlijk	Verlies van vertrouwen ICT-sector Aantasting integriteit ICT-sector Verstoring marktwerking

Figuur 6.3 Overzicht dreigingen en de beoordeling

Het algemene beeld op basis van deze risicoanalyse is dat de ICT-ontwikkelingen niet tot nauwelijks leiden tot veranderingen in illegale groothandelswaar, groothandelsondernemingen en de bedrijfsvoering daarvan. Als die veranderingen zich wel zouden voordoen, dan vallen de extra ongewenste effecten in het algemeen mee.

[80] De bijkomende ongewenste effecten van dreiging 2 zijn gelijk aan die van een gewone bedrijfsvoering. Daarom zijn die bij de dreigingen 4, 5 en 6 niet apart genoemd.

Nr.	Dreiging	Waarschijn-lijkheid	Ongewenste effecten[81]
1	Illegale ICT als groothandelswaar		
1A	Gestolen hard- en (fysieke) software als groothandelswaar	Waarschijnlijk	Product niet inherent schadelijk Afname veiligheid Financieel verlies slachtoffers Schade aan buitenlandse betrekkingen
1B	Illegale groothandel in ICT-producten als instrument voor marktreguleringsfraude	Waarschijnlijk	Product niet inherent schadelijk Financieel verlies overheden Schade aan buitenlandse betrekkingen
1C	Vervalste hard- en (fysieke) software als groothandelswaar	Waarschijnlijk	Product niet inherent schadelijk Financieel verlies kopers en producenten Schade aan buitenlandse betrekkingen
1D	Illegale kopieën van software als groothandelswaar	Niet waarschijnlijk	Product niet inherent schadelijk Financieel verlies producenten Schade aan buitenlandse betrekkingen
2	Inzet ICT in illegale bedrijfsvoering		
2A	Inzet ICT in illegale bedrijfsvoering voor communicatie, administratie en afscherming	Waarschijnlijk	Geen ongewenste effecten ten opzichte van een gewone bedrijfsvoering Ongewenste effecten van dreiging 7
2B	Inzet ICT in illegale bedrijfsvoering ter ondersteuning van andere veranderingen	Niet waarschijnlijk	Idem
2C	Inzet ICT in illegale bedrijfsvoering voor overige doeleinden	Niet waarschijnlijk	Idem
3	Illegale informatie als groothandelswaar		
3A	Gestolen en vervalste (fysieke vormen van) audio en video als groothandelswaar	Waarschijnlijk	Product niet inherent schadelijk Afname veiligheid Financieel verlies slachtoffer of branches Schade aan buitenlandse betrekkingen
3B	Spionage-informatie als groothandelswaar	Niet waarschijnlijk	Product niet inherent schadelijk Afname veiligheid en leefbaarheid Financieel verlies van slachtoffers Verstoring marktwerking Schade aan buitenlandse betrekkingen
3C	Gestolen en gemanipuleerde creditcard-[82] en identiteitsinformatie als groothandels-waar	Niet waarschijnlijk	Product niet inherent schadelijk Afname veiligheid en leefbaarheid Financieel verlies banken, slachtoffers Schade aan buitenlandse betrekkingen
3D	Illegaal gekopieerde audio en video als groothandelswaar	Niet waarschijnlijk	Product niet inherent schadelijk Financieel verlies branches Verstoring marktwerking Schade aan buitenlandse betrekkingen Ongewenste effecten van dreigingen 6 en 7
3E	Kinderporno-afbeeldingen (foto's en video) als groothandelswaar	Niet waarschijnlijk	Seksueel misbruik van kinderen Afname veiligheid en leefbaarheid Schade aan buitenlandse betrekkingen Ongewenste effecten van dreigingen 6 en 7
4	Vergroting inzet informatie in illegale bedrijfsvoering	Niet waarschijnlijk	
4A	Groter gebruik van opsporingsinformatie in illegale bedrijfsvoering (offensieve afscherming)	Niet waarschijnlijk	Afname van vertrouwen in de overheid Ongewenste effecten van dreiging 7
4B	Inzet van bij anderen ontvreemde informatie in illegale bedrijfsvoering	Niet waarschijnlijk	Afname van vertrouwen in de instantie Ongewenste effecten van dreiging 7

[81] Idem.
[82] Dit is inclusief de gegenereerde creditcardinformatie.

Nr.	Dreiging	Waarschijn-lijkheid	Ongewenste effecten[81]
4C	Gebruik van virtuele ruimte als informatiebron voor illegale bedrijfsvoering	Waarschijnlijk	Geen ongewenste effecten ten opzichte van een gewone bedrijfsvoering
4D	Vergroting inzet informatie in illegale bedrijfsvoering voor overige doeleinden	Niet waarschijnlijk	Geen ongewenste effecten ten opzichte van een gewone bedrijfsvoering Ongewenste effecten van dreiging 7
5	Virtuele illegale groothandelsonderne-mingen		
5A	Virtuele ruimte als marktplaats voor illegale producten	Niet waarschijnlijk	Het gaat om dezelfde producten als gewone illegale groothandelsondernemingen Ongewenste effecten van dreigingen 6 en 7
5B	Buitenlandse virtuele ondernemingen actief in Nederland	Niet waarschijnlijk	Het gaat om dezelfde producten als gewone illegale groothandelsondernemingen Afname veiligheid Ongewenste effecten van dreigingen 6 en 7
5C	Nederlandse virtuele ondernemingen actief in het buitenland	Niet waarschijnlijk	Het gaat om dezelfde producten als gewone illegale groothandelsondernemingen Schade aan buitenlandse betrekkingen Ongewenste effecten van dreigingen 6 en 7
6	Omzetting van gewone naar virtuele illegale bedrijfsvoering		
6A	Omzetting van gewone naar virtuele illegale bedrijfsvoering voor de communicatie	Waarschijnlijk	In het algemeen geen ongewenste effecten ten opzichte van een gewone bedrijfs-voering Ongewenste effecten van dreiging 7
6B	Omzetting van gewone naar virtuele illegale bedrijfsvoering voor de administratie	Niet waarschijnlijk	Idem
6C	Misbruik virtuele organisaties ten behoeve van legitimering, facilitering en witwassen	Niet waarschijnlijk	In het algemeen geen ongewenste effecten ten opzichte van een gewone bedrijfs-voering Aantasting vertrouwen in virtuele organisaties Ongewenste effecten van dreiging 7
6D	Oprichting van virtuele organisaties ten behoeve van de illegale bedrijfsvoering	Niet waarschijnlijk	Idem
6E	Omzetting van gewone naar virtuele illegale bedrijfsvoering voor overige doeleinden	Niet waarschijnlijk	In het algemeen geen ongewenste effecten ten opzichte van een gewone bedrijfs-voering Ongewenste effecten van dreiging 7
7	Misbruik ICT-sector en -deskundigen voor illegale bedrijfsvoering		
7A	Onbewuste betrokkenheid ICT-sector en -deskundigen bij illegale bedrijfsvoering	Waarschijnlijk	Geen
7B	Bewuste betrokkenheid ICT-sector en -deskundigen bij illegale bedrijfsvoering	Niet waarschijnlijk	Verlies van vertrouwen ICT-sector Aantasting integriteit ICT-sector Verstoring marktwerking
7C	Investering in ICT-bedrijven voor illegale bedrijfsvoering	Niet waarschijnlijk	Idem

Figuur 6.4 Overzicht deeldreigingen en de beoordeling van waarschijnlijkheid en ongewenste effecten

7. Nabeschouwing

7.1. Inleiding

Dit proefschrift bestaat uit twee componenten. De eerste is een instrumentarium voor risicoanalyse. Dat instrumentarium is vooral toegespitst op het verschaffen van inzicht voor vroegtijdige beheersing van georganiseerde criminaliteit. De tweede component is een analyse van de risico's van veranderingen in georganiseerde criminaliteit als gevolg van de ICT-ontwikkelingen (zie figuur 7.1). Het achterliggende doel is om ervaring op te doen met de toepassing van het instrumentarium.

Het ontwikkelde instrumentarium bestaat uit drie onderdelen, namelijk. 1) een uitwerking van risicoanalyse, 2) een conceptualisering van georganiseerde criminaliteit en 3) een analysekader. Paragraaf 7.2 blikt terug op het tweede onderdeel. Paragraaf 7.3 beschrijft de ervaringen met het analysekader en geeft enkele suggesties voor nader onderzoek. Paragraaf 7.4 gaat nog eens in op de relatie tussen een strategische risicoanalyse en criminaliteitsbeheersing in het licht van een nieuw sturingsconcept, namelijk informatiegestuurde opsporing. Deze nabeschouwing eindigt met een slotoverweging (paragraaf 7.5).

Component		Onderdeel		Element	
1	Risicoanalyse-instrumentarium	1.1	Risicoanalyse voor vroegtijdige criminaliteitsbeheersing		
		1.2	Conceptueel model georganiseerde criminaliteit		
		1.3	Analysekader georganiseerde criminaliteit	1.3.1	Typologie van veranderingen
				1.3.2	Risicofactoren voor beoordeling waarschijnlijkheid
				1.3.3	Uitgangspunten voor beoordeling ongewenste effecten en beschrijving van enkele ongewenste effecten
2	Risicoanalyse veranderingen georganiseerde criminaliteit als gevolg van ICT-ontwikkelingen	2.1	Analyse van ICT-ontwikkelingen		
		2.2	Geïdentificeerde dreigingen en beoordeling ervan		

Figuur 7.1 Opbouw proefschrift

7.2. Georganiseerde criminaliteit als stelsel van illegale groothandelsondernemingen

Bij georganiseerde criminaliteit draait het om de activiteiten van illegale groothandelsondernemingen. Hun belangrijkste drijfveer is het op illegale wijze verdienen van geld. Een groothandel produceert zelf geen producten en verkoopt deze evenmin aan eindconsumenten. Hij neemt de producten af van andere partijen en verkoopt deze aan

andere groothandelaren en/of aan de detailhandel. Daarnaast kan de groothandel zich richten op het sorteren, opslaan, transporteren en financieren van de producten evenals op het nemen van marktrisico's ten behoeve van leveranciers en afnemers en het vergaren van marktinformatie.

Dit conceptuele model is behulpzaam bij de afbakening ten opzichte van andere daders en criminele activiteiten. Niet elk crimineel samenwerkingsverband vormt een misdaadonderneming. Niet elke misdaadonderneming kan de rol van groothandel op zich nemen. Bovendien zijn niet alle illegale producten geschikt voor de groothandel. En niet alle vormen van criminaliteit zijn gerelateerd aan de handel in illegale producten. Een nadeel is dat het concept niet empirisch is getoetst. Vele aannames, waaronder bijvoorbeeld die van de winstgerichtheid, zijn wel door anderen getoetst, maar niet tezamen. Als de onderliggende aannames wel zijn getoetst door anderen, dan is dat veelal gebeurd vanuit uiteenlopende theoretische hoofdstromen, modellen en achtergronden.

Een los einde in het concept betreft de eventuele uitwerking van het aspect 'grootschaligheid van de handel'. Grootschalige handel is immers niet eenduidig en kan variëren per misdaadmarkt. Bovendien kan het gaan om de omvang van de handel, de financiële omzet en/of de periodiciteit.[1] Aan die uitwerking kleeft zowel een normatieve component als een empirische. Normatief, omdat de keuze de vormen van handel en misdaadondernemingen afbakent die onder het beladen begrip georganiseerde criminaliteit vallen. Empirisch, omdat hiervoor gegevens nodig zijn per misdaadmarkt over de omvang van de handel, de financiële omzet en/of de periodiciteit. Deze gegevens zijn echter niet tot nauwelijks voorhanden.

Het perspectief van illegale groothandelsondernemingen werpt een ander licht op de samenhang met en de afbakening ten opzichte van andere vormen van criminaliteit. De illegale groothandelsondernemingen vervullen een rol in een groter geheel, namelijk in misdaadmarkten. Daarin opereren partijen vanuit uiteenlopende, maar wel onderling samenhangende rollen. Zo is de illegale groothandel afhankelijk van leveranciers en afnemers. Deze zijn op hun beurt weer afhankelijk van anderen. De handel vindt veelal plaats in mondiale netwerken met lokale vertakkingen. Zij kunnen één of meer misdaadmarkten omspannen. Per zakelijke transactie, bijvoorbeeld de import van een container drugs, kan de onderneming een samenwerkingsverband smeden vanuit de netwerken. Er is dus sprake van een samenhangend systeem van 'misdaadmarktgerichte criminaliteit'.

Doordat georganiseerde criminaliteit onderdeel uitmaakt van een groter geheel, moet de beheersing ervan eveneens vanuit dat grotere geheel plaatsvinden. Wanneer de politie alleen autodieven op districtelijk niveau aanpakt, blijven de helers, de illegale groothandel en de netwerken buiten schot. Een aanpak waarin alleen landelijke en regionale rechercheteams de illegale groothandel bestrijden, laat de helers en autodieven buiten schot. Er is daarom een samenhangende strategie en organisatie noodzakelijk op basis waarvan en van waaruit de belanghebbenden doelgericht kunnen interveniëren. In het ene geval zou bijvoorbeeld de politie met het arresteren van enkele sleutelfiguren één of meer misdaadmarkten (tijdelijk) kunnen lamleggen. In een ander geval zou de overheid juist met bijvoorbeeld regulatie van de grondstoffen voor de illegale waar een misdaadmarkt kunnen

[1] Zie paragraaf 3.7 voor dit vraagstuk.

frustreren. Een dergelijke integrale en multidisciplinaire aanpak vereist wel inzicht in de werking van misdaadmarkten op zowel strategisch als tactisch niveau.

7.3. Ervaringen met analysekader

Randvoorwaardelijk voor een risicoanalyse ten behoeve van vroegtijdige criminaliteitsbeheersing is inzicht in de trits 'ontwikkeling(en) – veranderingen in criminaliteit – ongewenste effecten' en de waarschijnlijkheid van die veranderingen. Het uitgangspunt is gehanteerd dat in ieder geval voor georganiseerde criminaliteit een expliciet analysekader nodig is. Dit in verband met de omvang van het domein.

Het analysekader bestaat uit drie elementen (zie figuur 7.1). Het eerste is een typologie van veranderingen, namelijk veranderingen in: illegale groothandelswaar, groothandelsondernemingen en bedrijfsvoering. Op basis van de combinatie daarvan met kenmerken van een maatschappelijke ontwikkeling, kunnen we concrete dreigingen identificeren. Het tweede element benoemt risicofactoren per soort verandering. Het derde element specificeert uitgangspunten ter bepaling van de ongewenste effecten en beschrijft er enkele. De eerste twee elementen zijn afgeleid van de gelegenheidsfactoren voor georganiseerde criminaliteit. Deze paragraaf blikt terug op de ervaringen op grond van de uitgevoerde risicoanalyse. Tevens schetst deze paragraaf enkele suggesties ter verbetering en voor andere denkbare toepassingen.

Ten behoeve van de identificatie van dreigingen is, in aanvulling op bovenstaand kader, gebruikgemaakt van literatuur en de meningen van enkele experts. De ICT-ontwikkelingen zijn per slot van rekening al enige jaren aan de gang. De bestudeerde onderzoeken richten zich op (nieuwe vormen van) criminaliteit als gevolg van bepaalde aspecten van de ICT-ontwikkelingen.[2] Voorbeelden daarvan zijn de technische kant van de ontwikkelingen, het internet en de computer zelf als doelwit of instrument voor het plegen van criminaliteit. De onderzoekers behandelen merendeels het gehele spectrum van criminaliteit, van het maken van een virus tot georganiseerde criminaliteit en terrorisme. De meeste behandelen ook het gehele spectrum van daders, van stalkers tot inlichtingendiensten. Zij hanteren verder uiteenlopende ordeningen voor de criminaliteitsvormen, waaronder hacken en creditcardfraude. In die ordeningen lopen doel en middel door elkaar. De intentie achter bijvoorbeeld het hacken kan variëren van een plezierige vrijetijdsbeleving, geld verdienen door fraude te plegen tot het plegen van een terroristische aanslag. Hacken is dus niet alleen een aparte criminaliteitsvorm, maar merendeels een middel voor andere vormen van criminaliteit. Evenmin kijkt het merendeel van de onderzoekers van buiten naar binnen[3] en zij behandelen niet afzonderlijk de veranderingen in illegale groothandelswaar, groothandelsondernemingen en de bedrijfsvoering. In aanvulling op de bestudeerde literatuur zijn tevens vier interviews gehouden (zie bijlage 4). Tijdens die interviews is niet alleen gevraagd naar bekende vormen van criminaliteit, maar ook naar mogelijke nieuwe vormen. De geïnterviewden noemden uiteenlopende voorbeelden vanuit de eigen referentiekaders.

[2] Bestudeerd zijn onder andere {Boni & Kovacich, 1999}, {DNRI, 2004}, {Galeotti, 2000B}, {Hoogenboom, 2001}, {NCIS, 1999}, {O'Brien, 2000}, {Power, 2000A}, {Power, 2000B}, {Robinson, 2000}, {Stol e.a., 1999A}, {Stol e.a., 1999B}, {Vriesde e.a., 1999}, {Williams, 1999}

[3] O'Brien, Williams en Hoogenboom hebben dat op onderdelen wel gedaan {O'Brien, 2000}, {Williams, 1999} en {Hoogenboom, 2001}.

Op basis van de kenmerken van de ICT-ontwikkelingen en de typologie van veranderingen (identificatiekader) zijn zeven dreigingen geïdentificeerd. Deze werkwijze heeft *geen* echt wezenlijk andere veranderingen opgeleverd ten opzichte van de geraadpleegde literatuur en experts. Dat betekent echter niet dat het analysekader geen toegevoegde waarde heeft. Zonder het kader zou niet te beoordelen zijn geweest in hoeverre de aangetroffen en genoemde voorbeelden een volledig beeld geven. Private partijen, de overheid, de politie maar ook criminelen, zijn immers nog relatief onbekend met de ICT-ontwikkelingen. Bovendien bevinden de door anderen genoemde dreigingen zich op uiteenlopende abstractieniveaus en zijn bedacht of onderzocht vanuit een specifiek aspect of een andere invalshoek. Het kader daarentegen dwingt om per kenmerk de vraag te stellen welke soorten veranderingen daaruit voort zouden kunnen komen. Dit komt de precisie en de volledigheid ten goede. Bovendien biedt het kader een kapstok ter bepaling van het abstractieniveau en de ordening, namelijk op basis van de kenmerken en de soorten veranderingen.

Een nadeel is dat de kenmerken van de ICT-ontwikkelingen niet empirisch zijn getoetst. Daardoor is niet zeker dat dit echt de kenmerken zijn. Evenmin zijn zij getoetst of bediscussieerd in een wetenschappelijk forum. Hetzelfde geldt voor de soorten veranderingen die voortkomen uit het gehanteerde concept van georganiseerde criminaliteit. Dit nadeel is inherent aan het doel en de gekozen opzet van het proefschrift.

Het *tweede element* van het analysekader richt zich op de beoordeling van de waarschijnlijkheid. Enkele van de bestudeerde onderzoeken vermelden dat georganiseerde criminaliteit inspeelt op de ICT-ontwikkelingen. Een expliciete onderbouwing daarvan ontbreekt, of deze is summier of arbitrair. Zo raakt volgens O'Brien transnationale georganiseerde criminaliteit steeds meer betrokken bij cyberdiefstal. Hij verwijst ter onderbouwing van deze stelling onder andere naar een door Power beschreven casus van de Phonemasters. Die casus betrof een groep criminelen die zich bezighield met informatiemakelaardij. Het ging in die casus primair om de activiteiten van een groep van vier mannen uit de Verenigde Staten. Die groep verkocht informatie aan buitenlanders en via een omweg aan de maffia in Sicilië. Deze groep is al in augustus 1994 ontdekt, in februari 1995 ontmanteld en uiteindelijk in 1999 veroordeeld. Hoezo betrokkenheid van georganiseerde criminaliteit en (in 2000) een toenemende betrokkenheid bij cyberdiefstal? O'Brien merkt verder op dat de Russische maffia de criminele activiteiten verplaatst van drugs naar de meer winstgevende misdaadmarkten van computers. Hierbij ontbreekt een onderbouwing of bronverwijzing. Hoewel hij dus veronderstelt dat georganiseerde criminaliteit inspeelt op de ICT-ontwikkelingen, is de onderbouwing afwezig of arbitrair. Nu is hij geen gerespecteerde expert of onderzoeker, maar het gemak waarmee hij dat veronderstelt, zien we ook bij anderen.[4] Natuurlijk is het niet ingewikkeld om bijvoorbeeld de verwachting uit te spreken dat ook criminelen via het internet illegale goederen kunnen aanbieden. Maar een beoordeling op basis van risicofactoren geeft meer houvast dan losstaande verwachtingen. Datzelfde geldt voor feiten. Een eventuele stijging in één jaar tijd van 0 naar 100 websites waar criminelen drugs aanbieden, zegt bijvoorbeeld nog

[4] Boni en Kovacich, Galeotti, O'Brien, Power, Robinson en Williams veronderstellen dat georganiseerde criminaliteit inspeelt op de nieuwe mogelijkheden van ICT zonder grondige onderbouwing {Boni & Kovacich, 1999}, {Galeotti, 2000B}, {O'Brien, 2000}, {Power, 2000B}, {Robinson, 2000}, {Williams, 1999}. In het Nationaal Dreigingsbeeld onderbouwen de onderzoekers de waarschijnlijkheid wel {DNRI, 2004}. Dit onderzoek is echter pas totstandgekomen nadat de analyses van dit proefschrift al waren uitgevoerd.

weinig over de waarschijnlijkheid van 'virtuele illegale groothandelsondernemingen' en de geschiktheid van de virtuele ruimte voor criminele e-commerce.

Op grond van de beoordeling van de risicofactoren zijn zes van de zeven geïdentificeerde dreigingen als onwaarschijnlijk beoordeeld. Dat is een verrassende uitkomst. De keuze om de risico's van de ICT-ontwikkelingen te analyseren, kwam tot stand tijdens de hoogtijdagen van wat we nu beschouwen als de internethype. De virtuele boekenzaak 'Amazon.com' was het toonbeeld van de revolutie die gaande was in het bedrijfsleven. Het beeld werd gecreëerd dat alle niet-virtuele boekenzaken op korte termijn hun zaak zouden kunnen sluiten. Elk bedrijf dat zich niet met e-commerce zou bezig houden, zou op termijn verdwijnen. Al rond 1994 speelden twee grote oplichtingszaken met een virtuele bank, de European Union Bank[5] en de Citibank.[6] Het beeld drong zich op dat criminelen volop gebruikmaakten of zouden maken van de nieuwe mogelijkheden van ICT. In elk geval bestond de stellige indruk dat zeker plegers van georganiseerde criminaliteit daarvan gebruik zouden (gaan) maken. Men neemt immers aan dat zij flexibel inspelen op gewijzigde omstandigheden. Ook collegae waren daar van overtuigd of wekten op zijn minst de indruk. En, hoe kon het ook anders in die tijd? Weliswaar bleek uit de toenmalige EU-inventarisatie van criminele groepen in Nederland en de (eerste) WODC-monitor uit 1999 nog niet dat georganiseerde criminaliteit daadwerkelijk inspeelde op de ICT-ontwikkelingen. Maar, dat was eerder een extra bevestiging van het selectieve beeld dat opsporingsinstanties hebben, dan een signaal dat het wel eens zou kunnen meevallen. Nu weten we dat elk dorp nog steeds beschikt over boekenzaken en dat vele andere virtuele boekenzaken hun website al weer lange tijd geleden hebben opgeheven. We weten nu ook dat vele virtuele organisaties vrijwel net zo snel zijn verdwenen als ze ooit tevoorschijn kwamen. De oplichting met virtuele banken heeft, voorzover bekend, geen grote navolging gekregen. 'Amazon.com', de European Union Bank en de Citibank lijken redelijk uniek te zijn (geweest). Desondanks zijn de bevindingen van de risicoanalyse opmerkelijk omdat men nog steeds aanneemt dat georganiseerde criminaliteit inspeelt op de ICT-ontwikkelingen en dat deze leiden tot ongewenste veranderingen.[7] Gewezen wordt dan op bijvoorbeeld de voordelen van het internationale karakter van de virtuele ruimte en de anonimiteit daarin. In dit proefschrift is juist beargumenteerd dat naast die voordelen er ook nadelen aan kleven.

Een beperking is dat de risicofactoren in het kader niet empirisch zijn getoetst. De waarde ervan staat nog niet vast. De risicofactoren zijn verder ook nog niet geoperationaliseerd tot risico-indicatoren. Een ander nadeel is dat de beoordeling slechts is gebaseerd op de argumenten van één persoon. Deze nadelen zijn inherent aan het doel en de gekozen opzet van het proefschrift.

De risicofactoren roepen enkele vragen op. Als gevolg van de keuze om deze af te leiden van de gelegenheidsfactoren, resulteert de samenhang tussen de gelegenheidsfactoren ook in samenhang tussen de risicofactoren. Wanneer bepaalde illegale producten niet geschikt zijn als groothandelswaar, is het ook niet aannemelijk dat een illegale groothandelsonder-

[5] Zie paragraaf 5.6.
[6] {O'Brien, 2000}, {Power, 2000B, 92, 102-113}, {Sweeney, 1999}, {Robinson, 2000, 362}.
[7] Eigen waarneming binnen de politie en mede gebaseerd op twee Group Decision Room-sessies met recherchechefs op 18 november 2003 en anderen, waaronder wetenschappers en leden van het Openbaar Ministerie, op 20 november 2003. Op grond van (onder andere) die twee sessies is het gebruik van ICT één van de specifieke invalshoeken geweest in het Nationaal Dreigingsbeeld {DNRI, 2004, 9-12}.

neming daarin wil of kan handelen. Opvallend daarbij is dat de analyse grotendeels zou kunnen volstaan met een beoordeling van twee risicofactoren. De mate van geschiktheid van de handelswaar bepaalt het oordeel over de nieuwe illegale producten en deels over nieuwe groothandelsondernemingen.[8] De mate van aantrekkelijkheid van de andere mogelijkheden voor de bedrijfsvoering bepaalt het oordeel over de veranderingen in de bedrijfsvoering en deels over de opkomst van virtuele groothandelsondernemingen.[9] Dit opvallende punt kan wijzen op een fout in het analysekader, in de analyse of op toeval berusten.

Verder heeft het kader nog als aanvullende meerwaarde dat opmerkelijke punten aan de hand van de risicofactoren nader kunnen worden onderzocht. Zo maakt het Nationaal Dreigingsbeeld melding van betrokkenheid van georganiseerde criminaliteit bij kinderporno. De aanname hier is echter dat kinderporno-afbeeldingen niet geschikt zijn als illegale groothandelswaar. Aan de hand van de risicofactoren kan de beschikbare casuïstiek nader worden onderzocht en kan worden gekeken of en in hoeverre één van de aannames niet juist is.[10]

Volgens Hughes-Wilson geldt dat het achterhalen van iemands intenties de echte uitdaging vormt voor (militair) inlichtingenwerk.[11] En juist over de intentie van illegale groothandelaren is weinig bekend. Tijdens de risicoanalyse kwamen enkele vragen naar boven. Bij welk niveau van sociale controle stappen ze uit of in de handel? Bij welke mate van geschiktheid van de producten gaan ze handelen? Wanneer huren ze ondersteuning in als ze zelf de noodzakelijke bekwaamheden ontberen voor lucratieve handel? Hebben ze inderdaad een voorkeur voor bepaalde soorten handelswaar, ongeacht de mate van winstgevendheid? Op grond van een beter inzicht daarin kan de waarschijnlijkheid zorgvuldiger worden beoordeeld. Nader onderzoek naar de intentie van illegale groothandelaren is daarom wenselijk.

Het beoordelingskader voor de ongewenste effecten, het *derde element* van het analysekader, is minder ver uitgewerkt dan oorspronkelijk was beoogd. De beoordeling van de ongewenste effecten van illegale groothandelsactiviteiten roept vele vragen op waarop het antwoord niet eenvoudig en bovendien subjectief is. Wat zijn de ongewenste effecten van de afzonderlijke illegale producten die zich lenen voor de groothandel? Moeten we de overlast door verslaafden en schade aan het imago van Nederland toerekenen aan het product drugs, aan de groothandel erin of juist aan de verslaafden? Moeten we een onderscheid maken naar de soorten groothandelsfuncties, zoals de koop, verkoop en transport? Ook niet duidelijk is wat de ongewenste effecten zijn van diverse soorten misdaadondernemingen. Leiden buitenlandse misdaadondernemingen tot een grotere aantasting van belangen dan autochtone? Leiden enkele illegale groothandelsondernemingen tot meer ongewenste effecten dan vele kleinere? En wat zijn de ongewenste effecten van (aspecten van) de illegale bedrijfsvoering? Is het inderdaad wel zo ongewenst dat misdaadondernemingen investeren in de bovenwereld als oudedagsvoorziening? Is dat niet beter dan dat zij hun geld investeren in nieuwe illegale handelswaar?[12] In hoeverre moeten

[8] Dreigingen 1, 3 en 5.
[9] Dreigingen 2, 4 tot en met 7.
[10] Zie paragraaf 6.6.2.
[11] {Hughes-Wilson, 1999, 310}.
[12] Deze laatste vraagt werpt Naylor op {Naylor, 1997}.

we de effecten voor de internationale gemeenschap meenemen? De antwoorden op deze vragen zijn deels empirisch, deels analytisch, maar grotendeel normatief van aard. In verband met het doel van dit proefschrift voert het te ver om alle vragen te beantwoorden, voorzover dit al mogelijk is. Wel zijn op basis van beleidsdocumenten en literatuur enkele ongewenste effecten benoemd. Een nadeel daarbij was dat de beleidsdocumenten en literatuur veelal niet de gezochte antwoorden geven of niet aansluiten bij de geformuleerde uitgangspunten. Zo maakt men bijvoorbeeld geen onderscheid tussen de ongewenste effecten van de illegale handelswaar, onderneming en bedrijfsvoering. Toch is dit onderscheid cruciaal voor een zorgvuldige analyse. Verder benoemt men slechts zelden belangen die in het geding zijn, terwijl daarvoor wel goede argumenten zijn aan te voeren.[13]

Voor een risicoanalyse is het wenselijk dat uiteindelijk de verzameling van ongewenste effecten kan worden gekwalificeerd als ernstig of niet-ernstig. Op basis daarvan kunnen de risico's worden geordend. Daartoe moeten wel de afzonderlijke effecten worden voorzien van een gewicht. Is bijvoorbeeld verstoring van de marktwerking ernstiger dan schade aan buitenlandse betrekkingen? Zijn de ongewenste effecten van het product drugs ernstiger dan van het product mensenhandel? De bepaling van deze gewichten is normatief en betreft geen wetenschappelijke activiteit. Hooguit kunnen wetenschappers ondersteuning verlenen om op een transparante wijze dit oordeel van de besluitvormers te achterhalen en te onderbouwen. Uit het huidige beleid en de doelstellingen van de overheid en het Openbaar Ministerie kunnen dergelijke normatieve keuzen niet worden gedestilleerd.

Als gevolg van deze genoemde beperkingen zijn de ongewenste effecten in hoofdstuk 6 slechts globaal beoordeeld. Volstaan is om deze op hoofdlijnen te schetsen. Er is geen eindoordeel gegeven over de ongewenste effecten per dreiging in termen van ernstig of niet ernstig.

De politiedepartementen, politici en de top van het Openbaar Ministerie zouden er goed aan doen om een normatief kader te ontwikkelen. Wat beschouwen zij als de ongewenste effecten van de illegale groothandelswaar, groothandelsondernemingen en bedrijfsvoering? Welke daarvan moeten in elk geval worden voorkomen? Een ander, maar daar wel mee samenhangend element, betreft de bijdrage die men van afzonderlijke partijen verlangt bij criminaliteitsbeheersing. Waarop moet de politie haar aandacht vooral richten als het gaat om bijvoorbeeld mensensmokkel? Op alle smokkelaars? Op smokkelaars die grote aantallen vluchtelingen smokkelen? Moet de aandacht ook uitgaan naar smokkelaars met de Nederlandse nationaliteit, zonder dat de vluchtelingen Nederland binnenkomen? En tot hoe ver gaat dat wanneer het vreemdelingenbeleid steeds strenger wordt en dus de noodzaak voor asielzoekers om in zee te gaan met mensensmokkelaars steeds meer toeneemt? En waarop moeten anderen zich richten? Onbewuste betrokkenheid bij georganiseerde criminaliteit tast abstracte belangen aan die veelal op de lange termijn spelen en indirect en collectief van aard zijn. Het gaat dan om belangen zoals de integriteit van het financiële stelsel of van de overheid. De kosten van risicobeheersing gaan ruimschoots voor de baten uit. De vraag speelt daarbij wie welke bijdrage kan of moet leveren en ten koste van wat. De gehele Nederlandse economie heeft profijt wanneer bijvoorbeeld de Russische maffia via Nederland crimineel geld zou doorsluizen naar

[13] Zie subparagraaf 1.2.2.

andere landen. Moeten banken deze transacties weigeren? Moeten ze de transacties doorgeven aan de politie? In hoeverre is de politie überhaupt verantwoordelijk voor de integriteit van het financiële stelsel? En moet de overheid ook zelf niet meer rekening houden met de neveneffecten van het eigen beleid? Via fiscaal aantrekkelijke voorwaarden probeert de overheid buitenlandse bedrijven te stimuleren om te investeren in Nederland. Des te lager de formele eisen die men daar aan stelt, des te groter de kans dat malafide bedrijven gebruik maken van die regelingen. Een discussie over de bijdrage van de afzonderlijke partijen is gewenst. Deze discussie is gediend bij een normatief kader waarin is aangegeven welke belangen in het geding kunnen zijn en welke waarde men hecht aan de bescherming van die belangen. Door deze duidelijkheid zou het eenvoudiger zijn om het beleid te ondersteunen met wetenschappelijk onderzoek en analyses. Dat kan dan gerichter plaatsvinden, namelijk op basis van (de meest) ongewenste effecten. Het zou ook eenvoudiger zijn om de aanpak gerichter ter hand te nemen en de activiteiten in het kader van criminaliteitsbeheersing te prioriteren. De geformuleerde analytische uitgangspunten kunnen dienen als basis voor de discussie. Verder zou het behulpzaam zijn wanneer empirisch onderzoek beschikbaar is over de relatie tussen bepaalde soorten veranderingen en ongewenste effecten.

Het instrumentarium is nog niet compleet. Gekozen is om de identificatie en selectie van relevante ontwikkelingen en de interpretatie daarvan naar de toekomst toe, niet mee te nemen. Gekeken is vooral naar enkele huidige kenmerken van één specifieke cluster van ontwikkelingen, namelijk de ICT-ontwikkelingen. De huidige stand van zaken is niet doorgetrokken naar de toekomst. Naast de ICT-ontwikkelingen zijn ook vele andere ontwikkelingen onderzoekswaardig. Voorbeelden daarvan zijn de toekomstige uitbreiding van de EU met landen als Turkije, de intrede van biotechnologie, de creatie van een wereldwijd financieel systeem, mondialisering, de ontwikkelingen in het Midden-Oosten et cetera. Deze ontwikkelingen liggen nog redelijk voor de hand. Wellicht zijn er andere ontwikkelingen die leiden tot veranderingen met een hogere waarschijnlijkheid en/of meer ongewenste effecten. Omdat er zeer vele ontwikkelingen kunnen leiden tot veranderingen, zijn instrumenten voor de identificatie en selectie onontbeerlijk. Dat zou mede plaats kunnen vinden op grond van een normatief kader. De achterliggende vraag is dan: welke ontwikkelingen tasten de belangrijkste belangen van Nederland aan? Dit is eerder aangeduid als ‘achteruit redeneren’.[14] Wanneer gekozen is om ontwikkelingen te onderzoeken, is het wenselijk om deze ook naar de toekomst door te trekken. Hoe zien bijvoorbeeld de ICT-ontwikkelingen er over enkele jaren uit en wat betekent dat dan voor de dreigingen, de waarschijnlijkheid en ongewenste effecten? Instrumenten voor toekomstgericht onderzoek, waaronder het gebruik van scenariostudies, ontbreken nog in het ontwikkelde instrumentarium.

Een uitbreiding van het analysekader met een typologie van maatschappelijke ontwikkelingen in combinatie met bijbehorende risico’s, is eveneens wenselijk. De verdere uitbreiding van de EU in de nabije toekomst leent zich bijvoorbeeld voor een vergelijking met het verdwijnen van het IJzeren Gordijn en de uitbreiding in 2004. In de risicoanalyse van dit proefschrift staat een primair technologische ontwikkeling centraal. Bij andere technologische ontwikkelingen kan hiervan gebruik worden gemaakt. Soortgelijke dreigingen zijn dan immers denkbaar. Op die wijze kan lering worden getrokken uit

[14] Zie subparagraaf 2.4.4.

vergelijkbare ontwikkelingen uit het verleden. En hoewel niet eenvoudig, zou dat effect nog verder worden versterkt indien de uitgevoerde risicoanalyse na verloop van tijd wordt geëvalueerd. De aannames kunnen dan worden getoetst aan de hand van de dan beschikbare kennis en feiten.[15]

Het analysekader is ook voor andere doeleinden bruikbaar. Men kan het bijvoorbeeld ook gebruiken voor de analyse van andere ontwikkelingen, zoals de EU-uitbreiding. Verder kunnen nieuw beleid en/of nieuwe wetgeving ermee worden doorgelicht.[16] Ook in die gevallen kan immers sprake zijn van veranderingen in illegale groothandelswaar, groothandelsondernemingen en bedrijfsvoering. Mensensmokkel is bijvoorbeeld voor een (belangrijk?) deel een neveneffect van internationale ontwikkelingen en het asielbeleid. Daarom zou er bij wijzigingen in het asielbeleid expliciet moeten worden gekeken naar de effecten voor mensensmokkel. Hierdoor kan een integrale belangenafweging plaatsvinden tussen de doelen van het asielbeleid en van criminaliteitsbeheersing. Die afweging geeft tevens houvast om er een aanpak voor mensensmokkel van af te leiden. Beheersing van mensensmokkel kan zo mede bijdragen aan de uitvoering van het asielbeleid. Omgekeerd kan men in het asielbeleid dan rekening houden met de belangen die bij criminaliteitsbeheersing in het geding zijn. In dat kader vormt de wisselwerking en/of spanning tussen allerlei beleidsterreinen van de overheid en criminaliteitsbeheersing een interessant thema voor nader onderzoek. Op die wijze ontstaat inzicht in de mate waarin criminaliteitsbeheersing een rol speelt in de besluitvorming binnen de overheid en wie op welke wijze de belangen afweegt. Op basis daarvan kan de overheid een extra dimensie toevoegen aan het streven naar een integraal veiligheidsbeleid.

Ook de analyse van de ICT-ontwikkelingen in hoofdstuk 5 is breder bruikbaar. De bevindingen van de uitgevoerde risicoanalyse beperken zich tot veranderingen in georganiseerde criminaliteit. Hoewel niet onderzocht, bestaat de indruk dat de waarschijnlijkheid van veranderingen in andere criminaliteitsvormen en terrorisme, hoger ligt. Afzonderlijke risicoanalyses zouden hierover uitsluitsel kunnen geven.

Hoewel de dreigingen overwegend als onwaarschijnlijk zijn gekwalificeerd en de effecten als beperkt, betekent dat niet dat er geen preventieve maatregelen nodig zijn. Het feit dat de veranderingen in georganiseerde criminaliteit nog wel mee lijken te vallen, betekent niet dat andere typen criminelen niet met andere criminaliteitsvormen inspelen op de ICT-ontwikkelingen. Alle belanghebbenden hebben er dus baat bij om wel degelijk preventieve maatregelen te treffen tegen bijvoorbeeld diefstal van informatie en misbruik van de virtuele ruimte en de ICT-sector. Bovendien is in de beoordeling van de dreigingen meegewogen dat sociale controle mogelijk is en ook plaatsvindt. Wel geldt over de gehele linie dat vooral andere instanties, niet zijnde opsporingsinstanties, (preventieve) maatregelen zouden moeten treffen. Hoewel in het algemeen de werking van het strafrecht al beperkt is, geldt dat zeker voor de dreigingen die zijn geïdentificeerd.

[15] In paragraaf 1.2.2 is aangegeven waarom een dergelijke evaluatie niet eenvoudig is.
[16] Leppä bepleit om bij de ontwikkeling van nieuwe (internationale) wetgeving expliciet de risico's te analyseren {Leppä, 1999}.

7.4. Strategische risicoanalyse voor criminaliteitsbeheersing

Risico's komen lang niet altijd op basis van een risicoanalyse op de maatschappelijke of politieke agenda. Evenmin komen de in analyses genoemde risico's altijd op de agenda.[17] Dat geldt in het algemeen en zeker ook voor criminaliteitsbeheersing. Meesters en Niemeijer stellen dat de strategische betekenis van criminaliteitsbeelden, een specifieke vorm van strategische analyse, betrekkelijk beperkt is.[18] Ook zogenaamde fenomeen-onderzoeken, tijdelijk populair rond 1994, zijn nauwelijks van de grond gekomen en de bevindingen hebben slechts een beperkte waarde gehad. Dergelijke analyses moeten strijden met andere urgente vraagstukken die zich nu voordoen en nu om actie vragen. Desondanks is de aanname dat een risicoanalyse een nuttige bijdrage kan leveren aan (de agendavorming ten behoeve van) criminaliteitsbeheersing.

Dat een overzicht van en inzicht in criminaliteit een belangrijke bijdrage kunnen leveren, onderkennen korpschefs, leden van het Openbaar Ministerie en dergelijke in toenemende mate. Daarbij komt steeds duidelijker naar voren dat het beschikbare overzicht en inzicht daarvoor niet toereikend zijn. Tot voor enkele jaren geleden werd in dat kader vooral gewezen op de gebrekkige informatiehuishouding van de politie. De politiedepartementen, de Raad van Hoofdcommissarissen, het Hoofdofficierenberaad en de Raad van Korps-beheerders zochten de oplossingen vooral in meer informatie, een betere toegankelijkheid van de gegevens, betere geautomatiseerde functionaliteiten en verbeteringen in de technische infrastructuur. Hoewel men nog steeds hoog opgeeft van deze oplossingsrich-ting, is sinds eind 2000 daarin een kentering waarneembaar.

Eind 2000 is namelijk een stuurgroep geformeerd door de Raad van Hoofdcommissarissen met als taak om een Angelsaksisch sturingsconcept, 'intelligence led policing' genaamd, te vertalen naar de Nederlandse situatie. Intelligence led policing is vooral in Groot-Brittannië, Canada, Australië en de Verenigde Staten al enige jaren in opmars.[19] Door de stuurgroep is het Angelsaksische concept omgedoopt in informatiegestuurde opsporing. Dit concept lijkt beperkter dan intelligence led policing. Toch is dat niet het geval. Om pragmatische redenen is gekozen voor informatie in plaats van intelligence of inlichtin-gen[20] en om het concept vooralsnog te gebruiken voor de opsporingstaak van de politie. De gedachte daarachter is echter gelijk aan die van intelligence led policing. Heden ten dage is het sturingsconcept verbreed tot informatiegestuurde politie.

Anderson typeert intelligence led policing (ILP) als volgt:

> *"At it's most fundamental, ILP involves the collection and analysis of information to produce an intelligence end product designed to inform police decision making at both the tactical and strategic levels. lt is a model of policing in which intelligence serves as a guide to operations, rather than the reverse. lt is innovative, and, by some standards,*

[17] Zie subparagraaf 1.2.3.
[18] {Meesters & Niemeijer, 2000}.
[19] {Stuurgroep Informatie gestuurde opsporing, 2001B}
[20] Het Angelsaksische begrip intelligence heeft een rijkere betekenis dan het Nederlandse woord inlichtingen. Volgens de Concise Oxford Dictionary is de definitie van intelligence: "the sum of what is known, integrated with new information and interpreted for meaning" {McDowell, 1996}. Intelligence is eveneens een ruimer begrip dan informatie.

even radical, but is predicated on the notion that a principal task of the police is to prevent and detect crime than simply to react to it."[21]

Informatie, criminaliteitsanalyse en toegepast wetenschappelijk onderzoek, samen resulterend in overzicht en inzicht, spelen dus een cruciale rol in het concept van intelligence led policing en informatiegestuurde opsporing. Besluitvorming moet daarop zijn gebaseerd. Centraal staat ook dat overzicht en inzicht niet vanzelf totstandkomen, maar expliciete besluitvorming en aansturing vereisen. Wanneer men bijvoorbeeld aan kinderporno hoge prioriteit toekent, terwijl daarover nog weinig informatie beschikbaar is, moet de politie niet wachten totdat die informatie naar boven komt. Zij moet daarin dan gericht investeren. Voor bijvoorbeeld informantenrunners heeft dat als consequentie dat zij op zoek moeten naar informanten die wat weten over kinderporno. Een ander element van het sturingsconcept is dat expliciete besluitvorming vooraf gaat aan operationele activiteiten. Nog een ander element is dat de operationele activiteiten, waaronder opsporingsonderzoeken, ook moeten bijdragen aan overzicht en inzicht in criminaliteit. Met andere woorden, informatiegestuurde opsporing beoogt om samenhang te creëren tussen de opbouw van overzicht en inzicht in criminaliteit en het beleidsproces (inclusief opsporing).

Hoewel informatiegestuurde opsporing op menig verjaardag uit te leggen valt, blijkt vanuit de Angelsaksische praktijk dat het gaat om een fundamentele verandering. Volgens de stuurgroep die het concept in Nederland heeft geïntroduceerd, gaat het om veranderingen in leiderschap, cultuur en analyse.[22] Veranderingen zijn echter niet alleen nodig binnen de politie, maar ook bij het Openbaar Ministerie, bestuurders, politiedepartementen en politici.[23] Het Openbaar Ministerie moet strategische keuzen leidend laten zijn bij de keuze van opsporingsonderzoeken[24] evenals bij keuzen binnen het opsporingsonderzoek[25]. Daarbij kunnen andere instrumenten de voorrang krijgen boven het strafrechtelijke instrument. Voor bestuurders en de politiedepartementen geldt hetzelfde. De politie-beleidsplannen evenals de prestatiecontracten zouden moeten zijn gestoeld op overzicht en inzicht in criminaliteit en op duidelijke keuzen. En het in de praktijk wel gehoorde verwijt dat politici op basis van krantenberichten de prioriteiten voor de recherche bepalen, zou dan ook tot het verleden moeten horen.

De verwachtingen over informatiegestuurde opsporing zijn hooggespannen en de ervaringen ermee in het buitenland hoopgevend. Toch is het concept (nog) niet weten-schappelijk onderbouwd en getoetst. Bestaande wetenschappelijke kennis zou kunnen worden benut om de belangrijkste aannames te toetsen en eventueel te verbeteren. Gedacht kan worden aan kennis over beleids-, besturings-, besluitvormings- en informatieprocessen en over criminaliteit(sbeheersing). Wetenschappelijk onderzoek zou ook kunnen bijdragen aan het evalueren van de effecten van informatiegestuurde opsporing. Nederland staat nog aan de vooravond van de invoering ervan. Daarom is het een geschikt moment om nu het concept als wetenschappelijk studieobject te benoemen.

---

[21] {Anderson, 1997}.
[22] {Stuurgroep Informatie gestuurde opsporing, 2001A}.
[23] Beheersing van criminaliteit kan immers alleen in samenwerking met anderen. Bovendien bepaalt in formele zin niet de politie het beleid, de prioriteiten en de strategieën. Dit is voorbehouden aan de Korpsbeheerder en de Hoofdofficier van justitie en de departementen van BZK en Justitie.
[24] In informatiegestuurde opsporing aangeduid als tactische sturing.
[25] In informatiegestuurde opsporing aangeduid als operationele sturing.

Een element van het concept is de aanwezigheid van een orgaan op nationaal niveau dat zich bezighoudt met strategische sturing. Dit orgaan moet opdracht geven tot het uitvoeren van (strategische) risicoanalyses op nationaal niveau en fungeert daarmee als opdrachtgever. Deze rol is cruciaal voor de afbakening en diepgang van de analyse. Zo komen vele ontwikkelingen in aanmerking voor een risicoanalyse. Bovendien bestrijken illegale groothandelsactiviteiten vele soorten illegale producten, typen groothandelsondernemingen, aspecten van de bedrijfsvoering, soorten belangen die in het geding zijn et cetera. De onderzoekscapaciteit is daarentegen schaars. Betrokkenheid van de opdrachtgever is niet alleen van belang om die keuzen te maken, maar ook om zich bewust te worden van de materie. Daardoor is de kans groter dat hij uiteindelijk het eindproduct gebruikt in het beleidsproces of als ambassadeur van het eindproduct gaat optreden. Dit bevordert de aansluiting tussen risicoanalyse en criminaliteitsbeheersing.

In Nederland bestaat echter geen nationaal strategisch sturingsorgaan. Het Openbaar Ministerie claimt weliswaar de opdrachtgeverrol, maar hanteert vooral een strafrechtelijke invalshoek. Deze invalshoek past in elk geval niet goed bij strategische analyses ten behoeve van vroegtijdige criminaliteitsbeheersing. Immers, het strafrecht is slechts een beperkt en vooral reactief en repressief instrument. De politieministers claimen deze opdrachtgeverrol (nog) niet. Zij fungeren eerder als consument van (risico)analyseproducten dan als opdrachtgever. De Raad van Hoofdcommissarissen, een periodiek overlegorgaan van de korpschefs van de zesentwintig politieregio's, treedt slechts zelden op als opdrachtgever. Hetzelfde geldt voor de Raad van Korpsbeheerders, een periodiek overlegorgaan van de korpsbeheerders van de zesentwintig politieregio's. Strategische risicoanalyses op landelijk niveau ontberen daarom een vanzelfsprekende opdrachtgever en als gevolg daarvan ook een vanzelfsprekende afnemer. Daardoor spelen de eindproducten lang niet altijd een rol in het beleidsproces. Een nationaal sturingsorgaan zou het rendement van strategische risicoanalyses op landelijk niveau sterk kunnen verhogen.[26]

Informatiegestuurde opsporing kent een groot belang toe aan criminaliteitsanalyse en (toegepast) wetenschappelijk onderzoek. Daarvoor moeten wel enkele nieuwe analyseproducten worden ontwikkeld.[27] Dit proefschrift heeft er slechts één daarvan ontwikkeld en daar kleven nog beperkingen aan.[28] Bovendien is het analysekader alleen nog geschikt voor georganiseerde criminaliteit. Voor andere criminaliteitsvelden en andere veiligheidsterreinen is een afzonderlijk analysekader wenselijk evenals een normatief kader.[29] Verder zal vooral de onderbouwing van de waarschijnlijkheid problematisch blijven zolang er geen verklarende en voorspellende theorieën beschikbaar zijn.

Hoewel informatiegestuurde opsporing dus kan zorgdragen dat de samenhang tussen strategische risicoanalyses en agenda- en beleidsvorming toeneemt, is nog een lange weg te gaan. De politie moet het concept nog verder implementeren. De informatiehuishouding van de politie kan en moet verbeteren. Aanvullende analyseproducten moeten worden ontwikkeld om de beschikbare informatie en kennis te ontginnen. De beleidsmakers en

[26] Er is niet beoogd om het politiebestel ter discussie te stellen. Binnen de bestaande structuur kan een dergelijk nationaal strategisch sturingsorgaan worden vorm gegeven.
[27] Zie voor een overzicht van benodigde analyseproducten {NCIS, 2000A}.
[28] Zie de voorgaande paragraaf waarin enkele aanbevelingen zijn geformuleerd.
[29] De wenselijkheid van een normatief kader is beschreven in paragraaf 7.3.

besluitvormers moeten hun beleid en besluiten meer dan nu baseren op (risico)analyses en duidelijker formuleren aan welke informatie behoefte is en daarop sturen. Risico's zullen daarom de komende jaren nog niet altijd dankzij risicoanalyses op de agenda komen, of ze zullen ondanks een risicoanalyse niet op de agenda komen. Wanneer het concept daadwerkelijk is ingevoerd, mogen we echter aannemen dat strategische risicoanalyses een grotere rol spelen tijdens de agenda- en beleidsvorming en dat het belang dat men er aan hecht, verder toeneemt.

Een positieve ontwikkeling heeft zich recent voorgedaan. In het kader van een landelijk project om te komen tot een bovenregionale en nationale recherche is de behoefte ontstaan aan een Nationaal Dreigingsbeeld zware of georganiseerde criminaliteit. Nadat dit dreigingsbeeld in augustus 2004 is aangeboden, heeft zowel het OM als de politie zich hierover gebogen en (grotendeels) op basis daarvan prioriteiten voorgesteld evenals beleidsmaatregelen. De politieministers hebben het Nationaal Dreigingsbeeld en de voorgestelde prioriteiten en beleidsmaatregelen omgezet in tal van beleidsvoornemens en eind 2004 aangeboden aan de Tweede Kamer. Eén van de voornemens is dat de politietop, in nauwe samenwerking met het OM, sterker dan nu gaat sturen op strategische criminaliteitsanalyses en het inlichtingenproces. Daarmee is dus sprake van informatiegestuurde opsporing. Ook de politietop roept op tot het ontwikkelen van een normatief kader voor strategische besluitvorming en tot een studie naar één landelijk sturingsorgaan. De politieministers staan hier niet onwelwillend tegenover.[30]

7.5. Tot slot

De toepassing van het risicoanalyse-instrumentarium op de ICT-ontwikkelingen heeft er toe geleid dat dreigingen zijn geïdentificeerd en beoordeeld. Op basis van dat beeld kunnen de belanghebbenden bepalen in hoeverre de risico's op de agenda van criminaliteitsbeheersing moeten worden geplaatst of dat aanvullend onderzoek wenselijk is. Daarmee heeft de toepassing van risicoanalyse voor (vroegtijdige) criminaliteits-beheersing een toegevoegde waarde en past het goed in het sturingsconcept informatiegestuurde opsporing.

Het concept van georganiseerde criminaliteit als stelsel van illegale groothandelsondernemingen is bruikbaar gebleken. Het concept is echter nog niet bediscussieerd in wetenschappelijke fora en bij de beleidsmakers en de aannames zijn nog niet empirisch getoetst. Het concept werpt wel, zoals eerder is aangegeven, een ander licht op de samenhang met en de afbakening ten opzichte van andere vormen van criminaliteit. Dat roept achteraf wel de vraag op in hoeverre de risicoanalyse zich niet beter breder had kunnen richten op veranderingen in misdaadmarkten. Ook dan zou overigens de rol van illegale groothandelsondernemingen aan bod zijn gekomen, maar daarnaast ook de rollen van de detailhandel, producenten en consumenten. Die bredere invalshoek zou de analyse uiteraard wel veel omvangrijker en complexer hebben gemaakt.

[30] De beleidsvoornemens van de politieministers alsmede de verwijzing naar de beleidsdocumenten van de Raad van Hoofdcommissarissen en van het College van Procureurs-Generaal, zijn verwoord in een brief van het Ministerie van Justitie, Directoraat-Generaal Rechtshandhaving aan de Tweede kamer (kenmerk 5318234/504 van 22 november 2004). Deze nabeschouwing was reeds geschreven voordat de beleidsdocumenten totstandkwamen.

Het analysekader is eveneens bruikbaar geweest en is breder toepasbaar. Ook voor andere ontwikkelingen en nieuw overheidsbeleid kan immers worden geanalyseerd in hoeverre veranderingen in illegale groothandelswaar, groothandelsondernemingen en bedrijfsvoering zijn te verwachten. Er kleven echter ook enkele belangrijke nadelen aan het kader. Zo zijn de risicofactoren niet empirisch getoetst, waardoor de beoordeling van de waarschijnlijkheid kwetsbaar is. Een normatief en gezaghebbend kader voor de beoordeling van ongewenste effecten is niet opgenomen. Instrumenten ontbreken nog voor de identificatie en de selectie van dreigingen en voor de vertaling van ontwikkelingen naar de toekomst. Verder is het risicoanalyse-instrumentarium niet zomaar toepasbaar voor andere criminaliteitsvormen, terrorisme en openbare orde-vraagstukken. Om deze beperkingen teniet te doen, is aanvullend onderzoek en zijn aanvullende uitwerkingen vereist. Verklarende en voorspellende criminologische theorieën zouden een belangrijke katalysator vormen voor de verbetering van het kader. Zoals eerder is aangegeven, zijn deze zeldzaam, belichten ze een smal gebied en zijn ze merendeels ontworpen voor andere vormen van criminaliteit.[31]

In dit proefschrift zijn enkele discussiepunten benoemd. Voorbeelden daarvan zijn de vraag wat nu zo erg is aan georganiseerde criminaliteit in termen van ongewenste effecten en in welke mate welke partijen een rol moeten spelen bij criminaliteitsbeheersing. Het proefschrift creëert ook een behoefte aan nader wetenschappelijk onderzoek. Onderzoeksonderwerpen die in deze nabeschouwing zijn genoemd zijn:

- het concept van illegale groothandelsondernemingen;
- het concept van misdaadmarktgerichte criminaliteit;
- de intentie van illegale groothandelaren;
- de relatie tussen typen ontwikkelingen in de samenleving en de veranderingen in georganiseerde criminaliteit die daaruit voortkomen;
- de relatie tussen soorten veranderingen en ongewenste effecten;
- de validiteit van de benoemde risicofactoren;
- de consequenties van de ICT-ontwikkelingen voor andere criminaliteitsvormen en terrorisme;
- de rol van criminaliteitsanalyses bij criminaliteitsbeheersing;
- de wisselwerking en/of spanning tussen allerlei beleidsterreinen van de overheid en criminaliteitsbeheersing;
- het concept van informatiegestuurde opsporing en het effect daarvan op de criminaliteitsbeheersing.

Hoewel dit proefschrift dus antwoorden heeft gevonden op de gestelde vragen, levert het ook de nodige discussiestof op en onderwerpen voor nader wetenschappelijk onderzoek en een verdere uitwerking.

[31] Zie subparagraaf 1.2.2.

Summary

Risk analysis of organised crime

Creation of a toolbox and its application in the area of ICT developments

1. Introduction

Developments in society may bring about changes in organised crime, which in turn may have undesired effects. The sooner the police and other authorities implement measures or prepare themselves to combat these changes, the more effective they will prove. Insight into these changes, the probability and undesired effects of them are preconditions for this early form of crime control. The risk analysis toolbox is suitable for this task, but requires further elaboration.

This thesis comprises two components. The first is a toolbox for risk analysis. This toolbox is primarily intended to furnish insight to enable the timely control of organised crime. The second component is an analysis of the risks of changes occurring in organised crime as a consequence of information & communications technology (ICT) developments (see Figure S.1). The underlying objective is to gain experience of the application of the toolbox. The definition of the problem is as follows:

1. How might one analyse the risks of changes occurring in organised crime as a consequence of developments within society?
2. What are the risks of changes in organised crime ensuing from ICT developments?

Component		Part		Element	
1	Risk analysis toolbox	1.1	Risk analysis for the timely control of organised crime		
		1.2	Conceptual model of organised crime		
		1.3	Framework for analysis of organised crime	1.3.1	Typology of changes
				1.3.2	Risk factors for probability assessment
				1.3.3	Basic principles for the assessment of undesired effects and description of some effects
2	Risk analysis of changes in organised crime as a result of ICT developments	2.1	Analysis of ICT developments		
		2.2	Identified threats and their assessment		

Figure S.1 Structure of the thesis

2. Risk analysis toolbox

The toolbox developed consists of three parts. The *first* part concerns the elaboration of risk analysis for timely crime control. Risk analysis is a specialised form of policy and crime analysis. Three components of a risk are identified, namely threat, probability and undesired effects.

The *second* part conceptualises the term 'organised crime'. The definition is as follows:

> *Organised crime is the execution of illicit wholesale activities in one or more criminal markets by an illicit wholesale enterprise.*

Illicit wholesale enterprises exist to earn money from the trade in illicit products. A wholesaler does not manufacture products itself, nor does it sell to end users. In addition to buying and selling, the wholesale enterprise may focus on the sorting, storage, transportation and financing of the products. Other functions may be the taking of risks for the suppliers and customers and accumulating market data. These are its core business. The core business requires support activities, such as forging identity documents and protection activities. The core and support activities are collectively called 'illicit wholesaling operations'. These result in the involvement of suppliers, customers and supporters. Although this involvement is instrumental, it does not constitute part of the illicit wholesale activities. The trade in illicit products occurs in criminal markets, where a wide range of parties operates.

The third part is an analysis framework for converting developments in society into changes in organised crime and assessing the probability and undesired effects of the changes. One underlying assumption is that the opportunity theory will prove suitable for this purpose. A development in society may, after all, influence one or more opportunity factors and thus bring about a change in organised crime. The degree of influence exerted determines the probability thereof. Opportunity factors for organised crime are: illicit wholesale merchandise, illicit wholesale enterprise, social control and location. Three relevant sorts of changes have been identified, namely in illicit wholesale merchandise, wholesale enterprises and business operations. This typology enables us to closely examine a development and identify threats. Risk factors have also been specified with a view to assessing probability. These were derived from the opportunity factors. Basic analytical principles have been specified for the assessment of the undesired effects. A few of the undesired effects have been described on the basis of the policy documents and literature studied.

3. Risks of changes occurring in organised crime as a consequence of ICT developments

During the past few years, ICT has developed rapidly. This has invariably involved an interaction between ICT innovation and all sorts of societal changes, collectively referred to as 'ICT developments'. These have four, partially overlapping characteristics. The first is that ICT is a major consumer & capital good. A secondary, contributory, characteristic is that information is a major consumer good and an important production factor. A third

characteristic is the existence of virtual space as a result of the global interfacing of networks. And finally, the fourth characteristic is the emergence of the ICT sector and ICT experts. For the legal business community, ICT developments have led to innovation, increased flexibility and reduced transaction costs. Furthermore, they have an influence on mutual competition while reducing the disadvantages of network organisations. This can bring about increased productivity and strengthen the competitiveness of individual businesses, but it may also lead to a reduction in the overall profitability of the business sector. These changes for the legal business community are subject to compliance with a number of preconditions, which is not always the case as yet. Moreover, besides offering countless opportunities, ICT, information and virtual space also have their limitations and also raise quite a number of issues for social control.

The application of the framework for analysis in combination with the aforementioned characteristics results in seven threats (see Figure S.2).

1. Illicit ICT as wholesale merchandise
2. Utilisation of ICT in illicit business operations
3. Illicit information as wholesale merchandise
4. Increasing use of information in illicit business operations
5. Virtual illicit wholesale enterprises
6. Conversion from conventional to virtual illicit business operations
7. Abuse of the ICT sector & experts for illicit business operations

Figure S.2 List of identified threats

In contrast to the legitimate business community, innovation, increased flexibility and reduced transaction costs are unlikely to occur in criminal markets and enterprises. Nor are they inclined to experience increased productivity and competitiveness. The main reasons for this lie in the characteristics of criminal markets, the bottlenecks encountered in operating illicitly, the lack of incentives to make (innovative) changes, failure to meet the preconditions for innovation and the profiles of criminal entrepreneurs. The threat of 'illicit ICT as wholesale merchandise' was the only one to be considered a real possibility, while the others were regarded unlikely. Apart from those listed above, the main reasons for this conclusion are that the forms of illicit information and copied software are not a suitable wholesale commodity and that the disadvantages of illicit business operations far outweigh the benefits to be gained. The virtual space is at the same time not a suitable market place for illicit products. A few exceptions to the rule were nevertheless identified, which entail a higher degree of probability at a lower level of abstraction. This applies to: a) the utilisation of ICT for communications, administration and protection, b) stolen and counterfeited physical audio and video as wholesale merchandise, c) the use of the virtual space as source of information, d) the conversion to virtual illicit business operations for the purpose of communication and e) the unconscious involvement by the ICT sector & experts. A few aspects were also listed, which require further attention, in the form of a risk analysis for instance.

The general impression is that ICT developments hardly, if at all, lead to changes in illicit wholesale merchandise, wholesale enterprises and their business operations. Were the

changes to become manifest, however, the undesired effects would be relatively innocuous. After all, at the heart of the matter, the differences between illicit ICT and information and conventional merchandise are not so significant that they would cause other undesired effects. Nor, on the other hand, are the undesired effects of a virtual illicit wholesale enterprise significantly different to those of a conventional one. Neither do innovations in business operations lead to significant operational changes nor in fact to different undesired effects.

4. Experience gained in the application of the toolbox

The concept of organised crime as a system of illicit wholesale enterprises and the framework for analysis, which are two crucial parts of the toolbox developed, can be used to perform a risk analysis. The framework for analysis forces one to pose the question what sorts of changes are likely to ensue from each characteristic of a development. This greatly benefits the precision and completeness of the study, while also providing a guideline for the definition of the level of abstraction. The established risk factors call for explicit arguments, as does the framework for the assessment of the undesired effects. The framework for analysis is also more broadly applicable to other developments taking place in society and, for instance, for the assessment of new government policy in terms of the consequences for crime control. The experience gained in applying the toolbox to the ICT developments has therefore proved beneficial.

The toolbox does have its limitations, however. Additional research and further elaboration is therefore required to alleviate these limitations. A few suggestions for improvements have been formulated. Several subjects have also been identified as suitable for further scientific research and discussion.

Literatuur

Adamoli, S., Nicola, A., Savona, E.U. & Zoffi, P., *Organised crime around the world*, Helsinki, European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI), 1998

Albanese, J.S., 'The prediction and control of organized crime: risk assessment', *Crime & Justice International*, 18 (2002), 60 (march), pp 9-10, 26-27

Albrecht, H.J. & Kilchling, M., 'Crime Risk Assessment, Legislation, and the Prevention of Serious Crime – Comparative Perspectives', *European journal of crime, criminal law and criminal justice*, 10 (2002), 1, pp 23-38

Anderson, R., 'Intelligence Led Policing: a British Perspective', in *Intelligence Led Policing. International Perspectives on Policing in the 21st Century*, Lauwerenceville, IALEIA, 1997, pp 5-9

Anker, M.J.J. van den & Hoogenboom, A.B., *Schijn bedriegt. Overheid, bedrijfsleven en gelegenheidsstructuren voor milieucriminaliteit op de hergebruikmarkt*, 's-Gravenhage, VUGA uitgeverij B.V., 1997

Anker, M.J.J. van den, *Wie betaalt, bepaalt. Over intermediaire organisaties, milieucriminaliteit, organisatiecriminaliteit en integriteit in het complexe milieuveld*, Den Haag, Elsevier bedrijfsinformatie, 1999

Arlacchi, P., 'Some observations on Illegal Markets', in Ruggiero, V., South, N. & Taylor, I (ed.), *The New European Criminology. Crime and Social Order in Europe*, London, Routledge, 1998, pp. 203-215

Baarda, D.B., Goede, M.P. de & Teunissen, T., *Kwalitatief Onderzoek. Praktische handleiding voor het opzetten en uitvoeren van onderzoek*, 1e druk 4e oplage, Houten, Stenfert Kroese, 1997

Bartelsman, E. & Hinloopen, J., 'De verzilvering van een groeibelofte', in Soete, L., (red.) *ICT en de nieuwe economie. Preadviezen van de Koninklijke Vereniging voor de Staathuishoudkunde 2000*, Utrecht, Lemma BV, 2000, pp. 61-81

Black, C., Beken, T. van der & Ruyver, B. de, *Measuring Organised Crime in Belgium. A Risk-Based Methodology*, Antwerpen-Apeldoorn, Maklu, 2000

Boni, W.C. & Kovacich, G.L., *I-Way Robbery: Crime on the Internet*, Boston, Butterworth Heinemann, 1999

Bovenkerk, F., Bruinsma, G.J.N., Bunt, H.G. van de & Fijnaut, C.J.C.F., 'Discussie. Georganiseerde criminaliteit in Nederland: reactie op de commentaren', *Tijdschrift Voor Criminologie,* 39 (1997), 1, pp. 56-66

Bovenkerk, F., *Misdaadprofielen*, Amsterdam, Meulenhoff BV, 2001

Brink, Tj. ten & Leest, W. van der, *Risicoanalyse & scenariostudie. Projectvoorstel en uitwerkingen*, (concept) 9 september 2002 (interne notitie KLPD)

Bruinsma, G.J.N., *Beelden van criminaliteit*, Deventer, Gouda Quint BV, 1996

Bruinsma, G.J.N., Bunt, H.G. van de & Marshall, I.H., *Met het oog op de toekomst. Verkenning naar de kennisvragen over misdaad en misdaadbestrijding in 2010*, Rotterdam, 2001 (studie van de Adviesraad voor Wetenschaps- en Technologiebeleid) (www.awt.nl)

Bruning, F., 'Risicobeheersing is geen Russisch roulette', in Oelen, U.H. & Struiksma, N., *Puzzelen met beleid. Ontwikkelingen in de beleidsanalyse*, Alphen aan den Rijn, Samsom H.D. Tjeenk Willink, 1994, pp 45-54

Bryson, J.M., *Strategic planning for public and nonprofit organizations*, San Francisco, Jossey-Bass Publishers, 1995

Bunt, H.G. van de, 'Beleid uit wetenschap', *Justitiële verkenningen*, 25 (1999), 6 (augustus), pp. 13-21

Bunt, H. van de, Berg, E. van den & Kleemans, E., 'Georganiseerde criminaliteit en het opsporingsapparaat: een wapenwedloop?', *Tijdschrift voor Criminologie*, 1999, 4, pp. 395-408

Cachet, L. & Sluis, A. van, 'Van geprogrammeerde naar anticiperende veiligheidszorg', in Lehning, P.B. (red.), *De beleidsagenda 2000. Strijdpunten op het breukvlak van twee eeuwen*, Bussum, Uitgeverij Coutinho, 2000, pp. 160-177

Castells, M., *The Rise of the Network Society. Volume 1 of the Information Age*, Blackwell Publishers Inc., 1998

Castells, M., *The Information Age: Economy, Society and Culture. Volume III End of Millennium*, Blackwell Publishers Inc., 1998

Castells, M., *The Internet Galaxy. Reflections on the Internet, Business, and Society*, Oxford, Oxford University Press, 2001

Chang, D.H., 'Organized crime forms in the world. Can we win against organized crime?', *Eurocriminology*, 12 (1998), pp. 3-24

Clarke, R.V. & Felson, M., 'Introduction: Criminology, Routine Activity, and Rational Choice', in Clarke, R.V. & Felson, M.(ed.), *Routine Activity, and Rational Choice*, New Brunswick (etc.), Transaction Publishers, 1993, pp. 1-14

Cohen, L.E. & Felson, M., 'Social Change and Crime Rate Trends: A Routine Activity Approach', *American Sociological Review*, 1979, 44 (august), pp. 588-608

Commissie ICT en Overheid, *Burger en overheid in de informatiesamenleving. De noodzaak van institutionele innovatie*, 6 september 2001 (download van www.minbzk.nl)

Commission of the European Communities, *Commission staff working paper. Joint report from commission services and EUROPOL, 'Towards a European strategy to prevent organised crime'*, Brussels, 2001 (SEC (2001) 433)

Contract met de toekomst. Een visie op de elektronische relatie overheid-burger, 19 mei 2000 (via Internet)

Cops@Cyberspace, 5(2001), 18

Criminaliteitsbeheersing. Investeren in een zichtbare overheid, 2001 (download van internet)

De bestuurlijke aanpak van de (georganiseerde criminaliteit) in Amsterdam. De ontwikkeling van een effectief instrumentarium. Raadsvoordracht (boek 1)

Dienst Nationale Recherche Informatie Korps Landelijke politiediensten, *Nationaal Dreigingsbeeld zware of georganiseerde criminaliteit. Een eerste proeve*, Zoetermeer, KLPD Dienst Nationale Recherche Informatie, 2004

Dijk, J.J.M. van, 'De georganiseerde misdaad volgens Fijnaut', *Bestuurskunde*, 5 (1996), 2, pp. 77-80

Dijk, J.J.M. van, Sagel-Grande, H.I. & Toornvliet, L.G., *Actuele Criminologie*, 2e herz. druk, Lelystad, Koninklijke Vermande, 1996

Dijk, Th. van, Elffers, H., Hessing, D.J. & Hoogenboom, A.B., *Bewust van de gevaren van criminaliteit. Een inventarisatie van kwetsbaarheden, die in de logistieke keten en daarmee ook in de Rotterdamse haven voorkomen*, Gouda Quint, 1999

Duin, M.J. van, 'Omgaan met risico's en risico-analyse' in Oelen, U.H. & Struiksma, N., *Puzzelen met beleid. Ontwikkelingen in de beleidsanalyse*, Alphen aan den Rijn, Samsom H.D. Tjeenk Willink, 1994, pp 55-61

Dunn, W.N., *Public Policy Analysis. An introduction*, 2nd edition, Prentice Hall, Englewood Cliffs New Jersey, 1994

Duyne, P.C. van, Kouwenberg, R. & Romeyn, G., *Misdaadondernemingen. Ondernemende misdadigers in Nederland*, Den Haag, Gouda Quint, 1990

Duyne, P.C. van, 'Organized crime markets in a turbulent Europe', *European Journal On Criminal Policy and Research,* 1 (1993), 3, pp. 11-30

Duyne, P.C. van, *Het spook en de dreiging van de georganiseerde misdaad*, Den Haag, SDU uitgeverij, 1995

Duyne, P.C. van, 'Definitie en kompaswerking', in: Bovenkerk, F. (red.), *De georganiseerde criminaliteit in Nederland. Het criminologisch onderzoek voor de parlementaire enquêtecommissie opsporingsmethoden in discussie*, Deventer, Gouda Quint BV, 1996, pp 47-60

Duyne, P.C. van, Pheijffer, M., Kuijl, H.G., Dijk, Th.H. van & Bakker, J.C.M., 'Financial investigation of crime. A tool of the integral law enforcement approach', Koninklijke Vermande, 2001

Eerenbeemt, M. van den, 'De bovenwereld als onderwereld', *Volkskrant*, 7-5-1998

Enquêtecommissie Opsporingsmethoden, *Inzake opsporing, Eindrapport*, 's-Gravenhage, Sdu Uitgevers, 1996

Enquêtecommissie Opsporingsmethoden, *Inzake opsporing, Bijlage VII: Eindrapport onderzoeksgroep Fijnaut*, 's-Gravenhage, Sdu Uitgevers, 1996

Enquêtecommissie Opsporingsmethoden, *Inzake opsporing, Bijlage II: Verhoren, deel I*, 's-Gravenhage, Sdu Uitgevers, 1996

Enquêtecommissie Opsporingsmethoden, *Inzake opsporing, Bijlage X: deelonderzoek III onderzoeksgroep Fijnaut: De georganiseerde criminaliteit in Nederland: De vrije-beroepsbeoefenaars: advocaten, notarissen, accountants; Fraude en witwassen*, 's-Gravenhage, Sdu Uitgevers, 1996

Ericson, R.V. & Haggerty, K.D., *Policing the risk society*, Oxford, Clarendon Press, 1997

Felson, M & Rutgers, Ph.D, 'Routine activity theory: The theorist's perspective' in Adler, P., Adler, P.A. & Bryant, C.D. (Red.), Encyclopedia of criminology and deviant behavior. Volume I: Historical, conceptional, and theoretical issues, Philadelphia, PA, Brunner-Routledge, 2001, pp 338-339

Fijnaut, C.J.C.F., 'De ernst van de georganiseerde criminaliteit en de regulering van de bijzondere opsporingsmethoden', *Trema,* 18 (1996), special, pp. 80-83

Fijnaut, C.J.C.F., 'Over de opzet, de uitvoering en de resultaten van het onderzoek', in: Bovenkerk, F. (red.), *De georganiseerde criminaliteit in Nederland. Het criminologisch onderzoek voor de parlementaire enquêtecommissie opsporingsmethoden in discussie*, Deventer, Gouda Quint BV, 1996, pp. 17-24

Frei, D. & Ruloff, D., *Handbook of Foreign Policy Analysis. Methods for practical application in foreign policy planning, strategic planning and business risk assessment*, Dordrecht, Martinus Nijhoff Publishers, 1989

Frissen, P.H.A., 'Wat werkt moet blijken; sturing onder complexe condities', *Justitiële verkenningen*, 25 (1999), 6 (augustus), pp. 32-40

Galeotti, M, 'The new world of organised crime', *Jane's intelligence review*, 12 (2000), 9 (sept.), pp. 47-52

Galeotti, M(ickey)., 'Cybercrime. America bytes back', *CROSS BORDER CONTROL,* 2000, 14, pp. 13-14

Gartner, *White Paper. The Internet Economy in Europe- from Revolution to Evolution*, 2000 (www.cisco.com/go/gartner)

Geerts, R. W. M. & Boekhoorn, P.F.M., *Criminaliteitsbeheersing De wenselijkheid van publiek private samenwerking*, Arnhem, Gouda Quint BV, 1990

Gerstner, L., speech van CEO van IBM, 1999

Hajer, M. & Schwarz, M., 'Inleiding. Contouren van de risicomaatschappij', in Beck, U., *De wereld als risicomaatschappij: essays over de ecologische crisis en de politiek van de vooruitgang*, Amsterdam, De Balie, 1997, pp. 7-22

Hall, R., *Presentation tot the second International Conference for Criminal Intelligence Analysts*, London, march, 1999

Haller, M.H., 'Illegal enterprise: a theoretical and historical interpretation', *Criminology*, Volume 28 (1990), 2, pp. 207-253

Halstead, B., 'The use of models in the analysis of organized crime and development of policy', T*ransnational Organized Crime,* 4 (1998), 1, pp. 1-24

Hart, P. 't, 'Mogelijkheden van crisisanticipatie: de strategische veiligheidsanalyse'. In Rosenthal, U., Boin, A, Kleiboer, M. & Otten, M. (red.), *Crisis. Oorzaken, gevolgen, kansen*, Alphen aan den Rijn, Samsom, 1998, pp. 185-202

Hauber, A., 'Situationele en individuele preventie', in Lissenberg, E., Ruller, S. van, Swaaningen, R. van (Red.), *Tegen de regels IV. Een inleiding in de criminologie*, Nijmegen, Ars Aequi Libri, 2001, pp. 325-341

Heffen, O. van, 'Beleidsontwerpen en omgevingsfactoren: vier alternatieve strategieën', in Heffen, O. van & Twist, M.J.W. van, *Beleid en wetenschap. Hedendaagse bestuurskundige beschouwingen*, Alphen aan den Rijn, Samsom H.D. Tjeenk Willink, 1993, pp. 67-81

Heijden, T. van der, 'Wereldwijde aanpak georganiseerde misdaad', *Modus*, 9, 5/6 (december 2000), pp. 17-19

Herings, J.J. & Schinkel, M.P., 'Word-Wide-Welfare. Een micro-economische analyse van de nieuwe economie', in Soete, L., (red.) *ICT en de nieuwe economie. Preadviezen van de Koninklijke Vereniging voor de Staathuishoudkunde 2000*, Utrecht, Lemma BV, 2000, pp. 137-175

Hogwood, B.W. & Gunn, L.A., *Policy Analysis for the Real World*, Oxford, Oxford University Press, 1988

Holthuis, H.A., 'Op weg naar een deugdelijke criminele politiek', in: Bovenkerk, F. (red.), *De georganiseerde criminaliteit in Nederland. Het criminologisch onderzoek voor de parlementaire enquêtecommissie opsporingsmethoden in discussie*, Deventer, Gouda Quint BV, 1996, pp. 113-121

Hond, M., de, *Dankzij de snelheid van het licht versie 2.0. Over de grote gevolgen van internet voor burger, bedrijfsleven en overheid*, zesde druk, Utrecht, Het Spectrum B.V., 1997

Hoogenboom, A.B., *Schaduwen over Van Traa*, Lelystad, Koninklijke Vermande, 2000

Hoogenboom, A.B., *'t Neemt toe, men weet niet hoe. Scenariostudie financieel-economische criminaliteit in 2010*, Koninklijke Vermande, 2001

Hughes-Wilson, C.J., *Military Intelligence Blunders*, New York, Caroll & Graf Publishers, Inc., 1999

Huigen, J., 'De mythe van het informatietekort: bestuurscentrisme, bureaupolitisme en bureaucratisme', in Heffen, O. van & Twist, M.J.W. van, *Beleid en wetenschap. Hedendaagse bestuurskundige beschouwingen*, Alphen aan den Rijn, Samsom H.D. Tjeenk Willink, 1993, pp. 217-228

Huisman, W. & Niemeijer, E., *Zicht op organisatiecriminaliteit. Een literatuuronderzoek*, Den Haag, Sdu Uitgevers, 1998

Husken, M., *Charles Z. Ex-autocoureur en drugsbaron*, Amsterdam, Meulenhoff, 2001

Infodrome, *Instituties onder druk. De uitdaging van de informatiesamenleving voor politiek en beleid*, Amsterdam, 2000

Infodrome, *Controle geven of nemen; een politieke agenda voor de informatiesamenleving*, 12 december 2001 (download van www.infodrome.nl)

Integraal Veiligheidsprogramma, juni 1999 (download van het internet)

Jägers, H.P.M., Heijnsdijk, J & Steenbakkers, G.C.A., 'De invloed van informatietechnologie op de organisatiegrenzen: IT bezien vanuit de transactiekostentheorie', *Management & Informatie*, 1997, maart, pp. 18-27

Jackson, J.L. & Herbrink, J.C.M., *Profiling organised crime: the current state of the art*, Leiden, NSCR, 1996

James, L. & Cooper, J., 'Organised exploitation of the information super-highway', *Jane's intelligence review*, 12 (2000), 7 (July), pp. 52-54

Jansonius, A.W. & Kuiper, J., *Referentiekader resultaten politiewerk*, Den Haag, Ministerie van Binnenlandse Zaken; Inspectie Politie, 1997

Janssen, J.W.H.& Haans, H., *Winkelen via Internet. Winkelen langs de elektronische snelweg*, (editie 1997), Hoofdbedrijfschap Detailhandel, febr. 1997

Keesman, P. & Scholtes, M. 'Amsterdam pakt georganiseerde criminaliteit bestuurlijk aan. De ontwikkeling van een effectief instrumentarium', *Tijdschrift voor de politie*, 1998, 10, pp. 10-15

Kernteam Noord- en Oost-Nederland, *Algemene criminaliteitsbeeldanalyse Oost-Europa 2000-2001*, december 2001

Kerstens, R., 'Een vennootschap in 24 uur? Het kan zelfs in 8 minuten', *Ondernemersvisie*, juni 1995

Kleemans, E.R., Berg, E.A.I.M. van den & Bunt, H.G. van de, *Georganiseerde criminaliteit in Nederland. Rapportage op basis van de WODC-monitor*, Den Haag, Wetenschappelijk Onderzoek- en Documentatiecentrum, 1999

Kleemans, E.R., Brienen, M.E.I. & Bunt, H.G. van de, *Georganiseerde criminaliteit in Nederland. Tweede rapportage op basis van de WODC-monitor*, Den Haag, Wetenschappelijk Onderzoek- en Documentatiecentrum, 2002

Klerks, P.P.H.M., *Groot in de hasj. Theorie en praktijk van de georganiseerde criminaliteit*, Politiestudies 26, Deventer, Samsom, 2000

Klerks, P. & Versteegh, P., 'De analist in zijn relatie met opdrachtgever en klant', in Moerland, H. & Rovers, B. (red.), *Criminaliteitsanalyse in Nederland*, 's-Gravenhage, Elsevier bedrijfsinformatie, 2000, pp 371-390

Klijn, E.H., 'Vervlechten, activeren en constitueren van spelen in beleidsnetwerken', in Koppenjan, J.F.M., De Bruijn, J.A. & Kickert, W.J.M., *Netwerkmanagement in het openbaar bestuur. Over de mogelijkheden van overheidssturing in beleidsnetwerken*, 's-Gravenhage, Vuga, 1993, pp. 55-74

Koning, M.J. de, Dijkstra, R.F., Kuipers, M.A., Raskeyn, J.E. & Schmal, J.A., *Risicomodel voor de politie in het kader van Integrale Veiligheid*, Utrecht, Politie Utrecht.

Koppenol, P.A., 'Contouren nieuw concept informatiearchitectuur politie. Werk van agent is basis voor informatiehuishouding', *Tijdschrift voor de politie*, 61 (1999), 9 (september), pp. 9-12

Kortekaas, J.J.C. & Aalbersberg, P.J., *Recherche-informatiehuishouding: basis voor criminaliteitsbestrijding. Discussiestuk*, Zoetermeer, KLPD, divisie Centrale Recherche Informatie, 22 mei 1996

Kortekaas, J.J.C., 'Uitwisselen recherche-informatie: een dilemma?', *Algemeen Politie Blad*, 145 (1996), 9, pp. 12-14

Leest, W.P.E. van der & Bruinsma, G.J.N., *Voorstudie: het landelijk criminaliteitsbeleid 1992-1996 voor het ACCACIA-programma. Het landelijk criminaliteitsbeleid in de periode 1992-1996*, Enschede, 1996 (IPIT)

Leppä, S., *Anticipating Instead of Preventing: Using the Potential of Crime Risk Assessment in Order to Minimize the Risks of Organised and Other Types of Crime*, HEUNI Paper No. 11, Helsinki, 1999 (http://www.vn.fi.om/heuni)

Lier, R. van, *Samen werken aan veiligheid*, Venlo, 1998

Lier, R. van, 'Gemeenten en veiligheid. Lokaal bestuur moet verantwoordelijkheid actiever oppakken', *Algemeen Politieblad*, 147 (1998), 15, pp. 13

Lipsey, R.G.& Steiner, P.O., *Economics*, sixth edition, New York, Harper & Row Publishers, 1981

Lof, E, 'De barensweeën van de Nieuwe Economie', *Intermediair*, 1 (4 januari 2001), pp. 52-53

Luijks, E., 'De toepassing van fraudetectiesystemen binnen het creditcardbetalingsverkeer', in Moerland, H. & Rovers, B. (red.), *Criminaliteitsanalyse in Nederland*, 's-Gravenhage, Elsevier bedrijfsinformatie BV, 2000, pp. 223-231

Lupsha, P.A., 'Transnational Organized Crime versus the Nation-State', Transnational Organized Crime, 2 (1996), 1, pp. 21-48

Lyre, M., 'Typering van gelegenheden; risicoanalyse betreffende fraude met werknemersverzekeringen', in Moerland, H. & Rovers, B. (red.), *Criminaliteitsanalyse in Nederland*, 's-Gravenhage, Elsevier bedrijfsinformatie, 2000, pp. 213-222

Maltz, M.D., *Measuring the Effectiveness of Organized Crime Control Efforts*, The Office of International Criminal Justice, Chicago, Ill., 1990

Man, A.P. de, Geurts, D. & Dullemen, G. van, 'Working networks', in Zee, H.van der & Strikwerda, H. (eds.), *Capturing Value in the New Economy. Turning aspirations into profits in turbulent times*, Pearson Education Uitgeverij BV, 2001, pp. 120-135

March, J.G., *A Primer on Decision Making. How decisions happen*, New York, The Free Press, 1994

Marchand, D.A. & Horton, F.W., *Infotrends. Informatie als sleutel tot winst*, Amsterdam Brussel, De Management Bibliotheek, 1986

Mastrofski, S. & Potter, G., 'Controlling Organized Crime: A Critique of Law Enforcement Policy,' *Criminal Justice Policy Review*, 2, 3 (Sept. 1987), pp. 269-301

McCarthy, E.J., *Basic marketing a managerial approach*, 7th edition, Homewood Illinois, Richard D. Irwin, Inc., 1981

Mc Dowell, D., *Strategic intelligence training course*, Istana Enterprises PTY lTD (Australia), 1996

Mc Dowell, D., *Strategic intelligence. A handbook for practitioners, managers and users*, Istana Enterprises PTY LTD (Australia), 1998

Meesters, P., Kortekaas, J. & Tragter, M., 'Intelligence led policing: nieuw concept voor integratie van oude adagia', *Tijdschrift voor Criminologie*, 1999, 4, pp. 418-429

Meesters, P. & Niemeijer, B, 'Criminaliteitsbeeldanalyse: problemen en mogelijkheden', in Moerland, H. & Rovers, B. (red.), *Criminaliteitsanalyse in Nederland*, 's-Gravenhage, Elsevier bedrijfsinformatie, 2000, pp. 293-308

Meijers, H., 'Internethandel en lage inflatie in de informatie-economie', in Soete, L., (red.) *ICT en de nieuwe economie. Preadviezen van de Koninklijke Vereniging voor de Staathuishoudkunde 2000*, Utrecht, Lemma BV, 2000, pp. 83-104

Meyer, O.M.T., 'Informatisering en politieke agendavorming: de agendavormende waarde van informatiesystemen', in: Zuurmond, A. (red.), *Informatisering in het openbaar bestuur. Technologie en sturing bestuurskundig beschouwd*, 's-Gravenhage, VUGA, 1994, pp. 113-133

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Ministerie van Justitie, *Beleidsplan Nederlandse politie 1999-2002*, december 1998

Ministeries van Economische Zaken, Binnenlandse Zaken en Koninkrijksrelaties, Financiën, Justitie, Onderwijs, Cultuur en Wetenschappen en Verkeer en Waterstaat, *De digitale delta, Nederland online,* juni 1999

Ministerie van Justitie, *Wetgeving voor de elektronische snelweg*, 's-Gravenhage, Sdu uitgevers, 1998

Ministerie van Justitie, Directie Algemene Justitiële Strategie, *Justitie over morgen. Een strategische verkenning*, Den Haag, Sdu, 2001

Ministerie van Justitie, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, *Naar een veiliger samenleving*, Den Haag, oktober 2002 (www.justitie.nl en www.minbzk.nl).

Mitchell Robinson, D., *Routine Activity Theory: The commentator's Perspective*, in Adler, P., Adler, P.A. & Bryant, C.D. (Red.), Encyclopedia of criminology and deviant behavior. Volume I: Historical, conceptional, and theoretical issues, Philadelphia, PA, Brunner-Routledge, 2001, pp 335-337

Moerland, H. & Boerman, F., *Georganiseerde misdaad en betrokkenheid van bedrijven*, Deventer, Gouda Quint, 1999

National Crime Authority, *Discussion paper for the Intergovernmental Committee on the criteria for evaluating the impact on the Australian Community of specific types of organised criminal activity*, 1992

Naylor, R.T., 'Mafias, Myths, and Markets. On the theory and practice of enterprise crime', *Transnational organized crime*, 3 (1997), 3, pp. 1-45

NCIS Project Trawler: Crime on the information highways, june 1999

NCIS, *The National intelligence model*, London, 2000

NCIS, *2000 UK Threat Assessment. Unclassified Summary*, London, may 2000 (www.ncis.gov.uk)

NCIS, *2001 UK Threat Assessment. Unclassified Summary*, London, august 2001 (www.ncis.gov.uk)

NCIS, *UK Threat assessment 2002. The threat from serious and organised crime* (www.ncis.gov.uk)

Nelson, J., 'Grappling with crime wave on the web', *Los Angeles Times*, 30-11-1997

O'Brien, K.A., 'The fight against cyber-crime, *Jane's intelligence review*, 12 (2000), 12 (December), pp. 10-11

Openbaar Ministerie, *Perspectief op 2006*, Den Haag, 2002 (download van website Ministerie van Justitie)

Paoli, L., 'The paradoxes of organized crime', *Crime, Law & Social Change*, 37 (2002), xx, pp. 51-97

Patijn, S., 'De erven Van Traa', In *Bestuurlijke preventie van georganiseerde misdaad. Verslag van een conferentie gehouden op 9 april 1999 in de Raadzaal van de gemeente Amsterdam*, Dordrecht, 1999

Pieper, R, *De ingrediënten van de netwerkmaatschappij*, 2000 (www.roelpieper.com)

Pols, E.J.V. & Visser, F.M, 'Prioriteitstelling bij aanpak misdaad. Nieuw instrument om de maatschappelijke impact van criminele organisaties te meten', *Algemeen Politieblad Van Het Koninkrijk Der Nederlanden*, 147 (1998), 13 (20 juni), pp. 14-16

Porter, M.E., 'Strategy and the Internet', *Harvard Business Review*, 79, 3 (march 2001), pp. 62-78

Power, R., '2000 CSI/FBI Computer Crime and Security Survey', *Computer Security Journal,* Volume XVI, 2 (2000), pp. 33-49

Power, R. Tangled Web, *Tales of Digital Crime from the Shadows of Cyberspace*, Indianapolis Indiana, QUE, 2000

Projectgroep Opsporing Raad van Hoofdcommissarissen, *Visiedocument misdaad laat zich tegenhouden. Advies over bestrijding en opsporing van criminaliteit*, november 2001

Randall, D., 'Internetstrategieën: vier scenario's', *PEM*, 13(1997), 4, pp. 67-80 (vertaling uit *Long Range Planning*, 30, 2)

Reuter, P., *Disorganized Crime: Illegal Markets and the Mafia*, Cambridge, MA; London, The MIT Press, 1984

Robinson, J., *De Fusie. Hoe de georganiseerde misdaad de wereld overneemt*, Rijswijk, Elmar B.V., 2000 (oorspronkelijke titel "The Merger, UK, Simon & Schuster, 2000)

Rosenthal, U., Ringeling, A.B., Bovens, M.A.P. Hart, P. 't & Twist, MJ.W. van, *Openbaar Bestuur. Beleid, organisatie en politiek*, 5e druk, Alphen aan den Rijn, Samsom HD Tjeenk Willink, 1996

Rossum, G. van, 'Criminaliseren van internet-misbruik? Een pleidooi voor zelfregulering binnen internationale kaders', *Justitiele verkenningen*, jrg. 26 (2000), 5, pp. 45-57

Royal Canadian Mounted Police, *Sleipnir: The long matrix for organized crime. An analytical technique for determining relative levels of threat posed by organized crime groups*, Canada, 2000 (unclassified)

Ruggiero, V., *Organized and corporate crime in Europe. Offers that can't be refused*, Aldershot, Hants, Dartmouth Publishing Company, 1996

Shubik, M., 'Risk Society, Politicians, Scientists, and People', Shubik, M. (ed), *Risk, organizations, and society*, Boston, Kluwer Academic Publishers, 1991, pp. 7-29

Shubik, M. (ed.), *Risk, organizations, and society*, Boston, Kluwer Academic Publishers, 1991

Simon, H.A., *Administrative behavior. A Study of Decision-Making Processes in Administrative Organizations*, 4th edition, New York, The Free Press, 1997

Sinuraya, T., 'Integration of criminal capital from Russia into West European markets: An assessment of threat', *Journal of money laundering control,* 1 (1997), 1 (juni), pp. 32-41

Smith, D.C., 'Illicit Enterprise: An Organized Crime Paradigm for the Nineties,' in Kelly, R.J., Chin, K. & Schatzberg, R. (eds.), *Handbook of Organized Crime in the United States,* Westport Connecticut, Greenwood Press, 1994, pp. 121-150

Soete, L., *Infonomie, contouren van een nieuwe discipline*, Maastricht, 15 augustus 1999

Soete, L., 'Inleiding', in Soete, L., (red.), *ICT en de nieuwe economie. Preadviezen van de Koninklijke Vereniging voor de Staathuishoudkunde 2000*, Utrecht, Lemma BV, 2000, pp. VII-XIX

Starr, C.& Whipple, C, 'The strategic Defense Initiative and Nuclear Proliferation from a Risk Analysis Perspective', in Shubik, M. (ed), *Risk, organizations, and society*, Boston, Kluwer Academic Publishers, 1991, pp. 49-62

Stevens, L.G.M., *Basisboek Belastingen*, Deventer, Kluwer, 1997

Stol, W.Ph., Treeck, R.J. van & Ven, A.E.B.M. van der, *Aard, ernst en aanpak van criminaliteit met informatie- en communicatietechnologie. Een praktijkonderzoek met veertig aanbevelingen*, In-pact onderzoeksreeks, 1999

Stol, W., Treeck, R. van & Ven, S. van der, 'Criminaliteit met informatie- en communicatietechnologie. Politie in een nieuwe sociale context', *Tijdschrift voor criminologie*, 41 (1999), 4, pp. 364-376

Strikwerda, H., 'What's new about the new economy, and what isn't?', in Zee, H. van der & Strikwerda, H. (eds.), *Capturing Value in the New Economy. Turning aspirations into profits in turbulent times*, Pearson Education Uitgeverij BV, 2001, pp. 12-31

Strikwerda, H. & Ridder, S. de, 'Exit considerations, exit types and exit strategies', in Zee, H.van der & Strikwerda, H. (eds.), *Capturing Value in the New Economy. Turning aspirations into profits in turbulent times*, Pearson Education Uitgeverij BV, 2001, pp. 136-150

Stuurgroep Informatie gestuurde opsporing, *Informatie gestuurde opsporing. It's no rocket science, it's just common sense but it works'*, Woerden, Abrio-programmabureau, 10 april 2001

Stuurgroep Informatie gestuurde opsporing, 'Informatie gestuurde opsporing' moet Nederland veroveren. Going intelligence led in the UK', *Tijdschrift voor de Politie*, 63 (2001), 6, pp. 11-15

Sussmann, M.A., '*Locating and Identifying Cybercriminals Across National Borders*, Ghent Belgium, 24 january 2001

Svensson, J. & Wijk, A.H.W. van, 'Deel 2: Gratis zullen wij alles delen. Over bestandsuitwisseling en gedragsregels op het internet', in Svensson, J. & Zouridis, S., *Waarden en normen in de virtuele wereld. Twee verkennende studies met discussie*, Enschede, IPIT Instituut voor Maatschappelijke Veiligheidsvraagstukken Universiteit Twente, 2004, pp. 13-82

Svensson, J. & Zouridis, S., *Waarden en normen in de virtuele wereld. Twee verkennende studies met discussie*, Enschede, IPIT Instituut voor Maatschappelijke Veiligheidsvraagstukken Universiteit Twente, 2004

Swaaningen, R. van, 'Criminaliteitsbeleid en risicobeheersing' in Lissenberg, E., Ruller, S. van, Swaaningen, R. van (red.), *Tegen de regels IV. Een inleiding in de criminologie*, Nijmegen, Ars Aequi Libri, 2001, pp. 277-292

Sweeney, P., 'Cyber-Crime's Looming Threat', *Banking strategies*, july/august 1999, pp. 54-59

Teisman, G., 'De reconstructie van beleidsprocessen: over fasen, stromen en ronden', in Heffen, O. van & Twist, M.J.W. van, *Beleid en wetenschap. Hedendaagse bestuurskundige beschouwingen*, Alphen aan den Rijn, Samsom H.D. Tjeenk Willink, 1993, pp. 18-32

Termeer, C.J.A.M., 'Een methode voor het managen van veranderingsprocessen in netwerken', in Koppenjan, J.F.M., De Bruijn, J.A. & Kickert, W.J.M., *Netwerkmanagement in het openbaar bestuur. Over de mogelijkheden van overheidssturing in beleidsnetwerken*, 's-Gravenhage, Vuga, 1993, pp. 105-121

University of Texas, *Measuring the Internet Economy*, june 6, 2000 (www.internetindicators.com)

Valeri, L., 'Europe tackles cyber-crime', *Jane's intelligence review*, april 2001, pp. 52-54

Veld, R.J. in 't & Knaap, P. van der (auth.&red.), *Dynamische bestuurskunde. Informatie en sturing in publieke dynamiek Perspectieven voor het leervermogen van de overheid*, 's-Gravenhage, Phaedrus, 1994

Verschuren, P.J.M., *De probleemstelling voor een onderzoek*, 6e druk, Utrecht, Het Spectrum B.V, 1996

Vette, R.C.M. de, Landman, R. & Ven, N. van de, *Nederlandse opsporingsonderzoeken naar georganiseerde criminaliteit in 1998. Situatierapport in het kader van de inventarisatie georganiseerde criminaliteit van de Europese Unie*, Zoetermeer, 1999

Vijver, C.D. van der, 'De tranen van Foucault. De behoefte aan theoretische benaderingen van handhaving', *Het tijdschrift voor de politie*, 60 (1998), 11, pp. 29-35

Vries, M.S. de, 'Problemen op de agenda', in Hoogerwerf, A. & Herweijer, M. (red.), *Overheidsbeleid*, 6e druk, Alphen aan den Rijn, Samsom, 1998, pp. 39-57

Vriesde, R.H.P., Gels, M.C. & Oss, J. van, 'Criminaliteit op Internet (2). Een overzicht van de verschijningsvormen', *Algemeen politieblad van het koninkrijk der Nederlanden,* 148 (1999), 13, (19 juni), pp. 8-10

Vuijsje, F., *21 misverstanden over de Nieuwe Economie*, Amsterdam, Meulenhoff, 2000

Wardlaw, G., *The use of risk management techniques to increase the impact of strategic intelligence: a case study*, Barton (Australia), 1999. (Address to the 2nd International Conference for Criminal Intelligence Analysts, 'Assessing Tomorrow's Challenges Today', London, 1-3 March 1999)

Werken aan vertrouwen, een kwestie van aanpakken strategisch akkoord voor kabinet CDA, LPF, VVD, 3 juli 2002

Westerman, F., 'Te koop: Europese passen', *NRC webpagina's*, 18-9-99

Wiebrens, C.J. & Röell, A., 'Ondernemen in de onderwereld', *Justitiële verkenningen*, 14 (1988), 2, maart, pp. 53-82

Williams, P. 'The International drug Trade: An industry analysis', in Turbiville G.H. (ed.), *Global dimensions of high intensity crime and low intensity conflict*, 1995, Chicago, pp. 153-183

Williams, P., 'Getting Rich and Getting Even: Transnational Threats in the Twenty-First Century', in *Organized crime. Uncertainties and dilemmas*, Chicago IL, Office of International Criminal Justice, 1999, pp. 19-63

Williams, P. & Godson, R., 'Anticipating organized and transnational crime', *Crime, law and social change*, 37 (2002), 4, pp. 311-355

Zouridis, S., 'Deel 1: Samenvatting en discussie', in Svensson, J. & Zouridis, S., *Waarden en normen in de virtuele wereld. Twee verkennende studies met discussie*, Enschede, IPIT Instituut voor Maatschappelijke Veiligheidsvraagstukken Universiteit Twente, 2004, pp. 1-12

Zouridis, S. & Frissen, P.H.A., 'Deel 3: Over virtuele vrijplaatsen en civilisatie in cyberspace. Regulering, handhaving en sociale controle in de virtuele wereld', in Svensson, J. & Zouridis, S., *Waarden en normen in de virtuele wereld. Twee verkennende studies met discussie*, Enschede, IPIT Instituut voor Maatschappelijke Veiligheidsvraag-stukken Universiteit Twente, 2004, pp. 83-140

Begrippenlijst

Betrokkene (bij georganiseerde criminaliteit)
Een betrokkene is die persoon of organisatie die fungeert als leverancier, afnemer of ondersteuner van een illegale groothandelsonderneming en daar geen deel van uitmaakt.

E-commerce
Castells verstaat onder e-commerce "[….] any business activity whose performance of the key operations of management, financing, innovation, production, distribution, sales, employee relations, and customer relations takes place predominantly by/on the internet or other networks of computer networks, regardless of the kind of connection between the virtual and the physical dimensions of the firm".[1]

Gelegenheidsfactor illegale groothandelsonderneming
De factoren die bepalen in hoeverre misdaadondernemingen de functies van de groothandel voor hun rekening willen en kunnen nemen.

Gelegenheidsfactor illegale groothandelswaar
De factoren die bepalen in hoeverre een illegaal product geschikt is voor de illegale groothandel.

Gelegenheidsfactor locatie (georganiseerde criminaliteit)
De factoren die bepalen in hoeverre illegale groothandelsondernemingen (aspecten van) hun groothandelsactiviteiten in een specifiek land of gebied willen en kunnen uitvoeren.

Gelegenheidsfactor sociale controle (georganiseerde criminaliteit)
De factoren die bepalen in hoeverre betrokkenen, de overheid en anderen maatregelen willen of kunnen treffen om de risico's voor illegale groothandelsondernemingen zodanig hoog te maken dat zij afzien van de handel.

Georganiseerde criminaliteit
Georganiseerde criminaliteit is het uitvoeren van illegale groothandelsactiviteiten in één of meer misdaadmarkten door een illegale groothandelsonderneming.

Groothandelsfuncties
Deze functies zijn: kopen, verkopen, sorteren, opslaan, transporteren, financieren, het nemen van risico's en marktinformatie vergaren.

ICT (informatiecommunicatietechnologie)
Castells verstaat onder I(C)T "[….] the converging set of technologies in microelectronics, computing (machines and software), telecommunications/ broadcasting, and optoelectronics".[2] Hij spreekt overigens over Informatietechnologie (IT) in plaats van ICT. Bovendien rekent hij ook biotechnologie tot IT, een benadering die in dit proefschrift niet is gehanteerd. Ondanks deze kanttekeningen is hij één van de weinigen die een definitie geeft. Daarom is deze gebruikt.

[1] {Castells, 2001, 66}.
[2] {Castells, 1998A, 30}.

Onder ICT valt zowel hardware als software waaronder besturingssoftware (bijvoorbeeld Windows) en applicatiesoftware (bijvoorbeeld Microsoft Word). Onder hardware vallen zowel complete computers, computeronderdelen (bijvoorbeeld chips) als telefoongerelateerde hardware zoals een mobiele telefoon.

ICT-innovatie
De ontwikkelingen in ICT bezien vanuit de techniek.

ICT-ontwikkelingen
Een verzamelbegrip voor de wisselwerking tussen de <ICT-innovatie> en de daaruit voortkomende veranderingen in de samenleving (en vice versa).

Illegaal product
Een product dat bonafide bedrijven in het geheel niet, tegen hogere kosten of lagere winstmarge produceren of leveren doordat het product op zich en/of onderdelen van het productieproces a) strafbaar zijn of b) strikt gereguleerd zijn en er sprake is van overtreding van die regulerende wet- of regelgeving.

Illegale bedrijfsvoering
Verzamelbegrip voor de <uitoefening van de groothandelsfuncties> en de <ondersteunende (criminele) activiteiten>. Het accent ligt op de invalshoek van de bedrijfsvoering.

Illegale groothandel
Synoniem voor illegale groothandelsactiviteiten.

Illegale groothandelsactiviteiten
Verzamelbegrip voor de <uitoefening van de groothandelsfuncties> en de <ondersteunende (criminele) activiteiten>. Het accent ligt op de invalshoek van de activiteiten.

Illegale groothandelsonderneming
Een illegale groothandelsonderneming is een organisatie van kapitaal en arbeid die de volgende kenmerken vertoont:
- zelfstandigheid (handelt onder eigen naam, voor eigen verantwoordelijkheid en voor eigen risico);
- met als belangrijkste functie het leveren van illegale groothandelsactiviteiten;
- met een opzichzelfstaand illegaal winstoogmerk;
- voor haar bestaan afhankelijk van inkomsten uit criminaliteit;
- met een in beginsel niet beperkte kring van afnemers (detailhandelaren, andere groothandelsondernemingen of tussenconsumenten).

Misdaadmarkt
Een misdaadmarkt is een ruimte waarin voortdurend vraag naar en aanbod van illegale producten bij elkaar komen.

Misdaadonderneming
Een misdaadonderneming is een organisatie van kapitaal en arbeid die de volgende kenmerken vertoont:

- zelfstandigheid (handelt onder eigen naam, voor eigen verantwoordelijkheid en voor eigen risico);
- gericht op een duurzame markgerichte onwettige bedrijvigheid;
- met een opzichzelfstaand illegaal winstoogmerk;
- voor haar bestaan afhankelijk van inkomsten uit criminaliteit;
- met een in beginsel niet beperkte kring van afnemers.

Ondersteunende (criminele) activiteiten
De activiteiten die nodig zijn om de primaire (criminele) activiteiten mogelijk te maken en de criminele opbrengsten veilig te stellen. Deze activiteiten dragen niet bij aan de winst. Voorbeelden zijn personele, financiële en beveiligingsactiviteiten en witwassen.

Primaire (criminele) activiteiten
De primaire activiteiten hangen direct samen met de rol van groothandel, namelijk het kopen, verkopen, sorteren, opslaan, transporteren, financieren, het nemen van risico's en marktinformatie vergaren. Deze activiteiten genereren de winst waar het allemaal om te doen is. Een voorbeeld daarvan is het importeren en verkopen van partijen drugs.

Risico
Een risico is de combinatie van de waarschijnlijkheid dat een dreiging zich manifesteert en de ongewenste effecten daarvan.

Risicofactor
Een factor die de waarschijnlijkheid van de dreiging beïnvloedt.

Risico-indicator
Een operationalisatie van een risicofactor.

Secundaire (criminele) activiteiten
Activiteiten die nodig zijn om de primaire (criminele) activiteiten te kunnen uitvoeren, maar niet bijdragen aan de winst. Voorbeelden zijn het corrumperen van ambtenaren of het vervalsen van identiteitsdocumenten.

Transactiekosten
"Transaction costs are the costs arising from finding someone with whom to do business, of reaching an agreement about the price and other aspects of the exchange, and of ensuring that the terms of the agreement are fulfilled. Transaction costs are additional to, and do not include, the costs of production".[3]

Uitoefening van de groothandelsfuncties
Verzamelbegrip voor zowel de <primaire (criminele) activiteiten> als de <secundaire (criminele) activiteiten>.

Verandering in de illegale bedrijfsvoering
Er is daarvan sprake wanneer als gevolg van één of meer ontwikkelingen de werkwijze in de bedrijfsvoering van illegale groothandelsondernemingen wijzigt.

[3] {Halstead, 1998, 12}

Verandering in illegale groothandelsondernemingen
Er is daarvan sprake wanneer als gevolg van één of meer ontwikkelingen er een wijziging optreedt in de aard, samenstelling of structuur van illegale groothandelsondernemingen.

Verandering in illegale groothandelswaar
Er is daarvan sprake wanneer als gevolg van één of meer ontwikkelingen er 1) een nieuw illegaal product ontstaat dat geschikt is voor illegale groothandelsondernemingen, 2) het volume en/of de financiële omzet van bestaande illegale groothandelswaar op jaarbasis toenemen of 3) het volume en/of de financiële omzet van bestaande illegale groothandelswaar op jaarbasis toeneemt ten koste van andere bestaande illegale groothandelswaar.

Virtuele illegale groothandelsonderneming
Er is sprake van een virtuele illegale groothandelsonderneming wanneer deze de koop, verkoop, en/of de distributie in de virtuele ruimte heeft vormgegeven.

Virtuele illegale producten
Illegale producten waarvan de koop, verkoop en de distributie volledig in de virtuele ruimte plaatsvinden.

Virtuele ruimte
De virtuele ruimte is in de kern een communicatieomgeving waarin het mogelijk is om met velen mondiaal interactief te communiceren op elk gewenst moment van de dag. Het is de wereld van bits en bytes en van digitaal verbonden netwerken, waarvan het internet het belangrijkst is. Naast een technische dimensie, de netwerken die mondiaal aan elkaar zijn gekoppeld, kent de virtuele ruimte vooral een sociale dimensie. Doordat communicatie cruciaal is voor het menselijke bestaan, beïnvloedt de virtuele ruimte vele facetten van onze hedendaagse samenleving. In de virtuele ruimte bestaan tal van 'gemeenschappen' van bijvoorbeeld gelijkgestemden of personen met gemeenschappelijke problemen.[4]

Vroegtijdige criminaliteitsbeheersing
Verzamelbegrip voor <vroegtijdige preventie> en <vroegtijdige preparatie>.

Vroegtijdige preparatie
Het zich voorbereiden op veranderingen met ongewenste effecten voordat de veranderingen zich manifesteren.

Vroegtijdige preventie
Het voorkomen dat veranderingen zich voordoen en/of leiden tot ongewenste effecten voordat de veranderingen zich manifesteren.

[4] Zie paragraaf 5.4, 5.6 en 5.7 en {Castells, 2001, 2, 5}, {Zouridis & Frissen, 2004}.

Bijlagen

Bijlage 1 Ongewenste effecten georganiseerde criminaliteit

Impliciet noemt de onderzoeksgroep Fijnaut enkele belangen die in het geding zijn.

> *"Want waar gaat het volgens deze definitie in essentie om bij georganiseerde criminaliteit? Uiteindelijk om de vreedzaamheid van een maatschappij, om de integriteit van de democratische rechtsstaat, de vrijheid van het economisch leven en de rechten van individuele burgers.*
>
> *Meer nog dan de schade die georganiseerde criminaliteit teweegbrengt, is dit vermogen om zich effectief teweer te stellen, wat in het ultieme geval kan leiden tot de vorming van een 'staatje' binnen de staat, bedreigend voor het democratisch gehalte van de samenleving."*[1]

Verder noemt de onderzoeksgroep een aantal zorgelijke kwesties.[2]

NCIS heeft de maatschappelijke gevolgen van georganiseerde criminaliteit bepaald in financiële termen. Daarbij heeft men gebruikgemaakt van een systematiek om de gevolgen van verkeersongevallen om te rekenen naar financiële schade. De systematiek en de variabelen zijn niet gespecificeerd en de onderbouwing is daardoor niet transparant. NCIS heeft een rangorde aangebracht tussen verschillende misdaadmarkten op basis van de berekende financiële schade.[3]

Het Kernteam Noord- en Oost-Nederland heeft op basis van de criteria van de vergadering van PG's de maatschappelijke schade van criminaliteitsvelden en -vormen beoordeeld.[4] In de beoordeling weegt het kernteam het aantal incidenten mee. Met andere woorden, de maatschappelijke schade is niet alleen afhankelijk van de belangen die worden aangetast, maar ook van het aantal keren dat die belangen worden aangetast. Op deze wijze worden twee dimensies met elkaar vermengd. Daardoor neemt de transparantie van het eindoordeel af. Zijn weinig incidenten met veel schade ernstiger dan veel incidenten met weinig schade?

Maltz heeft geprobeerd de effectiviteit te meten van de bestrijding van georganiseerde criminaliteit. Hij onderscheidt vijf soorten schade, namelijk: a) fysieke schade, b) economische schade, c) psychologische schade, d) schade aan de gemeenschap of buurt en e) schade aan de samenleving als geheel. Hij onderkent dat de soorten schade elkaar niet uitsluiten. Fysieke schade zal bijvoorbeeld veelal ook leiden tot psychische schade en schade aan de samenleving als gevolg van onveiligheidsgevoelens. Voor economische schade hanteert hij twee meeteenheden: het economische verlies van de slachtoffers en de winst van de misdaadondernemingen. Hij kwantificeert dit in dollars. Indirecte effecten neemt hij niet mee, zoals faillissement als gevolg van beroving. Schade aan de samenleving heeft uiteindelijk ook van doen met sociale schade en economische schade. Gedacht kan worden aan: ontwrichting van een wijk, infiltratie in legale sectoren en dergelijke. Sociale schade is volgens hem bijzonder moeilijk kwantitatief of kwalitatief te meten. Is de

[1] {Enquêtecommissie, 1996B, 145, 24}.
[2] Zie subparagraaf 4.8.2.
[3] {NCIS, 2000B, 13}.
[4] {Kernteam Noord en Oost Nederland, 2001, 147-154}.

schade van georganiseerde criminaliteit in een buurt het gevolg van het feit dat de buurt veel slachtoffers kent, omdat de buurt in grote mate betrokken is of vanwege de vrees ervoor? Hij bepaalt de schade voor enkele misdaadmarkten. Zowel de aard als de omvang van de schade kan immers variëren. Wanneer misdaadmarkten onderling samenhangen is het lastig om dit te bepalen. Hoe schade te meten als bijvoorbeeld met de winsten van illegaal gokken, drugsimport wordt gefinancierd?[5] Wordt dan alleen gekeken naar de schade van het gokken? Vindt een cumulatie plaats met schade van de drugsimport? Of vindt een cumulatie plaats en wordt nog een extra verzwaring toegepast?

Klerks borduurt voort op de indeling van Maltz. Hij beoordeelt de effecten van een specifieke criminele groep op basis van zes variabelen. Hij gebruikt hiervoor de empirische gegevens die beschikbaar zijn over de groep en kent een score toe. Uiteindelijk past hij een correctie toe voor de geografische schaal waarop de groep actief is. Internationaal scoort hoger dan regionaal.[6]

De National Crime Authority van Australië hanteert een mengvorm van allerlei ongewenste effecten. Men neemt niet alleen ongewenste effecten in de beoordeling mee, maar ook kenmerken van de bedrijfsvoering. Zelfs de gevolgen van gerelateerde criminaliteit beoordeelt men (zie figuur B.1). Onder gerelateerde criminaliteit verstaan ze bijvoorbeeld drugsoverlast.[7] De Royal Canadian Mounted Police (RCMP) beoordeelt de dreiging van criminele groepen op basis van de kenmerken ervan. Voorbeelden zijn: het gebruik van corruptie en geweld, mobiliteit en dergelijke.[8] Volgens de gekozen uitgangspunten vallen deze buiten de ongewenste effecten. Wardlaw beoordeelt de risico's van georganiseerde criminaliteit op basis van enkele concrete belangen (zie figuur B.1). Het nadeel is dat de aanduiding niet altijd duidelijk maakt wat hij bedoelt. Een nadere omschrijving ontbreekt namelijk. Wat bedoelt hij bijvoorbeeld met immigratie of telecommunicatie? Daardoor is zijn opsomming nauwelijks bruikbaar.

Enkele van de in deze bijlage genoemde effecten vallen af op grond van de gehanteerde uitgangspunten. Dat geldt in elk geval als men kenmerken noemt van de bedrijfsvoering of instrumentele activiteiten voor de illegale bedrijfsvoering. Desondanks blijft een grote hoeveelheid over. Het abstractieniveau varieert evenals de terminologie. De National Crime Authority benoemt bijvoorbeeld als categorie sociale gevolgen, terwijl Maltz en Klerks spreken over schade aan de lokale gemeenschap en de samenleving. De onderzoeksgroep Fijnaut spreekt op haar beurt over 'vreedzaamheid van de samenleving', wat een aspect is van sociale schade of schade aan de samenleving. Alleen Wardlaw specificeert concreet de belangen die in het geding zijn.

[5] {Maltz, 1990, 41-47}.
[6] {Klerks, 2000, 449-453}.
[7] {National Crime Authority, 1992}.
[8] { Royal Canadian Mounted Police, 2000}.

Instantie	Doel	Genoemde vormen van consequenties
Maltz	Effectiviteitmeting van de bestrijding	De dimensies van schade zijn: a) fysieke schade (moord, aanranding en ander geweld), b) economische schade (vernietiging of diefstal van eigendommen, belemmeringen in zakendoen en hogere prijzen door onderhandse contracten), c) psychologische schade (intimidatie, dwang en angst), d) schade aan de gemeenschap of buurt en e) schade aan de samenleving als geheel (verlies van vertrouwen in autoriteiten of economisch systeem).
Klerks	Beoordeling van de negatieve gevolgen van een criminele groep	Variabelen zijn: volksgezondheid en milieu, economische schade, fysieke schade aan personen, psychische schade, schade aan lokale gemeenschap en schade aan samenleving als geheel.
National Crime Authority Australia	Het evalueren van de gevolgen van de activiteiten van georganiseerde criminaliteit	Criteria zijn: • Social impact: community health and mortality, erosion of public confidence in institutions, victims of organised criminal activity, erosion of individual privacy/civil liberties; • Economic costs: revenue evasion, higher prices for goods and services, impact of fraud and other white collar criminal activities, potential impact on balance of payments, impact of perceptions of organised crime involvement on business confidence, cost of crime prevention and reduction, the costs of the criminal justice system, cost of health and welfare services; • Amount and nature of related crime; • Secondary criminal activity; • Level of organisation and sophistication involved/required; • Degree of infiltration and penetration into the community; • Level of community concern; • Proceeds of crime generated; • Extent or magnitude; • Ability to deter the crime, and • Penalty for the offence.
Wardlaw	Beoordeling van de gevolgen ten behoeve van een risicoanalyse	Hij beoordeelt de volgende gevolgen: external affairs, immigration, telecommunications and post, customs and excise, national security and defense, protection of office-holders and property, currency and exchange, taxation and revenue, financial and corporate sectors, expenditure programs and matters of national interest

Figuur B.1 Genoemde ongewenste effecten[9]

Zoals in paragraaf 4.8 reeds is verwoord, zijn in het ‘Referentiekader resultaten politiewerk’ vier resultaatgebieden benoemd. Drie daarvan kunnen relevant zijn voor georganiseerde criminaliteit. Hoewel het hier niet gaat om echt ongewenste effecten, is een toelichting wel op zijn plaats. De resultaatgebieden geven namelijk wel een beeld van de impliciete doelstellingen voor en van de politie. Het resultaatgebied *veiligheid* “[….] betreft de feitelijke of objectieve veiligheid: de feitelijke kans voor de burger slachtoffer te worden van een criminele handeling. De burger als persoon is in het geding. Hij ondervindt

[9] {National Crime Authority, 1992}, {Maltz, 1990, 41}, {Klerks, 2000 441-453}, {Wardlaw, 1999}.

dit aan den lijve. Het betreft concrete zaken, waarvan de burger hoopt dat het hem niet zal overkomen. Beter gezegd, dat hij daar geen slachtoffer van wordt. Als het hem overkomt, zal hij daarvan vrijwel zeker aangifte doen". Het resultaatgebied *leefbaarheid* "[….] betreft de relatie van de burger tot zijn leefomgeving; wat neem ik daarin waar? Waar heb ik last van? Hij dient zich prettig te voelen in die omgeving. De politie heeft hierin een aandeel. Primair verantwoordelijk voor een goede kwaliteit van de leefomgeving is de gemeentelijke overheid [….] Het is bij dit gebied moeilijk, het betreft veelal een gevoel, om zaken tot concrete feiten te herleiden. Meestal zal het gaan om overtredingen (in tegenstelling tot misdrijven), wat tot gevolg heeft dat niet vaak aangifte wordt gedaan maar er wel zaken bij de politie gemeld worden". Het resultaatgebied *maatschappelijke integriteit* "[….] betreft het beperken van en optreden tegen georganiseerde misdaad en middencriminaliteit alsmede het omgaan met de, met de multi-etnische samenleving samenhangende, illegaliteit en criminaliteit. De integriteit van de maatschappij of samenleving is hier in het geding". De burger is hier geen direct betrokkene. Veelal neemt hij het ook niet vanuit zichzelf waar. Dit resultaatgebied staat verder van de burger af en bevindt zich op een hoger abstractieniveau. Onder dit resultaatgebied vallen ook veel zogenaamde slachtofferloze delicten.[10]

[10] {Jansonius & Kuiper, 1997, 40-48}.

Bijlage 2 Relaties tussen dreigingen

	Gevolg:[2]						
Oorzaak[1]**:**	*Illegale ICT als handelswaar*	*Inzet ICT in bedrijfsvoering*	*Illegale informatie als handelswaar*	*Vergroting inzet informatie in bedrijfsvoering*	*Virtuele illegale groothandels-ondernemingen*	*Omzetting van gewone naar virtuele bedrijfsvoering*	*Misbruik ICT-sector en -deskundigen voor bedrijfsvoering*
Illegale ICT als handelswaar							
Inzet ICT in bedrijfsvoering							Mogelijke ondersteuning
Illegale informatie als handelswaar						Omzetting kan randvoorwaardelijk zijn	Mogelijke ondersteuning
Vergroting inzet informatie in bedrijfsvoering		Inzet ICT kan randvoorwaardelijk zijn					Mogelijke ondersteuning
Virtuele illegale groothandels-ondernemingen		Inzet ICT kan randvoorwaardelijk zijn				Virtuele bedrijfsvoering randvoorwaardelijk	Mogelijke ondersteuning
Omzetting van gewone naar virtuele bedrijfsvoering		Inzet ICT kan randvoorwaardelijk zijn					Mogelijke ondersteuning
Misbruik ICT-sector en -deskundigen voor bedrijfsvoering							

Figuur B.2 Relaties tussen dreigingen

[1] Een relatie in dezelfde rij, bijvoorbeeld tussen 'illegale informatie als handelswaar' (oorzaak) en 'ondersteuning ICT-sector en -deskundigen' (gevolg), bepaalt mede de ongewenste effecten van de oorzakelijke dreiging.

[2] Een relatie in dezelfde kolom, bijvoorbeeld tussen 'inzet ICT in bedrijfsvoering '(gevolg) en 'vergroting inzet informatie in bedrijfsvoering' (oorzaak), kan een rol spelen bij de waarschijnlijkheid van de gevolgdreiging.

Bijlage 3 Overzicht beoordeling dreigingen in relatie tot risicofactoren

In hoofdstuk 6 zijn dreigingen geïdentificeerd en beoordeeld op waarschijnlijkheid en ongewenste effecten. Daarbij is niet altijd expliciet aangegeven wat de beoordeling is per risicofactor. In deze bijlage zijn per dreiging wel de risicofactoren gespecificeerd.

	Dreiging:	
Risicofactoren:	*Illegale ICT als groothandelswaar*	*Illegale informatie als groothandels-waar.*
Mate waarin handelswaar geschikt is voor de illegale groothandel	Geschikt (m.u.v. illegaal gekopieerde software)	Ongeschikt (m.u.v. gestolen en vervalste fysieke vormen van audio en video).
Mate waarin misdaadon-dernemingen de functies van de groothandel voor hun rekening willen en kunnen nemen	Vanwege de geschiktheid van het product zullen er misdaadonderne-mingen zijn die die functies voor hun rekening willen en kunnen nemen.	Vanwege de ongeschiktheid van het product zullen er geen misdaad-ondernemingen zijn die de functies voor hun rekening willen en kunnen nemen.
Mate waarin betrokkenen, de overheid en anderen onvoldoende maatregelen willen of kunnen treffen	Tot op zekere hoogte is sociale controle mogelijk.	Tot op zekere hoogte is sociale controle mogelijk.
Mate waarin Nederland geschikt is	De geschiktheid is vergelijkbaar met soortgelijke illegale producten.	Er zijn geen argumenten gevonden waardoor Nederland meer of minder geschikt is.

Figuur B.3 Overzicht beoordeling voor veranderingen in illegale groothandelswaar

Risicofactoren:	**Dreiging:** *Virtuele illegale groothandelsondernemingen*
Mate waarin handelswaar geschikt is voor een bepaalde soort illegale groothandelsonderneming	Er is geen geschikte handelswaar voor een virtuele groothandelsonderneming en de virtuele ruimte is geen geschikte marktplaats.
Mate waarin een bepaalde soort misdaadonderne-ming de functies van de groothandel voor haar rekening wil en kan nemen	Op grond van bovenstaande redenen zijn er geen misdaadondernemingen die de functies voor hun rekening willen en kunnen nemen.
Mate waarin betrokkenen, de overheid en anderen onvoldoende maatregelen willen of kunnen treffen	Tot op zekere hoogte is sociale controle mogelijk.
Mate waarin Nederland geschikt is	Ook voor Nederland gelden bovenstaande argumen-ten omdat de virtuele ruimte internationaal is.

Figuur B.4 Overzicht beoordeling voor veranderingen in illegale groothandelsondernemingen

Risicofactoren:	Dreiging:			
	Inzet ICT in illegale bedrijfsvoering	*Vergroting inzet informatie in illegale bedrijfs-voering*	*Omzetting van gewone naar virtuele illegale bedrijfsvoering*	*Misbruik ICT-sector en -deskun-digen voor bedrijfsvoering*
Mate waarin andere mogelijkheden aantrekkelijk zijn	Mogelijkheden zijn niet aantrek-kelijk, m.u.v. voor communicatie, ad-ministratie en af-scherming	Mogelijkheden zijn niet aantrek-kelijk, m.u.v. het gebruik van de virtuele ruimte als informatiebron	Mogelijkheden zijn niet aantrek-kelijk, m.u.v. voor de communicatie	Mogelijkheden zijn niet aantrek-kelijk, m.u.v. onbewuste betrok-kenheid voor com-municatie, admi-nistratie en afscherming
Mate waarin illegale groothandelsonderne-mingen die mogelijk-heden willen en kunnen benutten	Willen niet o.g.v. bovenstaand argument, m.u.v. genoemde doelen	Willen niet o.g.v. bovenstaand argument, m.u.v. genoemde doel	Willen niet o.g.v. bovenstaand argument, m.u.v. genoemde doel	Willen niet o.g.v. bovenstaand argument, m.u.v. genoemde vorm
Mate waarin betrokkenen, de overheid en anderen onvoldoende maat-regelen willen of kunnen treffen	Tot op zekere hoogte is sociale controle mogelijk	Tot op zekere hoogte is sociale controle mogelijk	Tot op zekere hoogte is sociale controle mogelijk	Tot op zekere hoogte is sociale controle mogelijk
Mate waarin Nederland geschikt is	Er zijn geen argumenten gevonden waardoor Nederland meer of minder geschikt is	Er zijn geen argumenten gevonden waardoor Nederland meer of minder geschikt is	De virtuele ruimte is internationaal.	Er zijn geen argumenten gevonden waardoor Nederland meer of minder geschikt is

Figuur B.5 Overzicht beoordeling voor veranderingen in illegale bedrijfsvoering

Bijlage 4 Overzicht geïnterviewden

Datum	Geïnterview-de(n)	Organisatie	Onderwerp
16-12-1998	Strategisch onderzoeker	Korps Amsterdam-Amstelland, Dienst Centrale Recherche, Bureau Recherche-Informatie	Bestuurlijke aanpak georgani-seerde criminaliteit in Amsterdam.
15-2-1999	C.J.C.F. Fijnaut	Hoogleraar Katholieke Universiteit Leuven en Katholieke Universiteit Tilburg	Problem-solving policing en community policing in relatie tot de aanpak van georganiseerde criminaliteit.
23-02-2000	Hoofd Unit Financieel-economische criminaliteit	KLPD, (toenmalige) divisie Recherche Informatie	Ontstaan van de informatiesamen-leving en de gevolgen ervan voor financieel-economische criminaliteit.
18-08-2000	R.H.P. Vriesde	Teamleider van het project Digitaal Rechercheren van het KLPD[1]	Het doel van het interview was: (1) informatie krijgen over de werkzaamheden van het project digitaal rechercheren en (2) het verkrijgen van inzicht in bekende feiten over criminaliteit in de informatiesamenleving.
7-09-2000	P.J. Aalbersberg	Chef van het kernteam Noord-Oost-Nederland[2]	Het doel van het interview was: (1) het inventariseren van mogelijk-heden voor misdaadondernemers, (2) het verkrijgen van inzicht in bekende feiten over criminaliteit en (3) het verkrijgen van inzicht in mogelijke verschuivingen in de populatie van misdaad-ondernemers.
25-10-2000	Drie medewerkers van de security-afdeling van een internationaal opererend ICT-bedrijf.		Het doel van het interview was het verkrijgen van inzicht in: beelden over de informatiesamenleving, bekende feiten over criminaliteit en de verwachtingen omtrent criminaliteit in de informatie-samenleving.

Figuur B.6 Overzicht geïnterviewden

[1] De heer Vriesde heeft deze functie tot 1 september 2000 vervuld.
[2] De heer Aalbersberg heeft nu een andere functie binnen de politie.