Wetenschappelijk Onderzoek- en Documentatiecentrum
Ministerie van Justitie en Veiligheid

Cahier 2018-8

Georganiseerde criminaliteit en ICT

Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit

E.W. Kruisbergen
E.R. Leukfeldt
E.R. Kleemans
R.A. Roks

Met medewerking van
R.J. Kouwenberg
S.S. Nabi
T. Fiorito
T. van Ruitenburg

ERASMUS SCHOOL OF LAW
ERASMUS UNIVERSITEIT ROTTERDAM

VU VRIJE UNIVERSITEIT AMSTERDAM

nscr Nederlands Studiecentrum Criminaliteit en Rechtshandhaving

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

Voorwoord

Bij de start van de Monitor Georganiseerde Criminaliteit in 1996 was een mobiele telefoon nog een zeldzaamheid. Het was iets voor dure zakenlieden, binnenvaartschippers en beroepschauffeurs ter vervanging van de 27MC. Om te ervaren hoe sterk onze wereld veranderd is, kan ik elke lezer van dit rapport aanraden om het fragment van Frans Bromet uit 1998 nog eens te bekijken waar hij voorbijgangers interviewt over het nut van een mobiele telefoon.[1]
We zijn inmiddels twintig jaar verder en we kunnen niet meer zonder de mobiele telefoon. Het is een open deur, maar de technische ontwikkelingen gaan razendsnel. De mobiele telefoon heeft een vaste plek gekregen in ons dagelijkse bestaan, net als ICT (informatie- en communicatietechnologie) en het gebruik van internet. Het is de normaalste zaak van de wereld. We kunnen niet meer zonder én de criminelen dus ook niet.
Om deze ontwikkelingen in perspectief te kunnen plaatsen vind ik het werk van de onderzoekers in deze Monitor Georganiseerde Criminaliteit zo nuttig en zo mooi. Het dwingt praktijkmensen als mijzelf om een stap naar achteren te doen, even een moment halt te houden en terug te blikken op ons werk. De monitor geeft op deze manier al ruim twintig jaar inzicht in de aard en ontwikkeling van de georganiseerde criminaliteit in Nederland. Dit tweede deelrapport van de vijfde monitor richt zich op een essentieel onderdeel, namelijk de georganiseerde criminaliteit en ICT.
De constante veranderingen in de ICT maken dat wij ons in de opsporing en vervolging steeds moeten aanpassen in onze werkwijze en creatief moeten zijn. Onze opsporingsbevoegdheden en onderliggende wetgeving moeten daar op blijven aansluiten.
Tot slot biedt deze monitor ons ook houvast. Sommige dingen veranderen namelijk niet. Contant geld blijft toch nog steeds favoriet bij de georganiseerde criminaliteit ondanks alle verhalen over de zogenoemde E-currency, zo kunnen we lezen in dit rapport. Dat geeft ons houvast en focus in onze aanpak, ook in deze snel veranderende digitale wereld.

Mr. F.K.G. Westerbeke
Hoofdofficier Landelijk Parket, Openbaar Ministerie

[1] https://youtu.be/TNwhIHqM60g

Dankwoord

Een project als de Monitor Georganiseerde Criminaliteit kan alleen bestaan dankzij de inzet van veel verschillende mensen. Aan de basis van iedere publicatie die verschijnt op basis van de Monitor Georganiseerde Criminaliteit ligt de analyse van, doorgaans grootschalige, opsporingsonderzoeken. Voor deze vijfde ronde van de monitor zijn dertig opsporingsonderzoeken bestudeerd. Binnen het onderzoeksteam van de monitor is dit gedaan door onder andere Ruud Kouwenberg, Shir Shah Nabi, Timo Fiorito en Teun van Ruitenburg. Zonder hun grondige werk had deze publicatie niet kunnen verschijnen. Hetzelfde geldt voor de Nederlandse onderzoekers en anderen die betrokken waren bij het *EU-Project Cyber-OC*. Vijf van de dertig zaken die in de vijfde ronde van de monitor zijn opgenomen, zijn eerder gebruikt in het zojuist genoemde onderzoek naar cybercrime (Odinot et al., 2017). De betrokken onderzoekers zijn onder andere Geralda Odinot, Maite Verhoeven, Ronald Pool, Christianne de Poot, Renushka Madarie en Mark Engelhart.
Verder hebben de voorzitter en de leden van de begeleidingscommissie (zie bijlage 1) een belangrijke rol gespeeld bij dit rapport. Wij danken hen voor de prettige samenwerking en de vele bruikbare opmerkingen. Ook gaat dank uit naar de meelezers van de politie, met name Emma Ratia en Albert Harteveld, die een eerdere versie van dit rapport van nuttig commentaar hebben voorzien. Ten slotte bedanken wij alle medewerkers van het Openbaar Ministerie en de politie die via interviews en inzage in opsporingsdossiers een belangrijke bijdrage hebben geleverd aan dit rapport.

Edwin Kruisbergen, Rutger Leukfeldt, Edward Kleemans en Robby Roks

Inhoud

Bijlagen

Samenvatting

Doel, probleemstelling en opzet van dit onderzoek

Doel
Het doel van deze studie is het vergroten van het inzicht in hoe daders binnen de georganiseerde criminaliteit ICT gebruiken en welke invloed dat gebruik heeft op hun criminele bedrijfsprocessen. We richten ons daarbij niet uitsluitend op cybercrime, maar verkennen juist het gebruik van ICT én de consequenties daarvan voor een breder scala van soorten georganiseerde criminaliteit, dus ook 'traditionele' georganiseerde criminaliteit zoals drugssmokkel.
Dit onderzoek maakt onderdeel deel uit van de Monitor Georganiseerde Criminaliteit. Een goed onderbouwde aanpak van de georganiseerde criminaliteit is alleen mogelijk wanneer er een gedegen inzicht bestaat in de aard van de georganiseerde criminaliteit zoals die zich in Nederland manifesteert. De Monitor Georganiseerde Criminaliteit biedt dat inzicht door zo veel mogelijk de kennis te benutten die wordt opgedaan tijdens omvangrijke opsporingsonderzoeken. Dit rapport is het resultaat van de meest recente, vijfde ronde van de monitor (eerdere rapportages: Kleemans et al., 1998, 2002; Van de Bunt & Kleemans, 2007; Kruisbergen et al., 2012). Om dieper op bepaalde thema's in te kunnen gaan, is ervoor gekozen om de vijfde ronde uit te laten monden in drie afzonderlijke deelrapporten. In oktober 2017 is het eerste deelrapport verschenen (Van Wingerde & Van de Bunt, 2017). Dat rapport richtte zich op de strafrechtelijke afhandeling van georganiseerde criminaliteit, met name de geëiste en opgelegde straffen. Voor u ligt het tweede deelrapport, dat dus volledig in het teken staat van georganiseerde criminaliteit en ICT (informatie- en communicatietechnologie).

Probleemstelling
De probleemstelling van deze deelstudie luidt:

Hoe gebruiken dadergroeperingen in de georganiseerde criminaliteit ICT en welke gevolgen heeft dit voor de wijze waarop zij opereren?

We spitsen de probleemstelling toe op drie deelthema's, die hieronder worden geïntroduceerd.
- Het gebruik van ICT in relatie tot het ontstaan en groeien van criminele samenwerkingsverbanden.
- Het gebruik van ICT in relatie tot de logistieke keten van criminele processen.
- Het gebruik van ICT in relatie tot criminele geldstromen.

Onderzoeksopzet
De empirische kern van de Monitor Georganiseerde Criminaliteit bestaat uit de analyse van afgeronde opsporingsonderzoeken. Net als bij de vierde ronde zijn deze vijfde ronde dertig opsporingsonderzoeken op het terrein van georganiseerde criminaliteit geanalyseerd. Dit betekent dat voor deze opsporingsonderzoeken, aan de hand van een aandachtspuntenlijst (zie bijlage 2), het volledige opsporingsdossier is doorgenomen, doorgaans nadat een interview had plaatsgevonden met de zaaksofficier en/of de teamleider.

Inmiddels zijn in vijf rondes van de monitor 180 zaken via deze vaste systematiek geanalyseerd. De empirische analyses in dit deelrapport zijn gebaseerd op de ge-

noemde dertig zaken uit de vijfde ronde. We merken daarbij op dat vijf zaken op het terrein van cybercrime/ICT-gerelateerde georganiseerde criminaliteit, ook onderdeel uitmaakten uit van de studie van Odinot et al. (2017).
De dertig zaken uit de vijfde ronde van de monitor beslaan een breed scala aan delicten en criminele werkwijzen. Op basis van de mate waarin het gebruik van ICT kenmerkend is voor een zaak, zijn de dertig zaken onderverdeeld in vier categorieën. De eerste categorie omvat zaken van *traditionele georganiseerde criminaliteit*, dat wil zeggen zonder een sterke ICT-component. Hierin vallen 23 zaken. Een tweede categorie betreft zaken van *traditionele georganiseerde criminaliteit met ICT als belangrijk vernieuwend element* in de modus operandi. Daartoe rekenen we twee zaken van door ICT gefaciliteerde drugshandel/-smokkel en een zaak waarin het witwassen van bitcoins centraal staat. De derde categorie betreft gevallen van *georganiseerde low-tech cybercriminaliteit*, waartoe we een skimming- en een phishingzaak rekenen. Een vierde categorie ten slotte omvat twee zaken van banking malware en deze classificeren we als *georganiseerde high-tech cybercriminaliteit*.

Conclusies

Criminele samenwerking en het gebruik van ICT

De meeste netwerken binnen de monitorzaken van de vijfde ronde kennen een min of meer vaste groep kernleden die gedurende een langere periode samenwerken. Ook is er binnen de meeste netwerken sprake van meer en minder belangrijke verdachten en afhankelijkheidsrelaties.
Binnen de cybercrimezaken zijn technische kennis en vaardigheden voor de uitvoering van de delicten van groot belang. Opvallend is dat de betrokken daders zelf vaak niet veel technische kennis bezitten, maar deze kennis wel weten te verkrijgen via facilitators. Bij de high-tech cybercriminaliteit komen kernleden aan de benodigde technische expertise door het gebruik van forums, bij de low-tech cybercriminaliteit maken daders gebruik van contacten die ze hebben in het criminele milieu. Het zoeken naar technische kennis vindt in het eerste geval dus plaats via online interacties en in het laatste geval door offline interacties.
Wat betreft de instroom- en doorgroeimechanismen zien we over het algemeen ook in deze vijfde monitorronde dat sociale relaties een belangrijke rol spelen. Netwerken die zich bezighouden met cybercrimes, zowel de high-tech als low-tech varianten, kenmerken zich bijvoorbeeld door kernleden die afkomstig zijn uit Nederland en elkaar hebben leren kennen in de offline wereld. Deze kernleden weten zich te bewegen op forums op het darkweb, maar rekruteren ook facilitators en katvangers binnen hun eigen offline sociale netwerk.
Een zekere binding met de fysieke omgeving zien we ook in een ander opzicht. Zo beperkten de Nederlandse online verkopers van drugs en de bitcoinwisselaars in de onderzochte zaken zich vooral tot het bedienen van klanten in Nederland en andere Europese landen.
Kenmerkend voor een deel van de netwerken die zich bezighouden met het plegen van cybercrime of die zich bezighouden met traditionele criminaliteit met een vernieuwende ICT-component is dat dergelijke netwerken wat samenstelling betreft vaak een 'mix' zijn. Enerzijds gaat het om personen die hun sporen al hebben verdiend met het plegen van traditionele criminaliteit en allerlei contacten hebben in de onderwereld. Anderzijds zijn er vaak slechts weinig leden met een zekere mate van technische expertise. Met name bij high-tech netwerken spelen online forums daarom een belangrijke rol bij het vinden van facilitators die beschikken over technische expertise die bij de kernleden ontbreekt.

De logistiek van het criminele bedrijfsproces en het gebruik van ICT
Verder zijn we ingegaan op de rol die ICT speelt bij het oplossen van logistieke problemen die criminele activiteiten met zich meebrengen. Ontmoetingen en communicatie met mededaders zijn een belangrijke logistieke vereiste binnen veel criminele processen. ICT speelt daarbij een belangrijke rol, vooral door de mogelijkheden van bijvoorbeeld versleutelde communicatie, maar ook door bijvoorbeeld technische middelen die daders gebruiken om fysieke ruimten te beschermen tegen afluisteren.
Een belangrijke logistieke flessenhals bij verschillende vormen van transitcriminaliteit bestaat uit het veilig passeren van grenzen. Door de essentiële rol die ICT speelt binnen controles en afhandeling van vervoersstromen op lucht- en zeehavens, is het voor daders belangrijker geworden om toegang te hebben tot geautomatiseerde systemen, via personeel of, zoals in een zaak gebeurde, door in te breken op de desbetreffende computernetwerken. Bij het laten meeliften van goederen op bestaande vervoersstromen is de kern van deze logistieke bottleneck echter niet veranderd: om de lading te volgen en op tijd de illegale goederen uit deze legale lading te halen, moet men nog steeds zelf toegang hebben, moet men gebruikmaken van insiders of moet men deze insiders misleiden.
Voor criminele markten heeft ICT tot belangrijke innovaties geleid: vragers en aanbieders van bijvoorbeeld drugs kunnen elkaar anoniem 'ontmoeten' en, eveneens tot op zekere hoogte anoniem, transacties verrichten (vooral voor kleinere hoeveelheden). Toch zien we dat niet het gehele criminele bedrijfsproces wordt gedigitaliseerd. Naast online aspecten kennen deze criminele activiteiten nog steeds belangrijke offline aspecten (in ieder geval in ons casusmateriaal), waarvoor digitalisering geen oplossing biedt, zoals bijvoorbeeld het onderhandelen over en overdragen van grotere hoeveelheden verdovende middelen.
Bij fraude met het betalingsverkeer zien we dat door de digitalisering van het betalingsverkeer de directe dader-slachtofferconfrontatie, die kenmerkend is voor traditionele diefstal, meer indirecte vormen aanneemt, zoals 'skimmen' van creditcards, phishing, malware en andere vormen van fraude met internetbankieren. In de kern komen deze criminele activiteiten echter neer op het mensen afhandig maken van geld. Wat internet heeft veranderd, is dat veel consumenten via internet benaderd kunnen worden door cybercriminelen en dat deze cybercriminelen heel veel slachtoffers tegelijk kunnen benaderen en in principe ook kunnen afwachten wie wel en niet 'hapt' op een 'phishing-mail' of malware-aanval. Het potentiële bereik voor daders is dus veel groter geworden.
Aan de andere kant is het einde van deze criminele bedrijfsprocessen nog steeds vaak heel fysiek het cashen van geld. Het rekruteren en gebruiken van bijvoorbeeld money mules is een logistieke bottleneck en het risico van deze money mules blijft – ook door de toegenomen beveiliging en fraudedetectie – hoog. Ten slotte blijkt dat digitalisering het ook voor banken en slachtoffers gemakkelijker kan maken om beveiliging en fraudedetectie te verbeteren. In de afgelopen jaren is het schadebedrag ten gevolge van de genoemde fraudevormen sterk gedaald (althans voor zover dit blijkt uit de gepubliceerde cijfers van de Nederlandse Vereniging van Banken (NVB)).

Criminele geldstromen en het gebruik van ICT
Criminele geldstromen lijken zowel in zaken van traditionele georganiseerde criminaliteit als in gevallen van cybercrime nogal eens buiten het zicht van de opsporing te blijven. Toch genereren de dertig geanalyseerde zaken ook hier belangrijke inzichten. Zowel wat betreft consumptie van criminele inkomsten als investeringen (aangetroffen bezittingen) in de legale economie passen de uitkomsten op hoofdlijnen bij eerder gevonden resultaten. Bij die investeringen gaat het vaak om huizen

en ander onroerend goed en (dekmantel)bedrijven, waarbij deze bedrijven vaak worden gebruikt bij de criminele activiteiten van daders. De analyses laten hier geen grote verschillen zien tussen traditionele en cybercriminaliteit.
Bij het afschermen van criminele inkomsten zien we wel belangrijke verschillen tussen traditionele georganiseerde criminaliteit enerzijds en ICT-gerelateerde criminaliteit anderzijds. Binnen de 23 zaken op het terrein van traditionele georganiseerde criminaliteit zien we de verschillende witwasmodaliteiten zoals die in de vorige monitorronde zijn beschreven: het verbergen en verplaatsen van contant geld, het afgeschermd consumeren van criminele inkomsten in Nederland en meer complexe witwasconstructies zoals het fingeren van legale inkomsten uit dienstbetrekking of bedrijf. Het gebruik van cryptovaluta hebben we in deze 23 zaken niet gezien. Al met al zijn de traditionele zaken van georganiseerde criminaliteit ook wat betreft witwasactiviteiten dus nog steeds vrij 'traditioneel'.
De meer klassieke witwasmethoden kwamen we ook tegen in de zaken met een ICT-component. Belangrijker zijn hier echter de relatief nieuwe, financiële modi operandi die deze zaken kenmerken. Bij ICT-gerelateerde criminaliteit zijn de opbrengsten, in tegenstelling tot veel vormen van traditionele georganiseerde criminaliteit, vaak digitaal van aard. Verkopers van drugs die handelen op een darknet market ontvangen de opbrengsten van hun handelswaar vaak in een cryptomunteenheid zoals bitcoin. Plegers van phishing- en malware-aanvallen verkrijgen door hun fraudeleuze handelingen de controle over het online betalingsverkeer van hun slachtoffers, dat in digitale euro's verloopt. In de cyberzaken die we hebben geanalyseerd werden deze euro's vervolgens contant opgenomen en/of ze werden gebruikt voor de aanschaf van onder andere bitcoins, webmoney, vouchers en/of goederen. Ten behoeve van de criminele geldstromen in ICT-gerelateerde criminaliteit wordt verder gebruikgemaakt van 'nieuwe' soorten van dienstverlening, zoals bitcoin 'mixing services', money mules en bitcoinwisselaars.
Opvallend blijft echter ook de prominente rol van contant geld binnen de onderzochte zaken, zowel bij traditionele georganiseerde criminaliteit als cybercriminaliteit. Daders verbergen contant geld, zorgen dat contant geld in andere landen terechtkomt, wisselen digitale valuta (bitcoins of euro's) om in contant geld en kopen kostbare goederen en diensten met contant geld (afgeschermde consumptie). Vooral bij het verplaatsen, omwisselen en het besteden van contant geld, spelen verschillende actoren uit de omgeving van daders, al dan niet bewust, een belangrijke rol.

Synthese
ICT biedt daders dus nieuwe mogelijkheden op het terrein van criminele samenwerking, met betrekking tot logistieke aspecten van het criminele bedrijfsproces en wat betreft criminele geldstromen. Zo verlegt ICT de horizon voor daders die zoeken naar slachtoffers, mededaders, hulpmiddelen of klanten. ICT leidt zo tot nieuwe werkwijzen en nieuwe vormen van criminele samenwerking. Ook aanbieders en consumenten van drugs vinden op het dark web marktplaatsen die in beginsel vrij zijn van fysieke en sociale begrenzingen. Contacten in de offline wereld en hechte sociale verbanden lijken daardoor minder belangrijk, omdat het gemakkelijker is om mensen, expertise en hulpmiddelen te vinden.
Verder zien we dat daders dankbaar gebruikmaken van mogelijkheden om afgeschermd met elkaar te communiceren. Vrij toegankelijke hardware en software voor afgeschermde communicatie bieden een belangrijk voordeel voor daders die onderling zaken willen afstemmen zonder dat de politie dit kan onderscheppen (in hun perceptie). Ten slotte vormen ook door ICT mogelijk gemaakte voorzieningen als cryptovaluta een belangrijke innovatie. Cryptovaluta kennen een zekere mate van anonimiteit en zijn het betaalmiddel op darknet markets. Samen met de TOR-

netwerken waarop darknet markets functioneren maakt een munteenheid zoals bitcoin het mogelijk voor kopers en verkopers van illegale goederen en diensten om min of meer anoniem transacties aan te gaan.
De mogelijkheden die ICT biedt worden dus ook daadwerkelijk gebruikt en daardoor verandert de werkwijze van daders tot op zekere hoogte.

Aan de andere kant is, in ieder geval in ons casusmateriaal, traditionele georganiseerde criminaliteit nog steeds vrij 'traditioneel'. Zo zijn er geen aanwijzingen die duiden op een fundamentele verandering van de manier waarop offline opererende criminele netwerken zich ontwikkelen. Ook het logistieke proces van bijvoorbeeld drugssmokkel lijkt in ons casusmateriaal op hoofdlijnen niet wezenlijk te zijn veranderd. Verder zagen we het gebruik van bitcoins alleen in zaken van cybercrime en online drugssmokkel (en in een witwaszaak die zich richtte op bitcoinwisselaars). Deze financiële innovatie ontbrak dus in de andere zaken. Mogelijk is het voor veel daders niet nodig om via ICT hun werkwijze drastisch te veranderen.
Interessanter is dat wanneer we naar cybercrimezaken kijken er parallellen blijken te zijn met meer traditionele georganiseerde criminaliteit. Zo zien we dat ook daders in cybercrimezaken en andere zaken met een belangrijke ICT-component een zekere lokale inbedding kennen. Dat dit zo is bij traditionele offline georganiseerde criminaliteit, wisten we al uit eerdere rapportages op basis van de Monitor Georganiseerde Criminaliteit. Bij andere casussen is deze lokale inbedding minder voor de hand liggend. Een deel van de hoofddaders in cybercrimezaken lijkt dezelfde fysieke leefomgeving te delen en ook katvangers worden nogal eens gevonden in de naaste omgeving. De bronnen van sociaal kapitaal die worden benut voor participatie in georganiseerde criminaliteit, bestaan dus ook in deze zaken voor een belangrijk deel uit offline interacties.
Verder lijken ook darknet markets, ondanks dat online marktplaatsen in theorie niet worden gehinderd door grenzen, een belangrijke lokale (regionale), fysieke component te hebben. Bij de online marktplaats die wij bestudeerden bleek bijvoorbeeld een deel van de transacties, vooral die van grotere omvang, via fysieke ontmoetingen te worden afgehandeld. Verder bleken bij de transacties die via de marktplaats verliepen koper en verkoper nogal eens in nabijgelegen landen te wonen. Mogelijk worden door de desbetreffende daders de risico's van postzendingen als te hoog ingeschat wanneer het om, respectievelijk, grotere partijen en afstanden gaat.
Ten slotte zijn sommige daders in ICT-gerelateerde zaken in belangrijke mate afhankelijk van lokale voorzieningen, zoals postbedrijven voor online drugs verkopers en publieke plaatsen met wifi-toegang (zoals horecagelegenheden) voor bitcoinwisselaars.
Behalve de lokale dimensie is zoals gezegd de voorkeur van daders voor contant geld een andere belangrijke overeenkomst tussen traditionele en ICT-gerelateerde georganiseerde criminaliteit. Voor traditionele vormen van georganiseerde criminaliteit is de dominantie van contant geld een bekend gegeven, maar ook daders die online opereren geven er de voorkeur aan om in ieder geval een deel van hun digitale opbrengsten, euro's of bitcoins, om te wisselen voor contant geld.

Reikwijdte van het onderzoek
Het empirisch materiaal van de Monitor Georganiseerde Criminaliteit bestaat uit, vaak omvangrijke, opsporingsonderzoeken op het terrein van de georganiseerde criminaliteit. Voor deze vijfde ronde van de monitor zijn 30 opsporingsonderzoeken geanalyseerd. Opsporingsdossiers zijn dus de belangrijkste databron binnen de monitor. Deze opsporingsdossiers bieden een schat aan informatie en zijn van grote waarde voor wetenschappelijk onderzoek naar georganiseerde criminaliteit.

Iedereen die zich wil verdiepen in criminele fenomenen, wordt geconfronteerd met de 'muren van stilzwijgen' die criminele activiteiten omringen, vooral wanneer het gaat om georganiseerde criminaliteit (Van de Bunt, 2007, 2010). Alleen de politie heeft verregaande bevoegdheden om, via de inzet van opsporingsmethoden, door deze 'muren' heen te breken. Een onderzoeker die toegang heeft tot opsporingsdossiers profiteert mee van deze exclusieve bevoegdheden en kan zo een eveneens exclusief inzicht krijgen in de activiteiten van daders of in de wijze waarop zij zich tot elkaar en hun omgeving verhouden. Bronnen als het verslag van een undercoveroperatie, een afgeluisterd telefoongesprek of een afgeluisterde ontmoeting tussen verdachten, kunnen een onvervangbare inkijk geven in hoe daders te werk gaan (Kruisbergen, 2017, p. 184; Kleemans et al., 1998; Kruisbergen et.al., 2012). De uitgebreide zaaksverslagen die van die opsporingsonderzoeken zijn gemaakt, bieden inzicht in de *aard* van de georganiseerde criminaliteit in Nederland. Het materiaal leent zich echter niet voor het doen van kwantitatieve uitspraken. Uitspraken over de omvang van criminele activiteiten of de omvang van de schade als gevolg van die activiteiten, liggen buiten het bereik van dit onderzoek.[2]
Verder geldt voor de bestudeerde opsporingsonderzoeken dat zij vallen binnen de door ons gehanteerde begripsomschrijving van georganiseerde criminaliteit. Dit betekent onder meer dat (cyber)delicten met een terroristische, politieke, activistische of vandalistische achtergrond, maar ook delicten waarbij persoonlijk seksueel genot op de voorgrond staat, niet worden meegenomen. Mede om deze reden zijn in deze ronde bijvoorbeeld geen zaken meegenomen die zich richten op DDoS-aanvallen. Dat betekent niet dat een DDoS-aanval geen ernstig misdrijf met grote schadelijke gevolgen is. Praktijkvoorbeelden laten zien dat een DDoS-aanval, of die nu wordt uitgevoerd door bijvoorbeeld een eenling, een groep criminelen of een statelijke mogendheid, juist veel schade kan aanrichten.
Ook geldt dat alleen gevallen van georganiseerde criminaliteit zijn meegenomen die door Nederlandse autoriteiten zijn opgespoord en vervolgd. Ten slotte geldt dat de bestudeerde opsporingsonderzoeken alleen betrekking hebben op modi operandi zoals die zich in het verleden hebben voorgedaan (beide laatstgenoemde beperkingen gelden voor alle Nederlandse opsporingsonderzoeken; zie ook paragraaf 1.3).
Het rijke inzicht dat opsporingsdossiers biedt, kent dus ook beperkingen. Activiteiten en daders die niet in Nederlandse opsporingsdossiers terechtkomen, blijven ook buiten beeld van de onderzoeker. Deze beperking werkt voor cybercrime mogelijk sterker uit dan voor andere typen van (georganiseerde) criminaliteit. Juist bij cybercrime kan een modus operandi of een dadergroepering een sterke internationale component hebben, wat de opsporing en vervolging kan bemoeilijken. Ook een lager bewustzijn van slachtofferschap van cybercrime en een lagere aangiftebereidheid zouden het zicht op cybercrime kunnen bemoeilijken (Schuppers et al., 2016, p. 10). Bovendien zijn juist bij cybercrime lang niet alle door politie en justitie gepleegde interventies zichtbaar in individuele opsporingsdossiers. Zo is het online verzamelen van informatie of het online verstoren of voorkomen van criminaliteit, in zekere zin veel laagdrempeliger dan vergelijkbaar optreden in de offline wereld. Juist bij cybercrime zou daarom bijvoorbeeld voor verstorend optreden gekozen kunnen worden, wat vervolgens niet tot een 'zaak' in traditionele zin hoeft te leiden. Voor een goed wetenschappelijk en beleidsmatig zicht op cybercrime is het daarom van belang om behalve afgeronde, succesvolle opsporingsonderzoeken, ook andere bronnen te ontsluiten. Hierbij kan onder andere worden gedacht aan informatie-

[2] Dergelijke uitspraken vallen wel binnen de doelstelling van het *Nationaal dreigingsbeeld Georganiseerde criminaliteit* (Boerman et al., 2017).

verzameling rondom verstorende interventies tegen een darknet market of de inzet van een technisch, analytisch instrument als een *webcrawler*.

Mogelijke implicaties voor beleid

Regulering van cryptovaluta en aanverwante diensten?
Nieuwe criminele werkwijzen, en de opsporing daarvan, kunnen de vraag oproepen of bestaande wet- en regelgeving voldoende is toegerust voor de nieuwe situatie. Dit geldt bijvoorbeeld voor het criminele gebruik van cryptovaluta. Bitcoins en andere varianten zijn op dit moment grotendeels ongereguleerd. In dit rapport en in eerdere publicaties is beschreven hoe daders gebruikmaken van deze innovatie. Niet alleen de cryptovaluta zelf, ook aanverwante diensten vallen op dit moment grotendeels buiten financiële regulering en toezicht. Daardoor zijn bitcoinexchangers bijvoorbeeld ook niet meldplichtig in het kader van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft).
Regulering en toezicht kunnen handvatten bieden om witwassen via cryptovaluta tegen te gaan. Zo zouden bijvoorbeeld (Nederlandse) online wisselkantoren, zoals de bitcoinexchangers, onder het bereik van Nederlandse toezichthouders kunnen worden gebracht. Dit kan de witwasmogelijkheden via cryptovaluta verkleinen. Aan de andere kant zou regulering vanuit het perspectief van anti-witwasbeleid ook nadelen kunnen hebben. Op dit moment lijkt de acceptatie van cryptovaluta in de reguliere economie nog laag. Regulering zou bij kunnen dragen aan 'normalisering' van cryptovaluta en een hogere graad van acceptatie van cryptovaluta als betaalmiddel, waarmee de mogelijkheden om op criminele wijze verdiende cryptovaluta in de reguliere economie om te zetten – wit te wassen – juist worden vergroot (zie ook Oerlemans et al., 2016).

Opsporing
Inherente kwetsbaarheid technologie
De afschermingsmogelijkheden die ICT daders biedt en het internationale aspect dat sommige werkwijzen op het terrein van ICT-gerelateerde criminaliteit kenmerkt, bemoeilijken de opsporing. Maar ook cybercriminelen en daders die ICT gebruiken om hun criminele activiteiten uit te voeren, laten sporen na en/of zijn op een andere manier kwetsbaar voor tegenmaatregelen (zie ook Odinot et al., 2017; Oerlemans et al., 2016).
Ten eerste kent anonimiteit op internet ook beperkingen. Zo wordt internetverkeer vaak op de een of andere manier geregistreerd, ook al zijn die registraties niet altijd (direct) voor derden toegankelijk. De transactiegeschiedenis van bitcoins wordt bijvoorbeeld vastgelegd, waarbij wel geldt dat gebruik van een 'mixing service' het zicht kan ontnemen op de herkomst van een bitcoin. Een belemmering voor de opsporing is verder dat achter specifieke bitcoinadressen vaak pseudoniemen schuilgaan. Echter, door transactiegegevens te analyseren en te koppelen aan andere bronnen, en vanwege niet-optimaal gedrag van gebruikers, kunnen bepaalde transacties toch naar personen worden herleid (Meiklejohn et al., 2013; Ron & Shamir, 2013; Oerlemans et al., 2016). Een gebrek aan anonimiteit, kortom, zit soms tot op zekere hoogte ingebakken in de gebruikte technologie.
Maar, ten tweede, ook technologie waarvan wordt verondersteld dat deze wel 'waterdicht' is, biedt daders geen garantie op afscherming van politie en justitie. Dit blijkt bijvoorbeeld uit het opsporingsonderzoek tegen *Ennetcom*. Ennetcom was een belangrijke aanbieder van versleutelde communicatie, waarvan, in ieder geval volgens het Openbaar Ministerie (OM), veelvuldig gebruik werd gemaakt door criminelen. In 2016 kreeg het OM de beschikking over enorme hoeveelheden data van de

server waarvan Ennetcom gebruikmaakte. Klanten van Ennetcom gebruikten aangepaste smartphones (*Blackberries*) die waren voorzien van encryptiesoftware (*Pretty Good Privacy*). Deze software stelt bezitters van deze smartphones in staat om onderling afgeschermd te communiceren. Met het opsporingsonderzoek, waarbij onder meer een kopie is gemaakt van de server, kregen politie en justitie echter de 'sleutel' in handen tot de berichten die via Ennetcom werden verstuurd. Volgens politie en justitie zijn, via de ontcijferde informatie van de server, miljoenen berichten toegankelijk gemaakt, berichten die voorheen voor de opsporing verborgen bleven. De op deze wijze verkregen informatie zou van nut zijn voor een groot aantal opsporingsonderzoeken naar zware misdrijven.
Ten derde kunnen dezelfde kenmerken die een technologie aantrekkelijk maken voor daders, in sommige gevallen ook de politie handvatten bieden om die daders aan te pakken. Een sprekend voorbeeld vormt hier de darknet market *Hansa*. Deze ondergrondse marktplaats, waarop drugs werd verhandeld, is via een internationale operatie ontmanteld. Medio 2017 werden niet alleen de beheerders van deze marktplaats aangehouden, maar werden ook de servers in beslag genomen. Een kopie van de marktplaats werd vervolgens via Nederlandse servers voortgezet, onder controle van de Nederlandse politie en het OM. Op deze manier zijn grote aantallen transacties én kopers en verkopers in beeld gebracht. Het beheer van een dergelijke onlinemarktplaats door de politie zou als een undercoveroperatie kunnen worden beschouwd. Ook ons eigen casusmateriaal biedt een voorbeeld van een undercoveroperatie tegen daders die op een darknet market actief waren. De opkomst van internet biedt dus niet alleen daders nieuwe mogelijkheden. De (ogenschijnlijke) anonimiteit waarmee op darknet markets kan worden gehandeld en die deze marktplaatsen aantrekkelijk maakt, biedt ook opsporingsambtenaren immers een goede dekmantel. Daardoor zijn ook daders die online opereren kwetsbaar voor een, oorspronkelijk voor de offline wereld ontwikkelde opsporingsmethode als een undercoveroperatie.

Raakvlakken online-offline
ICT is een essentieel onderdeel van de huidige samenleving. Ook in veel vormen van (georganiseerde) criminaliteit speelt ICT op zijn minst enige rol, al was het maar omdat daders gebruikmaken van moderne communicatietechnologie. Kennis van ICT en daarop toegesneden opsporingsinstrumenten is daarom ook belangrijk voor de opsporing van traditionele georganiseerde criminaliteit. Het grote raakvlak tussen de online en offline wereld werkt echter twee kanten uit. In deze studie beschreven we dat ook in cybercrimezaken en andere zaken met een duidelijke ICT-component de werkwijze van daders gekenmerkt wordt door een zekere mate van lokale inbedding. Ook vanuit het perspectief van deze daders is de wereld van 'traditionele' georganiseerde criminaliteit niet strikt gescheiden van cybercrime. Ook bij ICT-gerelateerde criminaliteit is het immers vaak zo dat een of meerdere essentiële schakels van het criminele bedrijfsproces zich afspelen in de fysieke, offline wereld. We zagen bijvoorbeeld hoofddaders die dezelfde sociale, lokale herkomst delen, daders die katvangers rekruteren in hun lokale omgeving, bitcoinwisselaars die hun klanten bedienen op met wifi toegeruste publieke plekken en daders die drugs verhandelen via darknet markets die mede afhankelijk zijn van reguliere postbedrijven. Nieuwe verschijningsvormen van criminaliteit vereisen daarom niet alleen nieuwe bevoegdheden of specifieke, technische opsporingsinstrumenten, maar bieden ook veel aanknopingspunten voor meer klassieke methoden.

Financiële opsporing
Beleidsmatig wordt al geruime tijd ingezet op wat een financiële aanpak van georganiseerde criminaliteit kan worden genoemd. Dat omvat het financieel rechercheren, het voorkomen en bestrijden van witwassen en het afpakken van criminele verdiensten. Het ligt het voor de hand dat deze aanpak ook bij ICT-gerelateerde criminaliteit wordt gehanteerd. Ten eerste is het zo dat ook daders die online opereren vaak gemotiveerd zijn door financieel gewin. Ten tweede is het zo dat bij verschillende vormen van ICT-gerelateerde criminaliteit met name het incasseren of omwisselen van de opbrengsten een fase in het criminele bedrijfsproces is waarin daders kwetsbaar zijn, omdat ze dan direct of indirect in contact komen met de reguliere omgeving. Dit geldt voor daders van bijvoorbeeld banking malware en phishing die hun digitale euro's willen omwisselen in contanten. Het geldt ook voor de drugshandelaren die hun op het darknet verdiende cryptovaluta willen omruilen voor contante euro's. Contant geld speelt kortom nog steeds een hoofdrol in de criminele wereld, ook wanneer de criminelen zich met online activiteiten bezighouden.
Ten derde kan een financiële insteek bij de opsporing nieuw zicht bieden op bepaalde aspecten van criminele samenwerkingsverbanden. Zo kan het volgen van een geldstroom leiden tot nieuwe verdachten en kan informatie over de verdeling van criminele inkomsten duidelijk maken welke daders cruciale schakels zijn in criminele netwerken. Een financiële invalshoek kan belangrijke leeropbrengsten genereren, zeker gezien het feit dat er nog relatief weinig bekend is over het gebruik van specifieke ICT-gerelateerde witwasmogelijkheden en de ontwikkelingen op dit terrein elkaar snel opvolgen.

Situationele aanpak: drempels opwerpen
In de monitorrapportages die tot nu zijn verschenen komt steeds naar voren hoe sterk georganiseerde criminaliteit verweven is met haar sociale omgeving. In de situationele benadering – en aanpak – van georganiseerde criminaliteit wordt de nadruk niet gelegd op de hoofddaders zelf, maar wordt in plaats daarvan de aandacht gevestigd op de factoren die deze criminaliteit mogelijk maken. Ook bij de verschillende ICT-gerelateerde vormen van georganiseerde criminaliteit die in dit rapport zijn besproken, maken daders gebruik van personen of voorzieningen uit hun omgeving, bijvoorbeeld van banken. Zo vinden daders van bijvoorbeeld phishing- of banking-malware-aanvallen hun slachtoffers onder rekeninghouders bij reguliere banken. Banken spelen dan ook een cruciale rol in de preventie en bestrijding van verschillende vormen van criminaliteit. Banken zijn zich daarvan bewust en werken bijvoorbeeld samen in het Electronic Crimes Task Force (ECTF), een samenwerkingsverband tussen banken, politie en het OM. De gepubliceerde fraude gepleegd via het internetbankieren en via skimmen is de afgelopen jaren zeer sterk gedaald, hetgeen waarschijnlijk mede het gevolg is van de door banken in gang gezette maatregelen en campagnes. Maar ook bij de bestrijding van witwassen spelen banken een belangrijke rol. Bankrekeningen worden gebruikt voor het doorsluizen en cashen van criminele opbrengsten en voor het omwisselen van cryptovaluta in reguliere valuta. Banken kunnen meldingen doen wanneer bij bepaalde rekeningen opvallende stortingen en opnames plaatsvinden, wat kan wijzen op bijvoorbeeld het cashen van fraudegeld door money mules of omwisselacties van bijvoorbeeld bitcoinwisselaars. Deze meldingen doen zij ook – zoals ook uit ons casusmateriaal blijkt – wat de aanpak van deze vormen van criminaliteit ten goede komt. Dat het optreden van banken ertoe doet, blijkt uit het sterk afgenomen schadebedrag als gevolg van fraude met internetbankieren, maar ook uit opsporingsonderzoeken naar witwassen die opstarten na een melding door een bank. Gezien de centrale positie die banken innemen en de dynamiek in de modi operandi van daders, blijven ban-

ken een belangrijke rol spelen in de preventie en bestrijding van georganiseerde criminaliteit.
Banken, money mules (en andere manieren om geld weg te sluizen) en (fysieke) cryptowisseldiensten zijn cruciaal voor bepaalde delicttypen. De twee laatstgenoemde actoren kunnen hun rol spelen omdat ook in de wereld van gedigitaliseerde criminaliteit veel daders een voorkeur hebben voor contant geld. Op dat punt kan de aanpak meeliften met generieke maatregelen tegen contante geldstromen binnen de georganiseerde criminaliteit. Het casusmateriaal geeft aanleiding te vermoeden dat nog steeds veel, op criminele wijze verdiend geld in contante vorm zijn weg vindt in de reguliere economie. Daarbij geldt dat daders, bewust of onbewust, worden gefaciliteerd doordat zij bij sommige aanbieders kostbare goederen of diensten zonder problemen contant kunnen afrekenen (afgeschermde consumptie). Vanwege de dominante rol die contant geld speelt in offline én online criminaliteit, kan het bemoeilijken van bijvoorbeeld afgeschermde consumptie een effectieve bijdrage leveren aan de bestrijding van criminele geldstromen.
Andere voorbeelden van diensten en dienstverleners die bewust of onbewust een belangrijke rol spelen in de werkwijze van daders, zijn postbedrijven, 'mixing services' voor cryptovaluta, aanbieders van apparatuur of software voor afgeschermde communicatie, en online ontmoetingsplaatsen waarop technische expertise wordt gevonden die wordt ingezet bij criminele activiteiten. Het in kaart brengen van deze en andere voor daders cruciale diensten, is niet alleen van belang voor de preventie van georganiseerde criminaliteit maar ook voor de opsporing. Net als bij traditionele georganiseerde criminaliteit is bij de opsporing van ICT-gerelateerde criminaliteit de hoeveelheid potentiële verdachten waar de opsporing haar instrumenten op kan richten immers groot en de capaciteit daarvoor beperkt. Er moeten dus keuzes worden gemaakt. Een gerichte opsporing van facilitators kan criminele processen (tijdelijk) verstoren. Het zendt bovendien een boodschap uit aan hen die soortgelijke diensten verlenen en die zich, zeker wanneer het gaat om relatief nieuwe soorten van dienstverlening, beroepen op onwetendheid omtrent de bedoelingen van hun klanten.

Onze analyse van opsporingsonderzoeken laat zien dat ook ICT-gerelateerde criminaliteit duidelijke raakvlakken heeft met de offline wereld en, net als traditionele georganiseerde criminaliteit, mede afhankelijk is van de reguliere omgeving. Dit toont enerzijds aan dat het onderscheid tussen cybercrime en traditionele georganiseerde criminaliteit minder scherp is dan soms wordt gedacht. Anderzijds wijst het erop dat behalve technische instrumenten ook meer traditionele opsporingsmethoden en een situationele aanpak goede mogelijkheden bieden bij de aanpak van ICT-gerelateerde criminaliteit.

Literatuur

Boerman, F., Grapendaal, M., Nieuwenhuis, F., & Stoffers, E. (2017). *Nationaal dreigingsbeeld 2017: Georganiseerde criminaliteit*. Zoetermeer: Nationale Politie, Landelijke Eenheid, Dienst Landelijke Informatieorganisatie.

Bunt, H.G. van de (2007). Muren van stilzwijgen. In H.G. van de Bunt, P. Spierenburg & R. van Swaaningen (red.), *Drie perspectieven op sociale controle* (pp. 133-136). Den Haag: Boom Juridische Uitgevers.

Bunt, H.G. van de (2010). Walls of secrecy and silence: The Madoff case and cartels in the construction industry. *Criminology and Public Policy*, *9*(3), 435-453.

Bunt, H.G. van de, & Kleemans, E.R., m.m.v. Poot, C.J. de, Bokhorst, R.J., Huikeshoven, M., Kouwenberg, R.F., Nassou, M. van, & Staring, R. (2007). *Georgani-*

seerde criminaliteit in Nederland: Derde rapportage op basis van de Monitor Georganiseerde Criminaliteit. Den Haag: Boom Juridische uitgevers. Onderzoek en beleid 252.

Kleemans, E.R., Berg, E.A.I.M. van den, & Bunt, H.G. van de, m.m.v. Brouwers, M., Kouwenberg, R.F., & Paulides, G. (1998). *Georganiseerde criminaliteit in Nederland: Rapportage op basis van de WODC-monitor*. Den Haag: WODC. Onderzoek en beleid 173.

Kleemans, E.R., Brienen, M.E.I., & Bunt, H.G. van de, m.m.v. Kouwenberg, R.F., Paulides, G., & Barensen, J. (2002). *Georganiseerde criminaliteit in Nederland: Tweede rapportage op basis van de WODC-monitor*. Den Haag: Boom Juridische uitgevers. Onderzoek en beleid 198.

Kruisbergen, E.W. (2017). *Combating organized crime: A study on undercover policing and the follow-the-money strategy*. Amsterdam: Vrije Universiteit.

Kruisbergen, E.W., Bunt, H.G. van de, & Kleemans, E.R. (2012). *Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit*. Den Haag: Boom Lemma. Onderzoek en beleid 306.

Meiklejohn, S., Pomarole, M., Jordan, G. Levchenko, K., McCoy, D., Voelker, G.M., & Savage, S. (2013). *A fistful of bitcoins: Characterizing payments among men With no names*. San Diego: University of California. Geraadpleegd april 2018: http://dx.doi.org/10.1145/2504730.2504747.

Odinot, G., Verhoeven, M.A., Pool, R.L.D., & De Poot, C.J. (2017). *Organised cybercrime in the Netherlands: Empirical findings and implications for law enforcement*. Den Haag: WODC. Cahier 2017-1.

Oerlemans, J.J., Custers, B.H.M., Pool, R.L.D., & Cornelisse, R. (2016). *Cybercrime en witwassen: Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware*. Den Haag: Boom criminlogie. Onderzoek en beleid 319.

Ron, D., & Shamir, A. (2013). Quantitative analysis of the full bitcoin transaction graph. *Financial cryptography and data security*, *7859*, 6-24.

Schuppers, K. Rombouts, N., Zinn, P., & Praamstra, H. (2016). *Cybercrime en gedigitaliseerde criminaliteit: Nationaal dreigingsbeeld 2017*. Driebergen: Nationale Politie.

Wingerde, C.G. van, & Bunt, H.G. van de (2017). *Geëiste en opgelegde straffen bij de strafrechtelijke afhandeling van georganiseerde criminaliteit: Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit*. Apeldoorn: Politie & Wetenschap.

1 Inleiding

1.1 De Monitor Georganiseerde Criminaliteit

Een goed onderbouwde aanpak van de georganiseerde criminaliteit is alleen mogelijk wanneer er een gedegen inzicht bestaat in de aard van de georganiseerde criminaliteit zoals die zich in Nederland manifesteert. Het doel van de Monitor Georganiseerde Criminaliteit is het bieden van dat inzicht. Dat inzicht wordt geboden door zo veel mogelijk de kennis te benutten die wordt opgedaan tijdens omvangrijke opsporingsonderzoeken. Tijdens dergelijke onderzoeken worden vaak vergaande instrumenten ingezet, zoals telefoon- en internettaps, het afluisteren van face-to-facegesprekken, observatie, undercovertrajecten, huiszoekingen, inbeslagnames en verhoor van verdachten en getuigen. Omdat alleen de politie deze instrumenten kan inzetten en ze vaak een diepgaand beeld schetsen van de personen tegen wie ze worden gebruikt, leveren deze unieke kennis op over wat georganiseerde criminaliteit in de praktijk behelst. Wanneer deze kennis opgesloten blijft in afzonderlijke opsporingsonderzoeken, kan de bestrijding van georganiseerde criminaliteit in bredere zin er niet van profiteren. Het ontsluiten van die kennis vormt de bestaansreden van de Monitor Georganiseerde Criminaliteit (zie ook Minister van veiligheid en Justitie, 2013).[3]
De centrale probleemstelling van de monitor richt zich op de aard van de georganiseerde criminaliteit in Nederland en de ontwikkelingen die daarin zijn te onderkennen.[4] Om deze centrale vraag te beantwoorden worden grootschalige opsporingsonderzoeken bestudeerd. Dit gebeurt aan de hand van een uitgebreide aandachtspuntenlijst.[5]
De Monitor heeft geresulteerd in tientallen rapporten, artikelen in wetenschappelijke tijdschriften, boekbijdragen, presentaties en adviezen en twee proefschriften (Van Koppen, 2013; Kruisbergen, 2017). De kernpublicatie bestaat echter na iedere monitorronde uit de rapportage die naar de Tweede Kamer wordt gestuurd. Tot nu toe – tot en met de vierde ronde van de Monitor Georganiseerde Criminaliteit – betrof dat steeds één rapportage per ronde (Kleemans et al., 1998,, 2002; Van de Bunt & Kleemans, 2007; Kruisbergen et al., 2012). In die rapportages werden steeds wisselende thema's uitgediept. Om dieper op bepaalde thema's in te kunnen gaan, is ervoor gekozen om de vijfde ronde uit te laten monden in drie afzonderlijke deelrapporten. In oktober 2017 is het eerste deelrapport verschenen (Van Wingerde & Van de Bunt, 2017). Dat rapport richtte zich op de strafrechtelijke afhandeling van georganiseerde criminaliteit, met name de geëiste en opgelegde straffen. Dit tweede deelrapport staat volledig in het teken van georganiseerde criminaliteit en ICT (informatie- en communicatietechnologie).[6]

---

[3] Mede naar aanleiding van de conclusies die werden getrokken uit de Parlementaire Enquête Opsporingsmethoden, is door Minister van Justitie destijds aan de Tweede Kamer toegezegd om periodiek te rapporteren over de aard van de georganiseerde criminaliteit in Nederland en te signaleren ontwikkelingen (Ministerie van Justitie/ Ministerie van Binnenlandse Zaken, 1996). De Monitor Georganiseerde Criminaliteit is de concrete invulling van deze toezegging.

[4] Opgemerkt moet worden dat het onderzoek zich richt op de *aard* en niet op de *omvang* van de georganiseerde criminaliteit.

[5] In paragraaf 1.3 gaan we verder in op de onderzoeksvragen en de gebruikte methoden en bronnen, in bijlage 2 is de gebruikte aandachtspuntenlijst integraal opgenomen.

[6] Het derde deelrapport zal ingaan op de verwevenheid van georganiseerde criminaliteit met haar omgeving en de opsporing van georganiseerde criminaliteit.

1.2 Georganiseerde criminaliteit en ICT

Het doel van deze studie is het vergroten van het inzicht in hoe daders binnen de georganiseerde criminaliteit ICT gebruiken en welke invloed dat gebruik heeft op hun criminele bedrijfsprocessen. We richten ons daarbij niet uitsluitend op cybercrime, maar willen juist het gebruik van ICT én de consequenties daarvan verkennen voor een breder scala van soorten georganiseerde criminaliteit, dus ook 'traditionele' georganiseerde criminaliteit zoals drugssmokkel.
Het massale gebruik van internet, en meer in het algemeen de doorwerking van ICT in alle segmenten van de samenleving, brengt nieuwe mogelijkheden voor het plegen van criminaliteit met zich mee. Het internet opent nieuwe werelden, voor individuen en organisaties in het algemeen. Toch is er maar een beperkte hoeveelheid empirisch onderzoek naar hoe daders deze mogelijkheden gebruiken en de consequenties van het gebruik van ICT voor de wijze waarop daders opereren. Recentelijk is een aantal studies uitgekomen. Odinot en anderen analyseerden elf Nederlandse opsporingsonderzoeken op het terrein van cybercriminaliteit (Odinot et al., 2017).[7] Dit maakte onderdeel uit van een door de Europese Unie gefinancierd project waarin ook Duitse en Zweedse onderzoekers participeerden (Bulanova-Hristova et al., 2016). Leukfeldt en anderen deden eveneens empirisch onderzoek naar cybercriminaliteit, waarbij zij zich met name richtten op de ontstaans- en groeiprocessen en criminele mogelijkheden van cybernetwerken (Leukfeldt et al., 2017b, 2017c, 2017d). Ten slotte onderzochten Oerlemans en anderen (2016) hoe in specifieke gevallen van cybercrime, te weten banking malware- en ransomware-aanvallen, het witwassen verloopt.[8]
In ons onderzoek bouwen wij op het werk van deze (en andere) onderzoekers voort en proberen daarbij zowel verbreding als verdieping aan te brengen.
De verbreding bestaat uit het feit dat wij ons niet alleen richten op cybercrimezaken. We onderzoeken het gebruik van ICT en de gevolgen daarvan binnen de georganiseerde criminaliteit in bredere zin. Ons empirisch materiaal bestaat uit de dertig zaken uit de vijfde ronde van de Monitor Georganiseerde Criminaliteit. Deze zaken bevatten voorbeelden van cybercrime (waarbij een aantal zaken ook in de studie van Odinot en anderen is meegenomen), maar ook opsporingsonderzoeken naar meer traditionele vormen van georganiseerde criminaliteit, zoals drugshandel en -productie, mensenhandel, fraude en witwassen. De verdieping in ons onderzoek brengen we aan door het gebruik van ICT en de consequenties daarvan te analyseren in relatie tot drie essentiële aspecten van criminele bedrijfsprocessen: criminele samenwerking, logistiek en criminele geldstromen. Dit werken we in paragraaf 1.3 verder uit.

1.3 Onderzoeksopzet

Van oudsher richt de monitor zich op de aard van de georganiseerde criminaliteit in Nederland en de ontwikkelingen die daarin zijn te onderkennen. Zoals zojuist is toegelicht mondt de vijfde ronde van de Monitor Georganiseerde Criminaliteit uit in drie deelrapporten. Daarbij wordt de algemene probleemstelling vertaald naar een meer toegespitste vraagstelling op het desbetreffende deelthema. Voor het thema georganiseerde criminaliteit en ICT wordt deze vraagstelling hieronder uitgewerkt.

---

[7] De selectie van zaken bij dat project viel voor een deel samen met de selectie van zaken voor de Monitor Georganiseerde Criminaliteit. Vijf zaken op het terrein van cybercrime/ICT-gerelateerde georganiseerde criminaliteit zijn dan ook voor beide onderzoeksprojecten geanalyseerd.

[8] Dit is geen volledig overzicht. In hoofdstuk 2, 3 en 4 wordt de bestaande literatuur uitvoeriger besproken.

1.3.1 Probleemstelling en afbakening van het onderzoek

Probleemstelling
De probleemstelling van deze deelstudie luidt:

Hoe gebruiken dadergroeperingen in de georganiseerde criminaliteit ICT en welke gevolgen heeft dit voor de wijze waarop zij opereren?

We spitsen de probleemstelling toe op drie deelthema's, die hieronder worden geïntroduceerd:
- het gebruik van ICT in relatie tot het ontstaan en groeien van criminele samenwerkingsverbanden;
- het gebruik van ICT in relatie tot de logistieke keten van criminele processen;
- het gebruik van ICT in relatie tot criminele geldstromen.

Het gebruik van internet en ICT in meer brede zin roept in relatie tot georganiseerde criminaliteit verschillende interessante vragen op. Dit geldt des te meer wanneer nieuwe vormen van criminaliteit zoals cybercrime, of het gebruik van nieuwe technologie in traditionele georganiseerde criminaliteit, in verband wordt gebracht met bestaande kennis, concepten en theorievorming op het terrein van de georganiseerde criminaliteit.[9]
Zo is het een interessante vraag wat de komst van internet betekent voor de wijze waarop *criminele samenwerkingsverbanden* ontstaan en zich ontwikkelen. In eerdere rapporten van de Monitor Georganiseerde Criminaliteit en in andere studies is uitvoerig het belang van sociaal kapitaal beschreven voor participatie en succes in de georganiseerde criminaliteit; om succesvol te kunnen zijn in de georganiseerde criminaliteit moet je de juiste mensen kennen (producenten, afnemers, facilitators etc.). Hierbij ging het steeds om menselijke relaties in de offline wereld. Nu heeft de komst van internet, in ieder geval in beginsel, een sterk grensverleggend effect. Fysieke en andere grenzen hoeven geen belemmering meer te vormen om in contact te komen met personen, personen die wellicht zeer capabel zijn op een deelterrein van een crimineel bedrijfsproces. Wordt met andere woorden het belang van sociaal kapitaal, 'de juiste mensen kennen', langzamerhand kleiner ten gunste van 'je weg kennen op het (dark) web' (zie ook Lavorgna, 2013; Przepiorka et al., 2017)? En verschillen de instroom- en doorstroommechanismen die een rol spelen bij 'cyberdaders' van de mechanismen die van belang zijn bij de algemene daderpopulatie?[10]
Een ander interessant vraagstuk betreft de rol die ICT speelt in de *logistiek van georganiseerde criminaliteit*. Iedere vorm van georganiseerde criminaliteit bestaat uit een aantal stappen die moeten worden gezet om een bepaalde criminele activiteit tot stand te brengen (Sieber & Bögel, 1993; Cornish & Clarke, 2002; zie ook Kleemans, 2014). Zo moeten voor internationale drugshandel eerst drugs worden geproduceerd (of van een producent worden gekocht), vervolgens moeten de drugs worden vervoerd naar een afzetgebied en moet de handelswaar, na verder vervoer

[9] Zie ook de onderzoeksvragen die zijn voorgesteld door Kruisbergen (Töttel et al., 2016, p. 28-30) en Leukfeldt (2017).

[10] Verder is in iedere ronde van de Monitor Georganiseerde Criminaliteit het belang van facilitators naar voren gekomen, personen die specifieke diensten verlenen aan dadergroeperingen en een belangrijke schakel kunnen vormen binnen criminele netwerken. Brengt de komst van internet nieuwe facilitators met zich mee (zie Odinot et al., 2017; Bijlenga & Kleemans, 2017) en zo ja welke zijn dat? Ook zijn er over de daders zelf verschillende vragen te formuleren. Brengen nieuwe mogelijkheden voor criminaliteit ook nieuwe soorten daders met zich mee, of zien we eerder dat de *usual suspects* nieuwe technieken toepassen?

en opslag en eventuele bewerking, bij de afnemer terechtkomen, waarbij iedere stap weer uit deelstappen bestaat. Daarbij gaat het niet alleen om het verkrijgen en/of aan de man brengen van goederen en diensten en vervoer en opslag. Ook communicatie tussen daders, om activiteiten af te stemmen bijvoorbeeld (aankomsttijden, routes, locaties, prijzen, etc.), is vaak een vereiste om het criminele proces tot een goed einde te brengen. Iedere soort georganiseerde criminaliteit kan zo worden beschreven als een logistiek proces, met specifieke logistieke opgaven of *bottle necks*. Op welke wijze maken daders gebruik van ICT om deze flessenhalzen op te lossen, en brengt het gebruik van ICT mogelijk nieuwe flessenhalzen met zich mee?
Een specifieke 'flessenhals' die bij iedere succesvolle vorm van georganiseerde criminaliteit een rol speelt, is het *beheer van crimineel verworven geld*. Daders hopen met hun activiteiten veel geld te verdienen. Criminele verdiensten, zeker wanneer ze omvangrijk zijn, brengen echter ook problemen met zich mee. Daders doen er immers verstandig aan die verdiensten, én het uitgeven ervan, buiten het zicht van de autoriteiten te houden. ICT brengt ook op dit punt nieuwe mogelijkheden met zich mee. Wat valt er bijvoorbeeld te zeggen over het gebruik voor witwasdoeleinden van nieuwe betaalfaciliteiten zoals *bitcoin* (en andere cryptovaluta) en *vouchers* en/of *prepaidkaarten*? Deze mogelijkheden kunnen niet alleen door daders worden gebruikt die actief zijn in cybercriminaliteit, maar kunnen ook worden benut door daders die zich met meer traditionele activiteiten bezighouden. Zo kan een dader die zich met offline drugshandel bezighoudt ervoor kiezen zijn criminele verdiensten in bitcoins om te zetten, bijvoorbeeld omdat hij denkt dat die verdiensten daarmee uit zicht blijven of omdat hij hoopt op een koersstijging.
In dit rapport zullen we de bovengenoemde deelthema's niet uitputtend of 'definitief' kunnen behandelen. Wel hopen we, voortbouwend op eerder onderzoek en met eigen analyses van empirisch materiaal, bij te dragen aan een groter inzicht in de wijze waarop ICT door daders in hun criminele activiteiten wordt gebruikt.

Afbakening
Hieronder lichten we toe hoe we in dit rapport omgaan met de begrippen georganiseerde criminaliteit, ICT en cybercrime.
Wat betreft *georganiseerde criminaliteit* hanteren we, evenals in de eerdere monitorrondes, de definitie zoals die door de onderzoeksgroep Fijnaut ten tijde van de Parlementaire Enquêtecommissie Opsporingsmethoden (PEO) is opgesteld (PEO, Bijlage VII, 1996, p. 24; zie Kleemans et al., 1998, p. 22-23).

'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.'

Hierbij wordt onder meer een analytisch onderscheid gemaakt tussen 'georganiseerde criminaliteit' en 'organisatiecriminaliteit' (PEO, Bijlage VII, 1996, p. 24; zie Kleemans et al., 1998, p. 22-23). Het begrip 'afscherming' wordt binnen de monitor breed opgevat, waarbij het niet alleen gaat om corruptie en (dreiging met) geweld, maar ook om het gebruik van bijvoorbeeld dekmantelfirma's, codetaal, contra-observatie en misbruik van deskundige derden zoals notarissen, advocaten en accountants (Kleemans et al., 1998, p. 22-23).

In dit rapport refereren we met *ICT* (informatie- en communicatietechnologie) vooral aan digitale vormen van gegevensopslag en –verkeer (communicatie). Wat meer concreet gaat het dan dus onder andere om computernetwerken, internet en dien-

sten die via internet toegankelijk zijn, en andere vormen van telecommunicatie. Het gaat daarbij zowel om de benodigde hard- als software. Dit is natuurlijk een nogal brede begripsomschrijving. In onze analyses van opsporingsonderzoeken spitsen we ons echter toe op gebruik van ICT door daders dat in zekere mate vernieuwend en/of geavanceerd is en/of een centrale plaats inneemt binnen de modus operandi. Dat betekent dat we geen of weinig aandacht besteden aan de meest alledaagse, 'normale' toepassingen van ICT, zoals het gebruik van onversleuteld mobiel berichtenverkeer.

Voor *cybercrime* bestaan verschillende begripsomschrijvingen. In de *Criminaliteitsbeeldanalyse Hightech Crime 2012* is de volgende, ruime definitie gebruikt: '*Cybercrime omvat elke strafbare gedraging voor de uitvoering waarvan het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is'* (Bernaards et al., 2012, p. 11). In de meest recente *Cybercrime en gedigitaliseerde criminaliteit – Nationaal Dreigingsbeeld 2017*, wordt echter een minder ruime begripsomschrijving gehanteerd: '*Bij cybercrime gaat het om criminaliteit waarbij informatie- en communicatietechnologie (ICT) zowel het middel als het doelwit is'* (Schuppers et al., 2016, p. 4; zie ook Boerman et al., 2017, p. 239). De vraag of een misdrijf zich echt tegen ICT richt of dat ICT alleen als instrument dient, wordt vaker gebruikt om cybercriminaliteit van andere gedigitaliseerde criminaliteit te onderscheiden, of om gradaties van cybercriminaliteit te duiden. Dit laatste gebeurt bijvoorbeeld bij de typologie die Wall (2005) gebruikt. Ook kunnen de technologische complexiteit (of vernieuwing) en de aangerichte schade een criterium zijn om onderscheid aan te brengen. In de rapportages van het National Dreigingsbeeld 2017 wordt onderscheid gemaakt tussen gedigitaliseerde criminaliteit, cybercrime en high tech crime (Schuppers et al., 2016, p. 4-6; Boerman et al., 2017, p. 240).
Afhankelijk van de breedte van de definitie die men kiest, vallen er verschillende delicttypen onder cybercriminaliteit of een van de genoemde deelcategorieën: phishing, ransomware, banking malware, online drugshandel via een zogenoemd darknet market, ICT-gefaciliteerde witwasoperaties, online delicten met een zedencomponent (grooming, verspreiding van kinderpornografie), DDoS-aanvallen (Distributed Denial of Service) en nog verschillende andere soorten.[11] Binnen de Monitor Georganiseerde Criminaliteit beperken we ons tot zaken waarin van criminele activiteiten in een min of meer georganiseerd verband sprake is. Ook moet het gaan om delicten die met een winstoogmerk worden gepleegd. Dit laatste betekent onder meer dat (cyber)delicten met een terroristische, politieke, activistische of vandalistische achtergrond, maar ook delicten waarbij persoonlijk seksueel genot op de voorgrond staat, niet in de monitor worden meegenomen. Mede om deze reden zijn in ieder geval deze ronde geen zaken met een zedencomponent meegenomen.[12] Hetzelfde geldt voor DDoS-aanvallen. DDoS-aanvallen worden zeker ook gebruikt om geld te verdienen, bijvoorbeeld voor afpersingsdoeleinden (Boerman et al., 2017, p. 241), maar ten tijde van de selectie van zaken zijn daar geen geschikte voorbeelden van gevonden.[13]
Gegeven deze beperking, wordt in deze rapportage in eerste instantie een brede definitie van 'cybercriminaliteit' gehanteerd. Waar dat relevant is, maken we bij de

[11] Voor zover delicttypen in de door ons bestudeerde zaken voorkomen, worden zij bij bespreking van deze zaken toegelicht.

[12] Dit betekent niet dat bijvoorbeeld het verspreiden van kinderporno niet vanuit een winstoogmerk kan plaatsvinden.

[13] DDoS-aanvallen kunnen bijvoorbeeld ook een activistische achtergrond hebben of worden geïnitieerd door statelijke actoren.

analyses in deze rapportage een meer verfijnd onderscheid tussen zaken op basis van de ICT-component. Dit lichten we in paragraaf 1.4 toe.

1.3.2 Onderzoeksmethode en gebruikte bronnen

Analyse van afgesloten opsporingsonderzoeken
De empirische kern van de Monitor Georganiseerde Criminaliteit bestaat uit de analyse van afgeronde opsporingsonderzoeken. De belangrijkste methode van onderzoek bestaat daarmee uit gevalsstudies (waarbij de opsporingsonderzoeken de 'gevallen' (*cases*) vormen). Net als bij de vierde ronde zijn deze vijfde ronde dertig opsporingsonderzoeken op het terrein van georganiseerde criminaliteit geanalyseerd. Dit betekent dat voor deze opsporingsonderzoeken het volledige opsporingsdossier is doorgenomen, doorgaans nadat een interview had plaatsgevonden met de zaaksofficier en/of de teamleider. De empirische analyses in dit deelrapport zijn gebaseerd op de genoemde dertig zaken uit de vijfde ronde. We merken daarbij op dat vijf zaken op het terrein van cybercrime/ICT-gerelateerde georganiseerde criminaliteit, ook onderdeel uitmaakten uit van de studie van Odinot et al. (2017).
De zaken die voor de monitor worden geanalyseerd vormen geen aselecte steekproef van *de* georganiseerde criminaliteit in Nederland. Ten eerste is het niet mogelijk om een aselecte steekproef te trekken omdat iedere mogelijke steekproef van gevallen van georganiseerde criminaliteit nu eenmaal afhankelijk is van de opsporing door de politie.[14] Omdat de politie noodzakelijkerwijs prioriteiten aanbrengt in de zaken die zij onderzoekswaardig acht en ook niet alle geprioriteerde zaken worden opgespoord, zijn de resultaten van opsporingsactiviteiten per definitie selectief. Ten tweede is het trekken van een aselecte steekproef ook om meer praktische redenen niet mogelijk. Er bestaat namelijk geen geschikt, centraal overzicht van alle zaken die hebben gespeeld in Nederland,[15] wat de inventarisatie van zaken dan ook tijdrovend maakt. Ten derde is het ook niet wenselijk om een aselecte steekproef van zaken te analyseren. Zou dat wel gebeuren, dan is de kans groot dat vooral zaken worden bestudeerd die relatief weinig kennis over georganiseerde criminaliteit toevoegen, bijvoorbeeld omdat ze delicttypen betreffen waarover al veel bekend is (bepaalde vormen van drugshandel) of omdat de zaak heel klein is en er weinig is doorgerechercheerd (waardoor er ook weinig kennis is verzameld over de daders en criminele activiteiten).
Hoe worden zaken voor de Monitor Georganiseerde Criminaliteit dan geselecteerd? De selectie van dertig zaken voor de vijfde ronde is tot stand gekomen na een intensieve inventarisatie van opsporingsonderzoeken.[16] Die inventarisatie vond plaats via gesprekken met en bezoeken aan gespecialiseerde en verschillende landelijke, regionale eenheden binnen politie en OM. Zo zijn er gesprekken gevoerd met specialisten op het terrein van cybercrime, cocaïne en heroïne, synthetische drugs en hennep, fraude en witwassen, overvallen, ram- en plofkraken, mensenhandel, en Hollandse netwerken. Verder zijn er mogelijk interessante zaken geïnventariseerd bij (andere) regionale en landelijke eenheden. Uiteindelijk heeft die inventarisatie plaatsgevonden bij alle tien regio's van de politie/het Openbaar Ministerie (OM) en enkele landelijke eenheden.

---

[14] Dit geldt natuurlijk alleen wanneer men zich op opsporingsonderzoeken richt. Er zijn echter weinig (of geen) mogelijkheden om niet-opgespoorde vormen van georganiseerde criminaliteit op een brede en diepgaande wijze te onderzoeken.

[15] De belangrijkste beperking van bestaande overzichten is dat zij niet voldoende inhoudelijke zaaksinformatie bevatten om een goed onderbouwde selectie te maken.

[16] Voor informatie over de inventarisatie die bij eerdere rondes heeft plaatsgevonden, zie Kruisbergen et al., 2012, p. 52-53).

De inventarisatie leidde tot een 'longlist' van ongeveer zeventig zaken, waarvan er uiteindelijk dertig zijn geselecteerd. Bij die selectie (en het maken van de longlist) spelen verschillende criteria een rol. We noemen hier enkele belangrijke criteria.

- Er is sprake van een crimineel samenwerkingsverband (in een enkel geval kan een onderzoek dat zich richt op één hoofdverdachte worden meegenomen, mits die verdachte een belangrijke rol speelt in een groter verband).
- Het opsporingsonderzoek is afgerond (aanhouding van belangrijkste verdachten) in 2011 of later.[17] Bij twee zaken is van dit uitgangspunt afgeweken, omdat deze 'oudere' zaken een grote meerwaarde hadden en bij de vorige Monitorrondes nog niet waren meegenomen.
- De informatierijkdom van een zaak. Een opsporingsonderzoek is 'informatierijk' wanneer, vaak door gebruik van bijvoorbeeld een telefoon- en/of internettap, het afluisteren van face-to-facegesprekken, undercovertrajecten (WOD-trajecten) of de inbeslagname van een administratie, het opsporingsonderzoek goed zicht biedt op de werkwijze van een crimineel samenwerkingsverband (met name ook op enkele van de hierna te noemen punten).
- De mate waarin de zaak toegevoegde waarde heeft doordat er zicht is gekomen op aspecten zoals verwevenheid tussen de daders en hun reguliere omgeving ('onder-' en 'bovenwereld'), afscherming, criminele geldstromen, een internationale component of een nieuwe of opvallende modus operandi of dadergroepering.
- Er moet spreiding zijn over verschillende delicttypen, dus bijvoorbeeld niet alleen drugszaken maar (juist) ook zaken op terreinen als cybercrime, witwassen en fraude.

De dertig geselecteerde zaken zijn, doorgaans na een interview met de zaaksofficier en/of de teamleider van de politie, geanalyseerd aan de hand van een aandachtspuntenlijst (zie bijlage 2). Deze uitgebreide aandachtspuntenlijst gaat in op de volgende onderwerpen:

- het opsporingsonderzoek (inclusief ingezette opsporingsmethoden);
- het criminele samenwerkingsverband;
- criminele activiteiten en werkwijze;
- contacten met de omgeving;
- omvang, verdeling en besteding van het wederrechtelijk verkregen voordeel;
- strafrechtelijke afdoening;
- evaluatie van het opsporingsonderzoek / leerervaringen ten aanzien van georganiseerde criminaliteit en haar aanpak.

Ieder van deze onderwerpen wordt in de aandachtspuntenlijst in veel verschillende elementen uitgewerkt. De aandachtspuntenlijst is in hoofdlijnen dezelfde als de lijst die bij de eerste monitorronde is gebruikt. Wel hebben er in de loop der tijd wat wijzigingen plaatsgevonden. Voor deze vijfde ronde is de aandachtspuntenlijst uitgebreid met onderwerpen betreffende het gebruik van ICT. Het werken met de aandachtspuntenlijst leidt tot uitgebreide zaaksverslagen die, wat betreft de genoemde hoofdthema's, te zien zijn als samenvattingen van de onderliggende opsporingsdossiers. Inmiddels zijn 180 zaken via deze vaste systematiek geanalyseerd, wat een zeer rijke databron oplevert. We gebruiken voor dit deelrapport vooral de dertig zaken uit de vijfde ronde van Monitor Georganiseerde Criminaliteit. Opsporingsdossiers zijn dus de belangrijkste databron binnen de monitor. Het gebruik van politiegegevens voor onderzoeksdoeleinden kent natuurlijk bepaalde

[17] Zaken hoeven nog niet voor de rechter te zijn geweest, laat staan tot een definitief rechterlijk oordeel te zijn gekomen. Wanneer dit laatste als criterium meegenomen zou worden, zouden vooral oude zaken kunnen worden bestudeerd.

beperkingen. De meest fundamentele beperking betreft het al genoemde feit dat opsporingsdossiers uiteindelijk alleen betrekking hebben op personen en activiteiten die onder de aandacht van de politie zijn gekomen en waarover de politie informatie wilde en kon verzamelen. Dit gegeven kan leiden tot een vertekening in de onderzoeksuitkomsten. Activiteiten en daders die buiten het zicht vallen van de politie, blijven immers ook buiten beeld van de onderzoeker. Verder is de verslaglegging in een opsporingsdossier in zekere zin per definitie 'vertekend', het verzamelen van informatie en rapportage vindt immers plaats vanuit een strafrechtelijk perspectief (Kruisbergen, 2017, p. 184). Echter, vanuit het perspectief van kennisvergaring heeft het gebruik van opsporingsdossiers ook een belangrijk voordeel. Iedereen die zich wil verdiepen in criminele fenomenen, wordt geconfronteerd met de 'muren van stilzwijgen' die criminele activiteiten omringen, vooral wanneer het gaat om georganiseerde criminaliteit (Van de Bunt, 2007, 2010). Alleen de politie heeft verregaande bevoegdheden om, via de inzet van opsporingsmethoden, door deze 'muren' heen te breken. Een onderzoeker die toegang heeft tot opsporingsdossiers profiteert mee van deze exclusieve bevoegdheden en kan zo een eveneens exclusief inzicht krijgen in de activiteiten van daders of in de wijze waarop zij zich tot elkaar en hun omgeving verhouden (Kruisbergen, 2017, p. 184; voor meer overwegingen bij en informatie over de gebruikte bronnen en methode, zie Kleemans et al., 1998; Kruisbergen et al., 2012).[18]

Literatuuronderzoek
In dit deelrapport in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit neemt bespreking van literatuur een meer prominente plek in dan in eerdere rondes. Voor ieder van de drie aspecten (criminele samenwerking, de logistiek en criminele geldstromen) volgt steeds een beknopte beschrijving van wat bekend is uit de literatuur. Daarbij wordt steeds een onderscheid gemaakt tussen enerzijds eerder onderzoek naar traditionele georganiseerde criminaliteit (vooral eerdere monitorrapporten) en anderzijds onderzoek naar cybercriminaliteit.

1.3.3 Reikwijdte van het onderzoek

Op basis van de door ons geanalyseerde opsporingsonderzoeken zijn *kwalitatieve* uitspraken mogelijk over het verschijnsel georganiseerde criminaliteit. Hoe verhoudt het gebruik van ICT zich bijvoorbeeld tot het ontstaan en de ontwikkeling van criminele samenwerkingsverbanden? Hoe wordt ICT gebruikt in relatie tot logistieke aspecten van het criminele bedrijfsproces? Hoe regelen daders in cybercrimezaken hun geldstromen en hoe verhoudt zich dat tot zaken van traditionele georganiseerde criminaliteit? Voor het vinden van een antwoord op dit type vragen zijn juist systematische casusstudies uitermate geschikt. Deze aspecten worden immers vooral duidelijk wanneer bepaalde zaken intensief worden bestudeerd. De rijkdom van het empirisch materiaal en de diepte van de kwalitatieve analyses maken dit onderzoek dus bij voorkeur geschikt voor het beantwoorden van *kwalitatieve* vragen over de aard van de georganiseerde criminaliteit in Nederland (Kleemans et al., 1998, p. 28-29; Kruisbergen et al., 2012, p. 57-58).

[18] Een onderzoeker kan natuurlijk ook interviews afnemen met daders. Dit kan belangrijke inzichten opleveren (zie bijvoorbeeld Van Koppen, 2013; zie ook Bernasco, 2010) en is voor sommige onderzoeksdoeleinden misschien zelfs noodzakelijk. Maar ook deze methode van dataverzameling kent beperkingen. Hoe selecteer je de respondenten, hoe krijg je hen bereid mee te doen aan het onderzoek en hoe kun je hen zover krijgen om vrijuit en naar waarheid te vertellen? Een onderzoeker die toegang heeft tot bijvoorbeeld verslagen van afgeluisterde gesprekken tussen twee drugshandelaren, hoeft zich om deze problemen in ieder geval geen zorgen te maken (Kruisbergen, 2017, p. 184-185).

Het doen van k*wantificerende* uitspraken is op basis van ons onderzoeksmateriaal in het algemeen minder goed mogelijk. Wij kunnen bijvoorbeeld wel aangeven dat bepaalde verschijnselen voorkomen, dat zij meer dan incidenteel voorkomen of dat zij niet voorkomen in ons casusmateriaal (voor zover wij weten). Hoe vaak bepaalde verschijnselen voorkomen in (bepaalde vormen van) georganiseerde criminaliteit in het algemeen, is op basis van ons onderzoek niet goed aan te geven. Kwantificerende uitspraken als 'veel' of 'vaak' die in dit rapport worden gedaan, gelden dus alleen binnen de context van de door ons geanalyseerde zaken (Kleemans et al., 1998, p. 28-29; Kruisbergen et al., 2012, p. 57-58). Vanwege het grote aantal zaken dat inmiddels is bestudeerd, zijn, wanneer zo veel mogelijk zaken worden meegenomen, kwantitatieve analyses op specifieke deelterreinen soms wel mogelijk, mits daarbij het genoemde voorbehoud wordt gemaakt. Voorbeelden hiervan zijn de analyse van criminele carrières (Kleemans & De Poot, 2007; Van Koppen, 2013), analyse van investeringen van daders in de legale economie (Kruisbergen et al., 2015a, 2015b) en de analyse van de rechtsgang en de incasso bij ontnemingsmaatregelen (Kruisbergen et al., 2016).
Een andere beperking betreft het gegeven dat opsporingsonderzoeken per definitie alleen betrekking hebben op modi operandi zoals die zich in het verleden hebben voorgedaan (in de volgende paragraaf wordt beschreven in welke periode de geanalyseerde opsporingsonderzoeken liepen). Nu is dit een 'open deur', maar in het geval van onderzoek naar het gebruik van ICT kan het een belangrijke beperking zijn. Juist op het terrein van cybercrime en andere toepassingen van ICT door daders lijken de ontwikkelingen zich immers snel te voltrekken (zie ook Schuppers et al., 2016). Enerzijds is dit een gegeven dat inherent is aan de gevolgde onderzoeksmethode en het gekozen onderwerp van onderzoek. Anderzijds proberen we het risico van beperkte houdbaarheid van uitkomsten enigszins te beperken door ons niet (alleen) te richten op hele specifieke, technische aspecten van criminele werkwijzen maar op bredere, onderliggende thema's.
Ten slotte is het bereik van ons onderzoek beperkt tot die gevallen van georganiseerde criminaliteit die door Nederlandse autoriteiten zijn opgespoord en vervolgd. Dit is het gevolg van het feit dat opsporingsonderzoeken onze belangrijkste gegevensbron vormen en we bespraken dit al in paragraaf 1.3.2. In het geval van cybercrime is de beperking die het gebruik van opsporingsdossiers met zich meebrengt echter mogelijk groter dan bij andere vormen van criminaliteit. Juist bij cybercrime kan een modus operandi of een dadergroepering namelijk een sterke internationale component hebben, wat, mede afhankelijk van de betrokken landen, de opsporing en vervolging kan bemoeilijken (Schuppers et al., 2016, p. 10).[19]

1.4 Beknopte beschrijving van het onderzoeksmateriaal

In tabel 1 staat een overzicht van de 180 zaken die in de vijf rondes van de monitor zijn geanalyseerd.

[19] In *Cybercrime en gedigitaliseerde criminaliteit – Nationaal Dreigingsbeeld 2017*, worden verder onder andere een lager bewustzijn van slachtofferschap van cybercrime en een lagere aangiftebereid genoemd als factoren die het zicht op cybercrime belemmeren (Schuppers et al., 2016, p. 9-10).

Tabel 1 Overzicht van geanalyseerde opsporingsonderzoeken uit de eerste, tweede, derde, vierde en vijfde ronde van de Monitor Georganiseerde Criminaliteit naar de soort illegale activiteiten die in het opsporingsonderzoek de meeste aandacht hebben gekregen

	Ronde 1	Ronde 2	Ronde 3	Ronde 4	Ronde 5	Totaal
Traditionele drugs	13	7	7	10	6	44
Synthetische drugs	2	3	5	5	0	15
Traditionele + synthetische drugs	8	4	9	0	6	28
Mensensmokkel	4	6	6	0	0	16
Mensenhandel	7	2	6	3	1	19
Fraude en witwassen	5	10	6	11	7	40
Overige delicten	1	8	1	1	3	14
Cybercriminaliteit	0	0	0	0	7	7
Totaal	**40**	**40**	**40**	**30**	**30**	**180**

De vijfde ronde is de eerste waarin zaken op het terrein van cybercrime zijn geanalyseerd. In eerdere rondes waren nog weinig (geschikte) afgeronde opsporingsonderzoeken op het terrein van cybercrime beschikbaar.
We lichten hier kort de zeven cybercrimezaken toe en we geven aan hoe we die in dit rapport gebruiken.
Deze zeven zaken omvatten twee zaken waarbij drugshandel (smokkel) mede mogelijk is gemaakt dankzij het vernieuwende gebruik van ICT. Een van deze zaken betreft een dadergroepering die door middel van een hack in het netwerk van een haventerminal de afhandeling van binnenkomende containers manipuleert (casus 151). De andere zaak draait om betrokkenen bij een darknet market waarop onder meer drugs worden verhandeld (casus 152). In een derde zaak staat een moderne variant van witwassen centraal. Het gaat daarbij om daders die bitcoins, van personen die deze vermoedelijk via online drugshandel hebben verdiend, omwisselen voor contante euro's (casus 173). Een vierde zaak richt zich op een variant van skimmen (ook wel shimmen genoemd) waarbij niet de magneetstrip van een bankpas wordt gekopieerd, maar waarbij het dataverkeer wordt afgevangen tussen de zogenoemde EMV-chip op de pas en de terminal waar deze pas wordt ingestoken (casus 154). Een vijfde zaak draait om phishingoperaties, waarbij daders onder meer toegangsgegevens van slachtoffers voor internetbankieren proberen te verkrijgen (casus 156). In de zesde en zevende zaak staat banking malware centraal, waarbij daders via kwaadaardige software (malware) betalingen via internetbankieren manipuleren (casus 153 en 155).
De zeven zaken beslaan een vrij breed scala aan criminele werkwijzen. Waar dat relevant is, maken we bij de analyses in deze rapportage een meer verfijnd onderscheid tussen zaken op basis van de ICT-component die een zaak kenmerkt. Dit onderscheid omvat vier categorieën. De eerste categorie omvat zaken van *traditionele georganiseerde criminaliteit*, dat wil zeggen zonder een sterke ICT-component. Hierin vallen de 23 zaken uit tabel 1 die niet onder cybercriminaliteit vallen (en alle zaken uit de eerste tot en met de vierde ronde). Een tweede categorie betreft zaken van *traditionele georganiseerde criminaliteit met ICT als belangrijk vernieuwend element* in de modus operandi. Daartoe rekenen we de twee zaken van door ICT gefaciliteerde drugshandel/-smokkel (casus 151 en 152) en de zaak van de bitcoinwisselaars (witwassen, casus 173). De derde categorie betreft gevallen van *georganiseerde low-tech cybercriminaliteit*, waartoe we de skimming- en de phishingzaak rekenen (casus 154 en 156). Een vierde categorie ten slotte omvat de twee zaken

van banking malware (casus 153 en 155) en deze classificeren we als *georganiseerde high-tech cybercriminaliteit*.[20]
Ten slotte een opmerking over het tijdvak waarin de onderzochte zaken zich afspeelden. Bij 28 van de 30 bestudeerde opsporingsonderzoeken uit de vijfde ronde van de Monitor Georganiseerde Criminaliteit vonden de belangrijkste aanhoudingen plaats in de periode 2011-2016, in 2 zaken vonden die aanhoudingen eerder plaats.

1.4.1 Gebruik van het onderzoeksmateriaal in deze rapportage

Openbaar empirisch onderzoek naar georganiseerde criminaliteit is van groot maatschappelijk belang. Indien het niet mogelijk zou zijn om over dit onderwerp openbaar te publiceren, is het ook niet mogelijk om – empirisch gefundeerd – openbaar te debatteren over een dergelijk belangrijk maatschappelijk probleem. Dit klemt te meer, aangezien discussies over dit onderwerp betrekking hebben op keuzes over ingrijpende inbreuken op de grondrechten van burgers.
Bij een openbare rapportage dient zich echter wel de vraag aan hoe gedetailleerd en op welke manier zaken kunnen worden beschreven zonder dat deze beschrijvingen 'tot concrete personen herleidbaar' zijn en aan deze personen schade toebrengen. Enerzijds kan detaillering immers het inzicht in bepaalde zaken vergroten, anderzijds maakt detaillering de zaken een stuk herkenbaarder, wat zeker in sommige gevallen problematisch kan zijn.
Sommige risico's kunnen worden vermeden door het gebruik van meerdere casussen, door het casusmateriaal te gebruiken als toelichting bij een algemener en abstracter verhaal, en door te anonimiseren door middel van abstractie (zie ook Van de Bunt & Kleemans, 2000). Maar zonder details, die van belang zijn om voor de lezer de context van georganiseerde criminaliteit duidelijk te maken, wordt een verhaal wel heel abstract.
In dit rapport zijn, zoals dat in eerdere monitorrapportages ook is gebeurd, op verschillende plaatsen casusbeschrijvingen te vinden, soms meer en soms minder gedetailleerd. Daarbij is door de opstellers van dit rapport steeds een zorgvuldige afweging gemaakt tussen informatiewaarde enerzijds en het voorkomen van schade anderzijds. Verder is de begeleidingscommissie van het onderzoek gevraagd te toetsen of het beschreven casusmateriaal geen onevenredige schade kan toebrengen aan betrokken personen. Nog een laatste opmerking over het gebruik van casusbeschrijvingen: alle initialen, zoals 'verdachte A' of 'bedrijf W', zijn willekeurig gekozen en corresponderen niet met de werkelijke namen (Van de Bunt & Kleemans, 2002, p. 44-45).

1.5 Opbouw van dit rapport

Na deze inleiding worden in de hoofdstukken 2, 3 en 4 de resultaten van de empirische analyses beschreven. Deze hoofdstukken vallen samen met de drie onderzoeksvragen die centraal staan in dit rapport. Hoofdstuk 2 handelt over criminele samenwerking en het gebruik van ICT. Daarin staat ICT in relatie tot het ontstaan en de ontwikkeling van criminele samenwerkingsverbanden centraal. In hoofdstuk 3 komt het gebruik van ICT in relatie tot de logistieke aspecten van criminele activiteiten aan bod. In hoofdstuk 4 bespreken we het gebruik van ICT ten aanzien van

[20] Voor de indeling van zaken in de categorie cybercriminaliteit (en ook voor het gebruik van de meer verfijnde indeling), wordt alleen gekeken naar de modus operandi in het kerndelict. Het gebruik van ICT bij bijvoorbeeld de onderlinge communicatie tussen daders, zoals het gebruik van speciale, met versleuteling toegeruste *Blackberries*, wat regelmatig voorkomt in de bestudeerde zaken, speelt daarbij geen rol.

criminele geldstromen. Het afsluitende hoofdstuk 5 bevat een synthese van de empirische resultaten. Ook bespreken we in dat hoofdstuk mogelijke beleidsimplicaties. De bijlagen bevatten een weergave van de samenstelling van de begeleidingscommissie (bijlage 1), de gebruikte aandachtspuntenlijst (bijlage 2) en een beknopte beschrijving van alle 180 zaken die in de vijf rondes van de monitor zijn geanalyseerd (bijlage 3).

2 Criminele samenwerking en het gebruik van ICT

Dit hoofdstuk gaat in op de vraag in hoeverre en op welke manier de toegenomen beschikbaarheid en het gebruik van ICT heeft geleid tot verandering in de manier waarop daders met elkaar samenwerken. We starten met een overzicht van de literatuur. Wat weten we uit voorgaand empirisch onderzoek over criminele samenwerking bij georganiseerde criminaliteit? En in hoeverre levert de literatuur over cybercrime dezelfde of andere beelden op? In vorige rapportages op basis van de Monitor Georganiseerde Criminaliteit is reeds uitvoerig ingegaan op 'offline' criminele samenwerking. Paragraaf 2.1 geeft daarom een beknopt overzicht van deze inzichten. In paragraaf 2.2 gaan we na wat de literatuur ons leert over netwerken die zich bezighouden met het plegen van cybercriminaliteit. Daarbij bespreken we de recente inzichten in de structuur, samenstelling en instroom- en doorgroeimechanismen. Daarna wordt in paragraaf 2.3 ingegaan op de structuur en samenstelling van criminele samenwerkingsverbanden in de dertig nieuwe monitorzaken. In paragraaf 2.4 komen vervolgens de instroom- en doorgroeimechanismen aan bod. Het hoofdstuk sluit af met een recapitulatie (paragraaf 2.5).

2.1 Georganiseerde criminaliteit offline: een overzicht

Voorgaande rapportages op basis van de Monitor Georganiseerde Criminaliteit hebben verschillende inzichten opgeleverd over de aard van de georganiseerde criminaliteit in Nederland. We bespreken hier achtereenvolgens: de structuur en samenstelling van criminele groepen en netwerken; het belang van facilitators; sociale inbedding, vertrouwen en capaciteit; de relatie tussen beroepen en georganiseerde criminaliteit; de lokale inbedding van transnationale criminele activiteiten; en instroom- en doorgroeimechanismen.

Structuur en samenstelling

Piramidale organisaties bestaan wel degelijk, maar zijn in Nederland eerder uitzondering dan regel. Dit impliceert echter niet dat criminele samenwerkingsverbanden geen structuur kennen of dat de relaties in samenwerkingsverbanden inwisselbaar en horizontaal zijn. Sommige personen zijn belangrijker dan andere binnen een crimineel samenwerkingsverband.

In de vorige monitorrapportages is gewezen op de brede variëteit aan samenwerkingsverbanden en op het feit dat de logistiek van de criminele activiteiten (wat moet er allemaal worden geregeld?) grote invloed heeft op de manier waarop de samenwerking concreet gestalte krijgt (Kleemans et al., 1998, p. 31-59; 2002, p. 39-63). Zo zijn er vaak duidelijke hoofdrolspelers waarvan vele andere daders afhankelijk zijn vanwege hun geld, kennis of contacten. De vraag bij het analyseren van criminele netwerken moet dan ook niet zijn 'Wie is hier de baas?', maar 'Wie is afhankelijk van wie en om welke reden?'

De hoofdrolspelers zien we telkens weer terug, in verschillende opsporingsonderzoeken en in verschillende samenwerkingsverbanden. Maar andere daders kunnen gaandeweg steeds minder afhankelijk worden van deze hoofdrolspelers, doordat zij zelf geld, kennis en contacten vergaren en vervolgens steeds meer eigen criminele activiteiten ontwikkelen. Door niet a priori uit te gaan van een duurzame, piramidale organisatie, ontstaat er dus oog voor groei en ontwikkeling binnen criminele netwerken. Ook kan duidelijk worden dat facilitators, die veelal in de periferie van cri-

minele samenwerkingsverbanden opereren, hun diensten verlenen aan meerdere criminele samenwerkingsverbanden.

Facilitators

In de eerste twee rapportages op basis van de Monitor Georganiseerde Criminaliteit werd reeds gewezen op het belang van facilitators en van een faciliterende omgeving voor het functioneren van criminele samenwerkingsverbanden (Kleemans et al., 1998, p. 61-91; 2002, p. 56-62). Criminele samenwerkingsverbanden kunnen vaak bepaalde activiteiten niet zelf uitvoeren, omdat de capaciteiten daarvoor ontbreken, of zij willen bepaalde activiteiten niet zelf uitvoeren, omdat het risico te hoog is. In deze gevallen kunnen zij worden geholpen door 'facilitators' die specifieke diensten verlenen aan criminele samenwerkingsverbanden, zoals documentenvervalsers, transporteurs, geldwisselaars en financiële adviseurs.
Kenmerkend voor de werkzaamheden van de facilitators is dat deze activiteiten cruciaal zijn voor het uitvoeren van bepaalde criminele activiteiten. In de tweede plaats wordt daarbij veelal een brug geslagen tussen 'onderwereld' en 'bovenwereld'. Dit komt omdat daar vaak de logistieke 'bottlenecks' liggen voor criminele samenwerkingsverbanden. Een derde kenmerk is dat de facilitator vaak relatief moeilijk vervangbaar is, omdat de gevraagde capaciteiten relatief schaars zijn. Een vierde kenmerk is dat deze diensten vaak worden geleverd aan meerdere groepen. Dit komt omdat criminele samenwerkingsverbanden vaak dezelfde problemen kennen en zij via-via in aanraking komen met dezelfde facilitators. Hoe schaarser de deskundigheid en hoe crucialer deze deskundigheid is voor het uitvoeren van bepaalde criminele activiteiten, hoe belangrijker de rol is van deze facilitators binnen criminele netwerken.

Sociale inbedding, vertrouwen en capaciteit

Omdat er in wereld van de georganiseerde criminaliteit grote financiële belangen op het spel staan in een grotendeels ongereguleerde wereld, is sociale inbedding en vertrouwen van groot belang voor het functioneren van criminele samenwerkingsverbanden. In de vorige rapportages is het belang van bestaande sociale relaties bij criminele samenwerking uitvoerig belicht. Familie, vrienden en bekenden werken met elkaar samen en introduceren elkaar weer bij anderen. Maar bestaande sociale relaties bieden niet altijd een oplossing, omdat sociale relaties geclusterd zijn en er barrières bestaan tussen verschillende landen, verschillende etnische groepen en tussen onderwereld en bovenwereld. De beperkingen van bestaande lokale netwerken zien we terug bij transitcriminaliteit; winstgevende, internationale illegale activiteiten, zoals drugshandel, mensensmokkel, mensenhandel, wapenhandel, witwassen en fraude met accijnzen en heffingen, waarbij Nederland kan fungeren als productieland, doorvoerland of bestemmingsland. Dergelijke activiteiten vormen een zeer belangrijk onderdeel van de georganiseerde criminaliteit in Nederland.
Bij criminele samenwerking gaat het niet alleen om betrouwbaarheid of integriteit, maar ook om capaciteit. Daarom wordt gesignaleerd dat daders juist bij omvangrijke en risicovolle criminele operaties met 'buitenstaanders' – niet zijnde familieleden, vrienden of vaste zakenpartners – in zee kunnen gaan (Van de Bunt & Kleemans, 2007, p. 49-76). Nieuwe relaties kunnen nieuwe handelsmogelijkheden bieden. Maar hoe komt vertrouwen met dergelijke partners tot stand? In de eerste plaats kan worden gewezen op leereffecten: vertrouwen wordt gebaseerd op eigen ondervinding met betrekking tot de (eerdere) prestaties van de partner. In detweede plaats kan vertrouwen gebaseerd zijn op de (overgedragen) ervaringen van anderen. Ten derde kunnen reputaties ook gebaseerd worden op generalisaties ten aanzien van de (vermeende) eigenschappen van bepaalde groepen.

Beroepen en georganiseerde criminaliteit
Niet alleen familie- en vriendschapsbanden zijn van belang. Ook beroepen kunnen op verschillende manieren gelegenheid bieden voor georganiseerde criminaliteit (Van de Bunt & Kleemans, 2007, p. 77-96). Allereerst kan dat door internationale contacten en reisbewegingen, waardoor mogelijkheden voor (transit)criminaliteit kunnen worden ontdekt en geëffectueerd. Voorbeelden hiervan zijn beroepen die te maken hebben met transport en logistiek. In de tweede plaats is de individuele bewegings- en/of handelingsvrijheid van bepaalde beroepsgroepen van belang (autonomie). Deze autonomie maakt het mogelijk om legale en illegale activiteiten te combineren. In de derde plaats is het 'sociale' karakter van beroepen van belang. Beroepen waarin men veel met andere mensen in aanraking komt, bieden ook veel kansen tot ontmoetingen met potentiële mededaders.

Lokale inbedding van transnationale georganiseerde criminaliteit
Zonder lokale inbedding is het erg moeilijk om succesvol te opereren. Maar veel van de onderzochte daders weten het niveau van de 'local hero' niet te ontstijgen; zij ontberen exclusieve vaardigheden of specialismen die hen interessant maken voor criminele samenwerkingspartners van buiten de regio of van buiten Nederland. Toch zien we in verschillende zaken dat lokaal opererende daders aansluiting weten te vinden bij transnationale handelsactiviteiten. Van belang daarbij zijn (offline) ontmoetingsplaatsen, zoals cafés, clubhuizen en andere plaatsen waard daders potentiële mededaders kunnen ontmoeten (zie Felson, 2003, 2006). Meer in het bijzonder is in de internationale drugshandel de positie van 'marktplaats Amsterdam' relevant. Daarnaast stellen internationale 'bruggenbouwers' meer lokale groepen in staat om aansluiting te vinden bij internationale drugsmarkten, zonder dat dergelijke groepen ook maar een stap buiten Nederland hoeven te zetten.

Instroommechanismen en doorgroeifactoren
Uit een analyse van 92 'starters' in de georganiseerde criminaliteit blijkt dat mensen op velerlei manieren betrokken raken bij vormen van georganiseerde criminaliteit: door reeds bestaande sociale relaties, door werk- en beroepsgerelateerde relaties, door hobby's of nevenactiviteiten, door bepaalde 'life events' (vooral financiële tegenslagen) en door bewuste rekrutering (Kleemans & De Poot, 2007; Van de Bunt & Kleemans, 2007, p. 97-126).
Dit verklaart ook waarom een substantieel deel van de onderzochte daders pas later in het leven bij georganiseerde criminaliteit betrokken raakt, het fenomeen van de 'late starters' of 'zij-instromers' in de georganiseerde criminaliteit. Sommige gelegenheden voor het uitvoeren van winstgevende criminele activiteiten ontstaan immers pas later in iemands leven. Ook grijpen mensen bepaalde mogelijkheden pas later in het leven daadwerkelijk aan, bijvoorbeeld bij 'life events' zoals faillissementen en problematische schuldsituaties.
Naast de 'late starters' zijn er daders die al langer crimineel actief zijn voordat zij overstappen op vormen van georganiseerde criminaliteit. Criminele carrières kunnen in een stroomversnelling raken door: specialisatie (met name in de drugshandel en -productie); een *broker* die de dader toegang geeft tot interessante internationale markten; kapitaal dat de dader gebruikt om te investeren in handelsmogelijkheden en/of semilegale investeringen; of het beschikken over specifieke vaardigheden of transnationale contacten waarvan andere daders afhankelijk zijn. De katalysator in dat laatste geval is vooral de netwerkvorming die door anderen rond deze personen plaatsvindt: daders vertellen andere daders over de specifieke expertise van deze persoon, waardoor deze andere daders ook contact zoeken.

2.2 Inzichten uit de literatuur op het terrein van 'cybercrime'

Structuur en samenstelling

In theorie biedt internet een prima gelegenheidsstructuur voor gedecentraliseerde flexibele netwerken van criminelen die losjes georganiseerd samenwerken en werkzaamheden verdelen op basis van kennis en kunde. Toch blijkt dit in de praktijk lang niet altijd op te gaan voor cybercriminele netwerken.

Uit empirisch onderzoek naar georganiseerde cybercrime in Nederland, Duitsland, Engeland, Zweden en de VS blijkt bijvoorbeeld dat de structuur van cybernetwerken niet veel verschilt van die van traditionele netwerken (Bulanova-Hristova & Ksaper, 2016a, 2016b; Werner & Korsell, 2016; Leukfeldt et al., 2017b, 2017c, 2017d; Odinot et al., 2017[21]). Het merendeel van de door Leukfeldt et al. (2017b, 2017c, 2017d) bestudeerde netwerken kende bijvoorbeeld een min of meer stabiele groep kernleden die gedurende langere periode samen delicten plegen. De kernleden van deze netwerken kenden elkaar vaak uit de fysieke wereld en rekruteerden alleen enkele specialisten via online ontmoetingsplaatsen. Bij slechts enkele netwerken was sprake van een ad-hoc samenwerking waarbij op een online ontmoetingsplek allianties werden gesmeed en aanvallen werden uitgevoerd.

Verder laten verschillende studies zien dat er – net als bij traditionele netwerken – nog steeds belangrijke actoren zijn met een functie als bruggenbouwer binnen cybercriminele netwerken (Soudijn & Monsma, 2012; Lu et al., 2010; Yip et al., 2012; Holt & Smirnova, 2014; Décary-Hétu & Dupont, 2012; Décary-Hétu et al., 2012; Leukfeldt et al., 2017c, 2017e).

Ten slotte kan binnen cybernetwerken ook sprake zijn van een hiërarchie. Ondanks dat er geen sprake is van een maffia-achtige structuur, zijn binnen alle netwerken die Leukfeldt et al. (2017a, 2017b, 2017c) bestudeerden verschillende lagen waarneembaar. Bovenaan staan kernleden die de criminele activiteiten plannen, voor lange tijd samenwerken en andere geschikte mededaders zoeken. Onder de kernleden staan facilitators die specifieke criminele diensten leveren. Daarbij kan onderscheid worden gemaakt tussen professionele facilitators en gerekruteerde facilitators. Beide typen facilitators bieden diensten aan de kernleden van criminele netwerken aan zodat de criminele activiteiten (beter) uitgevoerd kunnen worden. Het verschil tussen beide groepen is dat professionele facilitators hun diensten zelf aan allerlei netwerken aanbieden, terwijl de gerekruteerde facilitators door kernleden worden aangezet om bepaalde diensten te leveren. De onderste laag wordt gevormd door katvangers. Dit is een groep criminelen die door de kernleden of door facilitators wordt ingezet om het spoor naar de criminele groep te onderbreken. Zo worden bijvoorbeeld de rekeningen van katvangers gebruikt om geld van slachtoffers van phishing weg te sluizen.

Overigens zijn er wel degelijk ook netwerken die de mogelijkheden die internet biedt ten volle benutten. Leden van dergelijke netwerken weten bijvoorbeeld door het gebruik van online criminele ontmoetingsplaatsen snel en met een relatief kleine groep leden een internationale positie te bemachtigen (Leukfeldt et al., 2017c, 2017d) of gaan een ketensamenwerking aan met andere criminelen die elk een specifieke criminele activiteit uitvoeren (Bulanova-Hristova et al., 2016a, 2016b, Odinot et al., 2017).

Er zijn dus netwerken die wat structuur betreft veel overeenkomsten vertonen met traditionele criminele netwerken – een langdurige samenwerking tussen de kernleden en afhankelijkheidsrelaties – en er zijn netwerken waarbij sprake is van meer kortstondige samenwerkingen waarbij de afzonderlijke leden zich gespecialiseerd

[21] Vijf zaken op het terrein van cybercrime/ICT-gerelateerde georganiseerde criminaliteit die in deze vijfde ronde van de monitor zijn opgenomen, maakten ook onderdeel uit van de studie van Odinot et al. (2017).

hebben in een specifieke activiteit. Deze verschillen in structuur hangen samen met de ontstaans- en groeiprocessen (Bulanova-Hristova et al., 2016a, 2016b, Leukfeldt et al., 2017b, 2017c, 2017d). Traditionele criminele netwerken die ook cybercrimes zijn gaan plegen, behouden hun structuur. Netwerken die alleen cybercrimes plegen, maar zijn ontstaan uit offline sociale contacten, hebben eveneens een structuur die lijkt op die van traditionele criminele netwerken. Netwerken die alleen cybercrimes plegen en waarbij de kernleden elkaar online hebben leren kennen, hebben soms een traditionele structuur (ook op online ontmoetingsplaatsen is er namelijk sprake van langdurige contacten, zie bijvoorbeeld Leukfeldt et al., 2017c, 2017d), maar bij dit type netwerk is er soms ook sprake van een kortstondige (keten)samenwerking.

Facilitators

Facilitators spelen bij cybercriminele netwerken een belangrijke rol. Enkele netwerken lukt het wel om zonder diensten van anderen delicten te plegen, maar het gros van de netwerken maakt in meer of mindere mate gebruik van facilitators (Odinot et al., 2017; Bulanova-Hristova et al., 2016a, 2016b; Leukfeldt et al., 2017a, 2017b, 2017c, 2017d, 2017e;). Daarbij kunnen we onderscheid maken tussen professionele dienstverleners die zelf hun diensten aanbieden en voor allerlei criminele netwerken werken en gerekruteerde dienstverleners die door een netwerk worden ingezet. Voorbeelden van professionele dienstverleners zijn malware schrijvers die malware leveren waarmee computers van eindgebruikers kunnen worden overgenomen, hackers die hun diensten aanbieden om in databases in te breken of personen die de beschikking hebben over netwerken van katvangers in allerlei landen die kunnen worden gebruikt om geld wit te wassen. De professionele dienstverleners bieden hun diensten vaak aan op forums, maar contacten tussen kernleden en facilitators kunnen ook ontstaan binnen offline sociale netwerken of op offline criminele ontmoetingsplaatsen. Voorbeelden van gerekruteerde dienstverleners zijn bankmedewerkers die gegevens van 'interessante' bankrekeningen aanleveren of die pinlimieten kunnen ophogen waardoor er minder katvangersrekeningen nodig zijn bij het cashen van geld afkomstig van phishingaanvallen.

Over de rol die facilitators spelen om een brug te slaan tussen 'onderwereld' en 'bovenwereld' voor cybercriminele netwerken is nog weinig bekend. Uit de analyses van Leukfeldt at al. (2017a) blijkt bijvoorbeeld dat hoewel respondenten aangeven dat er in sommige gevallen haast wel sprake moet zijn van betrokkenheid van corrupte Oost-Europese of Russische overheidsmedewerkers, hiervoor in de opsporingsonderzoeken geen bewijs kan worden gevonden. Wel is duidelijk dat medewerkers van legitieme bedrijven soms worden gerekruteerd door leden van cybercriminele groepen om mee te werken aan criminele activiteiten. Een concreet voorbeeld betreft de zojuist genoemde bankmedewerkers die inzicht hebben in de rekeningen van potentiële slachtoffers of die pinlimieten van de rekeningen van katvangers kunnen verhogen (Leukfeldt, 2014). Ook worden legitieme infrastructuren misbruikt door criminelen om hun delicten te plegen (Odinot et al., 2017). Een concreet voorbeeld betreft hosting providers die legale diensten aanbieden, zoals het verhuren van serverruimte, of illegale diensten, zoals bulletproof webhosting, waarbij het voor opsporingsdiensten erg lastig is om in te grijpen. Een ander voorbeeld betreft online advertentiebedrijven die advertenties op een groot aantal websites tonen. Er zijn gevallen bekend waarbij advertenties werden getoond die malware verspreiden. Ook kan worden gewezen op legitieme bedrijven zoals webshops waar spullen met crimineel verdiend geld worden aangekocht, of pakketbezorgers die met frauduleuze overboekingen aangekochte goederen onderscheppen. Ook financiële infrastructuren kunnen worden misbruikt, bijvoorbeeld voor het uitvoeren van onderlinge betalingen met behulp van e-currencies zoals bitcoins, of het gebruik

van exchangers (wisselaars) die e-currencies omzetten in euro's of Amerikaanse dollars (Odinot et al., 2017; Leukfeldt et al., 2017b, 2017c, 2017d, 2017e; zie hoofdstuk 4).

Forums als online ontmoetingsplaatsen

Door het grote aanbod van criminele dienstverleners op forums is het vinden van geschikte dienstverleners voor cybercriminele netwerken mogelijk minder moeilijk dan voor traditionele netwerken (Lusthaus, 2012; Yip et al., 2013; Holt & Smirnova, 2014; Holt et al., 2015; Dupont et al., 2016; Holt en Lampke, 2010; Bacher et al., 2005; Soudijn & Zegers, 2012; Leukfeldt, 2014; Franklin et al., 2007; Wehinger, 2011). Daardoor zijn dienstverleners in theorie dus gemakkelijker vervangbaar. Toch laten de analyses van Bulanova-Hristova et al. (2016a, 2016b) en Leukfeldt et al. (2017b, 2017c, 2017d) zien dat cybercriminele groepen soms voor langere tijd samenwerken met dezelfde facilitator. Enerzijds is het door forums met hun rating- en reviewsystemen vrij gemakkelijk geworden om betrouwbare facilitators te vinden. Anderzijds weten we ook dat slechts een heel klein deel van de leden van forums een zeer hoge mate van technische expertise hebben (Holt, 2007; Schell & Dodge, 2002; Holt el al., 2015) en dat reviewsystemen lang niet altijd goed werken (Holt et al., 2015; Decary-Hétu & Dupont, 2013; Dupont et al., 2016). Het is dus nog maar de vraag hoe gemakkelijk vervangbaar facilitators met een zeer hoge mate van technische expertise zijn.

Facilitators die actief zijn op forums bieden hun diensten aan meerdere individuen en netwerken aan (bijvoorbeeld Peretti, 2008; Holt & Lampke, 2010; Chu et al., 2010; Soudijn & Monsma, 2012; Lu et al., 2010; Yip et al., 2013; Holt, 2013; Holt & Smirnova, 2014). Potentiële kopers kunnen contact opnemen met de verkoper via verschillende kanalen, bijvoorbeeld een privébericht via het forum of chatkanalen buiten het forum. Betalingen kunnen worden gedaan met de *virtual currencies* die op dat moment in gebruik zijn, bijvoorbeeld bitcoin, e-Gold, Liberty Reserve, Web Money, Yandex en Western Union (Franklin et al., 2007; Holt & Lampke, 2010; Holt & Smirnova, 2014; Holt et al., 2015).

Via dergelijke online forums worden verschillende typen waren aangeboden, zoals gestolen data, cybercriminele tools en diensten, en de illegale handel in meer traditionele zaken zoals drugs, medicijnen en wapens. Bij gestolen data gaat het om gegevens van creditkaarten, bankrekeningen en PayPal-accounts en identiteitsdocumenten (Franklin et al., 2007; Holt & Lampke, 2010; Peretti, 2008; Holt et al., 2015; Chu et al., 2010; Holt & Smirnova, 2014; Wehinger, 2011; Soudijn & Zegers, 2012, Leukfeldt et al, 2017c, 2017d, 2017e, 2017f). Voorbeelden van criminele tools zijn phishing kits en malware (Holt & Lampke, 2010; Herley & Florencio, 2010; Soudijn & Zegers, 2012; Leukfeldt, 2014; Leukfeldt et al., 2017c, 2017d; Holt & Smirnova, 2014; Chu et al., 2010) of botnets en Ddos aanvallen (Franklin et al., 2007, Chu et al., 2010; Décary-Hétu & Dupont, 2012). Criminele diensten die worden aangeboden zijn bijvoorbeeld 'escrow services' waardoor via een derde partij veilig kan worden betaald (Lusthaus, 2012; Yip et al., 2013; Holt & Smirnova, 2014; Holt et al., 2015; Dupont et al., 2016), 'exchangers' die virtueel geld omzetten in echt geld (Holt & Lampke, 2010), money mules om criminele verdiensten te cashen en niet traceerbaar te maken (Soudijn & Zegers, 2012; Leukfeldt, 2014), andere cash-out services zoals het kopen van goederen met gestolen creditkaarten (Franklin et al., 2007; Wehinger, 2011) en 'bulletproof webhosting' (Franklin et al., 2010). Bij illegale handel gaat het om zaken zoals drugs, medicijnen en wapens (Martin, 2014a, 2014b).

Instroom- en doorgroeimechanismen

Paragraaf 2.1 laat zien dat offline sociale banden een belangrijke rol spelen bij de totstandkoming van criminele netwerken. Daarentegen hoeven in de online wereld in principe geen geografische afstanden te worden overbrugd om in contact te komen met andere daders; afstand, locatie en ook tijd zijn in principe geen beperkende factor meer voor criminele samenwerking.

Verschillende studies laten zien dat digitalisering, en in het bijzonder online criminele ontmoetingsplaatsen, de ontstaans- en groeiprocessen van criminele netwerken kunnen beïnvloeden. Soudijn en Zegers (2012) en Yip et al. (2012) tonen aan dat nieuwkomers op digitale ontmoetingsplaatsen snel contacten weten aan te gaan met bestaande forumleden en relatief snel een centralere positie innemen. In een online omgeving lijkt de belangrijke rol die centrale personen normaal spelen binnen netwerken dus af te nemen.

De studies van Leukfeldt (2014), Leukfeldt et al. (2017a, 2017c, 2017d), Bulanova-Hristova et al. (2016a, 2016b) en Odinot et al. (2017) laten echter zien dat cybercriminele netwerken gebruikmaken van zowel offline sociale contacten als digitale ontmoetingsplaatsen. Bij netwerken waarbij offline sociale contacten de basis vormen voor ontstaan en groei is, net als bij traditionele criminele netwerken, te zien dat familie, vrienden en bekenden met elkaar samen werken en elkaar introduceren bij anderen. Overigens heeft slechts een enkel netwerk genoeg aan alleen offline sociale relaties. Online forums worden door dit soort netwerken gebruikt om specialistische kennis en kunde binnen te halen die binnen de offline sociale relaties ontbreken, bijvoorbeeld het aankopen van geavanceerde malware die kan worden gebruikt om fraude met internetbankieren te plegen. Bij netwerken waar online contacten de basis vormen voor het ontstaan en groei van het netwerk is ook een tweedeling te zien. Leden van deze netwerken leerden elkaar online kennen, bijvoorbeeld in chatkanalen of op forums. Een minderheid van de netwerken lijkt de criminele activiteiten uit te kunnen voeren met alleen online contacten. Bij deze netwerken leerden niet alleen de kernleden elkaar online kennen, maar werden ook alle facilitators online gerekruteerd. Bij andere netwerken leerden de kernleden elkaar online kennen, rekruteerden ze online facilitators, maar maakten ze ook gebruik van offline contacten, bijvoorbeeld om een netwerk van katvangers op te zetten.

Digitale ontmoetingsplaatsen zorgen ervoor dat de traditionele beperkingen van sociale netwerken worden opgeheven. Feitelijk is er geen verschil met traditionele offline criminele ontmoetingsplaatsen: zodra je daar binnen bent, kun je contacten opdoen en kun je personen ontmoeten die voor bijvoorbeeld nieuwe afzetmarkten kunnen zorgen (zie Felson, 2003, 2006). Op zich is er bij digitale ontmoetingsplaatsen dus niets nieuws onder de zon. Het lijkt er echter op dat de toegang tot digitale ontmoetingsplaatsen laagdrempeliger is dan toegang tot offline criminele ontmoetingsplaatsen (Leukfeldt et al., 2017c, 2017d). Voor de nieuwsgierige eenling is het gemakkelijker om op allerlei openbare forums rond te hangen en vragen te stellen dan in een bar vol criminelen. Belangrijk daarbij is ook dat forums een leerfunctie hebben en dat er een subcultuur is waarbij het delen van informatie over criminele mogelijkheden vrij normaal is (Chu et al., 2010; Holt & Kilger, 2008; Holt el al., 2012; Hutchings & Holt, 2015; Hutchings, 2014; Leukfeldt et al., 2017c, 2017e; Soudijn & Zegers, 2012). Iemand die wil leren kan dus terecht op een forum. Via discussies en oproepen kun je vervolgens aan informatie komen, maar je kunt ook mensen betalen om jou vaardigheden te leren (Hutchings & Holt, 2015; Chu et al., 2010; Holt & Lampke, 2010; Hutchings & Holt, 2015). Betrouwbare mededaders kunnen worden gevonden dankzij de rating- en reviewsystemen die forums hebben (Soudijn & Zegers, 2012; Herley & Florencio, 2010; Wehinger, 2011; Yip et al., 2013; Lusthaus, 2012; Dupont et al., 2016; Décary-Hétu & Dupont, 2012, 2013;

Holt, 2013; Holt & Smirnova, 2014; Holt et al., 2015; Chu et al., 2010; Ablon et al., 2014).
Ten slotte speelt ook nog het punt dat ICT in zekere zin neutraal is en dat vaak pas de concrete toepassing ervan leidt tot illegale activiteiten. Dat biedt voor daders dus veel meer kansen voor samenwerking met de legale wereld, vooral in de 'grijze zone' tussen legale en illegale toepassingen van ICT. Uit onderzoek van Bijlenga en Kleemans (2017) blijkt dat criminelen soms gemakkelijk ICT-expertise weten te vinden in deze 'grijze zone', omdat bepaalde tools soms geheel legaal worden aangeboden, via internet of via Spyshops (waarbij ook nog extra dienstverlening aan criminele klanten plaatsvindt). Ook bij het aanpassen van tools (voor criminele doeleinden) hoeft voor experts op voorhand niet duidelijk te zijn waarvoor de tools uiteindelijk zullen worden gebruikt. Hierdoor kan gemakkelijk vrij zakelijke samenwerking tot stand komen (op basis van vraag en aanbod), via werkrelaties of via online of offline ontmoetingsplaatsen. Ook kunnen criminelen vrij snel 'to the point' komen, omdat het criminele karakter bij het begin van de samenwerking voor de betrokkene niet duidelijk zichtbaar hoeft te zijn of achteraf kan worden ontkend (Bijlenga & Kleemans, 2017). De neutraliteit van ICT maakt samenwerking in dat opzicht gemakkelijker.

Vertrouwen
Enerzijds blijken offline sociale relaties dus nog steeds van belang bij het ontstaan en groeien van cybercriminele netwerken. Blijkbaar kiezen daders nog steeds mededaders uit kringen van bekenden vanwege het vertrouwen dat nodig is om effectief samen te werken. Anderzijds bieden online ontmoetingsplaatsen een gelegenheidsstructuur waar nieuwe betrouwbare mededaders kunnen worden gevonden. Het kan daarbij gaan om kernleden of facilitators.
Met betrekking tot vertrouwen en online ontmoetingsplaatsen weten we dat erop gesloten forums al een goede reputatie is vereist om überhaupt binnen te komen. Om toegang te krijgen tot het forum worden de potentiële leden gescreend door administrators (of leden die door de administrator zijn aangewezen) en moeten de nieuwe leden bewijs aanleveren dat ze actief zijn op cybercrimegebied (bijvoorbeeld het aanleveren van gestolen creditkaartgegevens of een tutorial) (Soudijn & Zegers, 2012; Yip et al., 2013; Lusthaus, 2012; Ablon et al., 2014; Holt et al., 2015). Lusthaus (2012) legt daarnaast vooral de nadruk op de sociale mechanismen binnen een forum. Verder kan de reputatie van een lid worden afgelezen aan de status van dat lid. Bijvoorbeeld 'nieuw lid', 'verkoper' en 'geverifieerd verkoper'. Ten slotte kennen veel forums een reviewsysteem; leden die data, tools of diensten hebben gekocht, beoordelen de verkoper door middel van een geschreven review of een score op een rating schaal (Soudijn & Zegers, 2012; Herley & Florencio, 2010; Wehinger, 2011; Yip et al., 2013; Lusthaus, 2012; Dupont et al., 2016; Décary-Hétu & Dupont, 2012, 2013; Holt, 2013; Holt & Smirnova, 2014; Holt et al., 2015; Chu et al., 2010; Ablon et al., 2014).

Lokale inbedding
Er is nog niet veel onderzoek gedaan naar de lokale inbedding van cybercrime (zie o.a. Leukfeldt et al., 2017f; Lusthaus & Varese, 2017). Leukfeldt et al. (2017c, 2017d, 2017e) laten zien dat er in het geval van phishing- en malware-aanvallen op het betalingsverkeer in de regel wel sprake is van lokale inbedding. Dit is te zien bij zowel Nederlandse netwerken als netwerken die bijvoorbeeld vanuit Oost-Europese landen opereren. Cruciaal bij dit soort aanvallen zijn namelijk katvangers die rekeningen hebben of openen waarnaar geld van slachtofferrekeningen kan worden overgemaakt. Vervolgens wordt het geld cash opgenomen en witgewassen. Het valt op als er geld naar katvangers in andere landen wordt overgemaakt vanaf slacht-

offerrekeningen (want banken hebben betaalprofielen van klanten en kunnen zien of er vreemde transacties worden gedaan en die vervolgens tegenhouden). In hoofdstuk 4 wordt dieper ingegaan op criminele geldstromen.
De 'local hero' en internationale specialist zijn ook te zien bij de cybernetwerken (Leukfeldt et al., 2017c, 2017d, 2017e). Er zijn bijvoorbeeld netwerken waarvan alle kernleden, facilitators en slachtoffers zich binnen Nederland bevinden. Vaak zijn dit de netwerken die low-tech aanvallen uitvoeren, bijvoorbeeld phishingaanvallen. Niet altijd overigens, er zijn ook netwerken die gebruikmaken van geavanceerde malware om hun delicten te plegen waarbij vrijwel alle kernleden, facilitators en slachtoffers zich in één land bevinden. Daarnaast zijn er ook internationaal opererende specialisten te zien. Netwerken die goed gebruik weten te maken van de voordelen van forums kunnen nu relatief snel en met een kleine groep mensen groeien tot internationale spelers. Ook is te zien dat specialisten samenwerken in een ketensamenwerking, waarbij verschillende actoren (individuen of netwerken) verantwoordelijk zijn voor een specifiek deel van het crime script (Odinot et al., 2017).

2.3 Analyse van bestudeerde zaken: structuur en samenstelling van criminele samenwerkingsverbanden

In deze paragraaf gaan we in op de structuur en samenstelling van criminele samenwerkingsverbanden in de dertig nieuwe monitorzaken. We maken daarbij steeds onderscheid tussen traditionele georganiseerde criminaliteit (casus 157-172, 174-180), traditionele georganiseerde criminaliteit waarbij het gebruik van ICT een belangrijk vernieuwend element is (casus 151, 152 en 173), georganiseerde low-tech cybercriminaliteit (casus 154 en 156) en georganiseerde high-tech cybercriminaliteit (casus 153, 155).

Traditionele georganiseerde criminaliteit
Uit de eerdere rapporten op basis van de Monitor Georganiseerde Criminaliteit komt een duidelijk beeld naar voren van criminele netwerken die zich bezighouden met transitcriminaliteit, illegale internationale handel waarbij Nederland productieland, doorvoerland of bestemmingsland is (Kleemans et al., 1998, 2002; Van de Bunt & Kleemans, 2007; Kruisbergen et al., 2012). In het gros van de zaken blijkt georganiseerde criminaliteit te gaan om smokkel van mensen (vrouwenhandel, mensensmokkel) en verboden waar, zoals drugs, wapens en gestolen auto's, en om illegale grensoverschrijdende handelingen, zoals ondergronds bankieren en het ontduiken van heffingen en accijnzen. De nieuwe casussen uit deze ronde van de monitor die vallen binnen de categorie traditionele georganiseerde criminaliteit zijn in de regel ook te scharen onder de noemer transitcriminaliteit: drugshandel (casus 158, 159, 161-164, 167, 169-172, 175 en 176), witwassen (casus 157, 166, 168, 177, 178, 180) en mensensmokkel-/handel (casus 160). Uitzonderingen zijn casus 165 (criminele organisatie die het plegen van liquidaties tot oogmerk had) , casus 174 (drugs- en wapenhandel en afpersing) en casus 179 (overige delicten/fraude), die geen duidelijke internationale component hebben.
De casussen met betrekking tot traditionele georganiseerde criminaliteit laten dan ook geen afwijkend beeld zien ten aanzien van de casussen uit de eerdere monitorrapporten. Er is geen sprake van een maffia-achtige piramidale organisatiestructuur, maar wel van meer of minder gestructureerde criminele netwerken, waarbij er hoofdrolspelers en facilitators zijn waar anderen van afhankelijk zijn. De manier waarop wordt samengewerkt hangt ook af van de aard van de criminele activiteiten die worden uitgevoerd.

Traditionele georganiseerde criminaliteit met cybercomponent
Het netwerk uit casus 151 betreft een vrij traditioneel crimineel netwerk dat betrokken is bij internationale drugshandel, vergelijkbaar met zaken uit de voorgaande monitorronden. Er is sprake van een goed georganiseerde samenwerking waarbij criminelen in losstaande subgroepen met elkaar samenwerken. In het opsporingsonderzoek worden ongeveer vijftig personen gelinkt aan dit criminele samenwerkingsverband. Het verschil met andere netwerken die zich bezighouden met traditionele handel in drugs, is dat dit netwerk de diensten van twee hackers inzet om containers, waarin drugs zijn verstopt, in havens te lokaliseren en op te halen voordat het reguliere transportbedrijf dit doet.
Het opsporingsonderzoek richt zich op dader A en daaraan gerelateerde personen. A kan worden gezien als een van de kernleden van een crimineel samenwerkingsverband dat zich in opdracht van andere criminelen bezighoudt met het regelen van transporten cocaïne van Zuid-Amerika naar Nederland en België. A stuurt met andere kernleden een aantal personen aan die criminele diensten leveren. Zo hebben de kernleden contact met de leveranciers van drugs in Colombia, maken ze gebruik van tolken voor communicatie, maken ze (vermoedelijk) gebruik van personen die werkzaam zijn bij reders of binnen de haven om transportdocumenten te vervalsen en informatie te verkrijgen en sturen ze de chauffeurs aan die daadwerkelijk containers met drugs vervoeren alsmede de beveiligers die het transport bewaken. Ten slotte maken kernleden en facilitators gebruik van allerlei bedrijfsconstructies op naam van katvangers om onder de radar te blijven.
Het samenwerkingsverband uit deze casus lijkt met andere woorden heel sterk op traditionele samenwerkingsverbanden. Het enige verschil is dat er hackers worden ingezet om containers met drugs in havens te lokaliseren en op te pikken voordat het reguliere transportbedrijf dit doet.
In casus 152 staat een online marktplaats centraal waar gehandeld wordt in drugs en wapens. Het onderzoek richt zich op de Nederlandse leden die het online forum hebben ontwikkeld en beheren. Het gaat om drie kernleden en een facilitator.
Twee van de kernleden zijn de bedenkers van dit specifieke forum. Deze personen hebben een eerste versie van het forum ontwikkeld die niet goed genoeg was om te gebruiken. De twee kernleden hebben wel een hoge mate van ICT-kennis, maar hebben de hulp van een facilitator die een van de kernleden al jaren kent ingeroepen om het forum te realiseren. Zonder hem had het forum niet op deze manier kunnen functioneren. Het derde kernlid heeft geen ICT-kennis, maar wel een crimineel verleden en ervaring met drugshandel.
Het forum is opgesplitst in een marktplaatsgedeelte en een discussiegedeelte. Binnen het marktplaatsgedeelte wordt bijvoorbeeld drugs aangeboden. Verkopers plaatsen advertenties van hun waren en kopers kunnen contact opnemen met de verkopers. In het discussiegedeelte kunnen leden informatie vinden over tal van onderwerpen, bijvoorbeeld de beste manier om drugs te verzenden, zelf discussieonderwerpen aanmaken en informatie vinden over verkopers.
Binnen het forum zijn verschillende lagen en rollen te herkennen. Bovenaan de hiërarchie staat de administrator. De administrator is de beheerder van het forum. Een van de kernleden is de administrator van dit forum. Onder de administrator staan moderators die verantwoordelijk zijn voor delen van het forum. Moderators hebben een voorbeeldfunctie voor medegebruikers van een forum. Ze zorgen dat leden zich gepast gedragen, reageren op vragen van gebruikers en kunnen statussen van leden aanpassen of bepaalde leden de toegang tot het forum ontzeggen. Twee van de kernleden worden gezien als moderators van het forum. Ten slotte zijn er kopers en verkopers op het forum. De verkopers plaatsen advertenties met hun waren. Na een verkoop kan de koper een review opstellen waarmee de verkoper wordt beoordeeld. Hierdoor kunnen andere kopers zien of ze te maken hebben met

een betrouwbare verkoper. De kernleden die de functie van administrator en moderator hebben beheren niet alleen het online forum, maar bieden zelf ook drugs en wapens aan via het online forum. De leveringen van illegale waar lijken zich vooral te richten op klanten in Europese landen.
Het samenwerkingsverband uit deze casus vormt de georganiseerde 'achterkant' van een forum dat zij beheren en waar zij zelf ook op handelen. De mogelijkheden om te handelen worden daarmee uitgebreid en tevens wordt aan het forum verdiend.
De criminele groepering uit casus 173 houdt zich bezig met het omwisselen van bitcoins naar cash geld. De bitcoins zijn vermoedelijk onder meer verkregen door de verkoop van drugs op online criminele markten op het darkweb.
Het opsporingsonderzoek richt zich op vijf hoofdverdachten die gedurende een langere periode gezamenlijk en individueel bitcoins omwisselen. De hoofdverdachten hebben advertenties geplaatst op verschillende online platformen waarin ze adverteren met de mogelijkheid om contant geld te krijgen voor bitcoins. De advertenties stonden op publiek toegankelijke websites, maar gezien de klanten van de groepering werd er waarschijnlijk ook op forums op het darkweb geadverteerd. Deze bitcoinwisselaars fungeren feitelijk als facilitators voor allerlei andere netwerken en zelfstandig opererende criminelen.
In dit opsporingsonderzoek komt alleen de samenwerking met een aantal online drugshandelaren aan bod. Ondanks dat een van de kernleden wordt aangeduid als coördinator in het opsporingsonderzoek, lijkt er geen sprake te zijn van een duidelijke hiërarchie binnen de groep kernleden. De kernleden werken soms samen, maar vaak ook zelfstandig voor eigen klanten. Om de bitcoins om te wisselen naar cash geld zetten de kernleden katvangers in die hun rekening ter beschikking stellen (in hoofdstuk 4 wordt uitgebreid ingegaan op deze casus).

Georganiseerde cybercriminaliteit: low-tech
Het netwerk uit casus 154 houdt zich bezig met het aanpassen van kaartlezers van een Nederlandse bank die nodig zijn voor het inloggen op online bankrekeningen.

> *Het netwerk bestaat uit drie lagen: vijf kernleden, één facilitator en zes uitvoerders. Dit netwerk werkt in deze samenstelling ongeveer 1,5 jaar samen. Binnen de groep kernleden is sprake van een hiërarchie. Eén kernlid is coördinator en heeft contacten met de facilitator. Deze facilitator werkt vanuit Engeland voor meerdere netwerken en levert cruciale diensten aan het netwerk. De kernleden hebben namelijk zelf geen technische kennis en zijn afhankelijk van de facilitator. Deze facilitator past de kaartlezers aan, geeft de kernleden duidelijke instructies hoe ze moeten handelen en beheert de database met gegevens die worden verkregen door het gebruik van de aangepaste kaartlezers. De andere kernleden worden beschreven als teamleiders die teams van uitvoerders aansturen. Deze 'uitvoerders' gaan fysieke bankfilialen binnen om de kaartlezers om te wisselen en na verloop van tijd weer op te halen.* (Casus 154)

Het netwerk uit casus 156, dat zich bezighoudt met phishingaanvallen op klanten van Nederlandse banken, bestaat uit vier lagen. Het netwerk bestaat uit een groep kernleden, professionele facilitators, gerekruteerde facilitators en katvangers. De acht kernleden werken in min of meer vaste samenstelling samen gedurende een periode van in ieder geval anderhalf jaar (de duur van het opsporingsonderzoek). Opvallend is dat geen van de kernleden een hoge mate van ICT-expertise heeft. In tegenstelling tot de malware netwerken uit casus 153 en 155, gebruiken de kernleden geen forums om aan facilitators met technische kennis te komen. De kernleden maken gebruik van een vriend van een kennis van een kernlid uit Nigeria die

phishingwebsites van Nederlandse banken kan bouwen. Verder maken de kernleden gebruik van een facilitator die valse identiteitsbewijzen levert. Hoe het contact met deze facilitator tot stand is gekomen blijft onduidelijk. Daarnaast maken de kernleden gebruik van de diensten van tal van anderen, waaronder personen die werken op callcenters van Nederlandse banken die informatie van rekeningen aanleveren en pinlimieten kunnen verhogen, postmedewerkers die aangevraagde inloggegevens kunnen onderscheppen, personen die potentiële slachtoffers opbellen om hen transactiecodes te ontfutselen en personen die katvangers ronselen of het cashingproces begeleiden. Al deze personen worden via-via geworven (meer hierover in paragraaf 2.4). De onderste laag van het netwerk uit casus 156 bestaat uit katvangers die hun bankrekening ter beschikking stellen aan de kernleden van de criminele groep. De katvangers worden gebruikt om het spoor van de slachtoffers naar de kernleden te onderbreken.

Georganiseerde cybercriminaliteit: high-tech

Zowel het netwerk uit casus 153 als het netwerk uit casus 155, dat met behulp van malware geld steelt van online bankrekeningen van klanten van Nederlandse banken, kent vier lagen. De bovenste laag bestaat uit de kernleden van het netwerk. Deze personen sturen de anderen binnen het netwerk aan en coördineren de aanvallen.

Bij casus 153 gaat het om vier kernleden, in casus 155 om vijf kernleden. Bij beide netwerken blijken de kernleden geen uitzonderlijk hoge mate van technische kennis te hebben. Wel hebben enkele kernleden duidelijk affiniteit met de criminele mogelijkheden die ICT biedt. Ze zijn bijvoorbeeld actief op forums waar informatie over het plegen van allerlei vormen van cybercrime kan worden gevonden en ze downloaden video's waarin staat uitgelegd hoe bepaalde vormen van malware werken. Een voorbeeld is te zien in het volgende chatgesprek tussen twee van de kernleden van netwerk 153:

> *Nadat B aan A een video had verstuurd, waarin het gebruik en de werking van een kwaadaardig webinject bij een site van een Duitse bank werd gedemonstreerd, vond via een chatprogramma de volgende conversatie plaats tussen A en B:*
> *(A): Dat filmpje ziet er gruwelijk uit, maar snap er niks van, ik snap niet hoe je iemands rekening kan plunderen van [banknaam].*
> *(B): TAN-codes komen via sms togg.*
> *(A): Je moet toch zijn [bank] inlogs hebben?*
> *(B): Je krijgt die exe en deze panel en die intercept die logins, je moet het zien als een inject. Wanneer eigenaar probeert in te loggen.*
> *(A): Hoe infect jij zijn mobiel en pc?*
> *(B): Het wordt gwn gelinked aan een botnet, gwn als normale inject.*
> *(A): Ik snap niet, ik log in op [bank].nl he? Dan krijg ik zo'n scherm te zien dat ik laatste 3 digits van me telefoonnummer moet invoeren toch? Dan hoe infect jij zijn mobiel om die sms'jes te onderscheppen?*
> *(B): Nadat jij je nummer hebt ingevoerd moet je ook je type mobiel selecteren. Daarna zie je een link om te downloaden of er wordt een sms naar je mobiel gestuurd.*
> *(A): Maar nu hebben we alles toch al, heb je software gekocht?*
> *(B): Ja man het werkt*
> (Casus 153)

In de laag 'onder' (of naast) de kernleden bevinden zich de professionele facilitators. Deze personen bieden hun criminele diensten aan meerdere netwerken aan.

In zowel casus 153 als casus 155 maken kernleden gebruik van online forums om facilitators met een hoge mate van technische expertise te vinden. Gezien de beperkte(re) technische kennis van de kernleden is dit noodzakelijk om de malware-aanvallen uit te kunnen voeren. Het netwerk uit casus 153 maakt gebruik van diverse facilitators, onder meer om malware aan te schaffen, om een botnet te huren en om valse identiteitsbewijzen te kopen. Het netwerk uit casus 155 maakt alleen gebruik van een forum om een specifieke vorm van malware te kopen. Een van de kernleden past die vervolgens zelf aan om Nederlandse banken aan te vallen.
De netwerken uit casus 153 en 155 maken daarnaast ook gebruik van de diensten van personen die deze diensten niet aan allerlei netwerken aanbieden. Deze personen zijn gerekruteerd door de kernleden en bevinden zich in de regel binnen het sociale netwerk van een of meerdere kernleden. Het netwerk uit casus 153 maakt bijvoorbeeld gebruik van een postbode die pakketjes onderschept die zijn aangekocht middels frauduleuze overboekingen vanaf rekeningen van slachtoffers. Deze postbode is de buurjongen van een van de kernleden. Het netwerk uit casus 155 maakt gebruik van een persoon die katvangers ronselt. Deze katvangers stellen hun rekening beschikbaar aan de kernleden zodat geld van slachtofferrekeningen contant kan worden opgenomen. De ronselaar is al langer betrokken bij criminele activiteiten, waardoor hij een van de kernleden, die zich eerder bezig heeft gehouden met faillissementsfraudes, kent.
De onderste laag van de netwerken uit casus 153 en 155 bestaat uit katvangers die hun rekening ter beschikking stellen aan kernleden. De katvangers worden gebruikt om het spoor van de slachtoffers naar de kernleden te onderbreken. Op de rekeningen van de katvangers wordt geld overgemaakt dat afkomstig is van de rekeningen van slachtoffers. Daarna wordt het geld zo snel mogelijk cash opgenomen. De katvangers worden binnen de sociale netwerken van kernleden en facilitators geworven. Daarbij worden zowel offline sociale contacten (mensen uit de buurt, etc.) als online sociale contacten (oproepen op sociale media) gebruikt. Een van de ronselaars van het netwerk uit casus 155 rekruteert bijvoorbeeld nieuwe money mules onder kennissen. Als iemand meewerkt, worden ook de vrienden van die persoon benaderd. Uit communicatie tussen de kernleden blijkt dat ronselaars bewust op zoek zijn naar personen die gemakkelijk zijn te beïnvloeden, bijvoorbeeld personen met hoge schulden of psychische problemen of drugsverslaafden. In het dossier zijn voorbeelden te vinden van een katvanger met schulden, een dakloze en iemand in een begeleid-wonen traject.

2.4 Analyse van bestudeerde zaken: instroom- en doorgroeimechanismen

In deze paragraaf bespreken we hoe de criminele samenwerking tot stand kwam, hoe nieuwe leden en facilitators worden gerekruteerd, hoe vertrouwen wordt gewonnen en in hoeverre de criminele netwerken lokaal zijn ingebed.

Traditionele georganiseerde criminaliteit
De vorige rapportages van de monitor toonden het belang van bestaande sociale relaties binnen criminele netwerken. Familie- en vriendschapsrelaties zijn vaak van cruciaal belang bij de totstandkoming en groei van criminele netwerken: familie, vrienden en bekenden werken met elkaar samen en introduceren elkaar weer bij anderen. Daar waar bestaande sociale relaties tekortschieten, worden 'buitenstaanders' ingezet (anderen dan familieleden, vrienden of vaste zakenpartners). Criminele ontmoetingsplaatsen spelen hierbij een belangrijke rol.

De nieuwe casussen met betrekking tot traditionele georganiseerde criminaliteit laten geen afwijkend beeld zien ten aanzien van de casussen uit de eerdere monitorrapporten. Ook in deze casussen is het belang van sociale relaties duidelijk terug te zien evenals het belang van criminele ontmoetingsplaatsen. Is dit echter ook het geval bij traditionele georganiseerde criminaliteit met een cybercomponent en bij low-tech en high-tech cybercriminaliteit?

Traditionele georganiseerde criminaliteit met een cybercomponent
Casus 151 betreft een crimineel netwerk dat betrokken is bij internationale drugshandel. Het gaat om een criminele groep die zich, al dan niet in subgroepen, al langer bezighoudt met drugshandel en andere criminele activiteiten. De meeste verdachten zijn uit Nederland afkomstig, maar er zijn ook personen betrokken uit België, Spanje, Turkije, Kaapverdië, Servië, Albanië, Bulgarije, Indonesië en Colombia. Hoe het netwerk precies is ontstaan, is onduidelijk. Wel lijkt er sprake te zijn van een vrij klassiek voorbeeld van een crimineel samenwerkingsverband waarbij sociale banden een belangrijke rol spelen (zie paragraaf 2.1). Wat een groot deel van de ongeveer 50 personen die gelinkt worden aan dit criminele samenwerkingsverband gemeen hebben, zijn antecedenten op het gebied van drugs. Naast het gegeven dat een deel van de leden van het criminele samenwerkingsverband al langer actief is in het criminele milieu en elkaar daar hebben leren kennen, is er sprake van verschillende familie- en vriendschapsrelaties binnen het netwerk.

> *Zo is C een broer van T. E is de echtgenoot van Z. W is de zoon van X. ZZ is de vader van ZY. ZR is de vader van ZQ. ZM is de ex-zwager van B. ZV zegt X en O al twintig jaar van het voetballen te kennen. N kent M al vijf jaar vanuit de kroeg. Ook ZI zegt G te kennen vanuit de kroeg.* (Casus 151)

Wat dit criminele samenwerkingsverband bijzonder maakt is dat de kernleden gebruikmaken van twee hackers om containers met drugs ongezien op te pikken bij havens. Het gaat om twee buitenlanders die door een Nederlandse bank waren ingehuurd om systemen te ontwikkelen. Eén verdachte speelt vermoedelijk een cruciale rol bij de totstandkoming van de contacten tussen de ICT-specialisten en de leden van het criminele netwerk. Het is onbekend hoe en waarom deze verdachte contact opnam met deze twee ICT-specialisten.
Het criminele samenwerkingsverband uit casus 152 houdt zich ook bezig met drugshandel, maar gebruikt daarvoor een online forum. De drie kernleden zijn de ontwikkelaars van het forum en hebben rollen als administrator en moderator. Dader B, die volgens eigen zeggen een bijzondere ziekte heeft en niet uit huis komt, lijkt de spil te zijn waardoor de kernleden bij elkaar zijn gekomen. B en C, die in Duitsland woonachtig is, kennen elkaar via forums. Ze waren allebei eerder actief op een forum waarin in drugs werd gehandeld. Toen dat forum offline dreigde te gaan, besloten deze kernleden een nieuw online platform te ontwikkelen. B en A, een persoon met een crimineel verleden die al jaren actief is in de drugshandel, kennen elkaar ook al jarenlang. Het is onduidelijk hoe dit contact is ontstaan. Ondanks dat twee kernleden zelf kunnen programmeren en een hoge mate van technische expertise hebben, lukt het ze niet om een goed platform te bouwen. Daar hebben ze de hulp van E voor nodig. Ook dit kernlid kent B via online forums.
B en E vonden elkaar in een gedeelde interesse voor bitcoins en het minen ervan. Ze hadden in het verleden ook al eens samen geprogrammeerd en aan gesprekstof was geen gebrek. B wilde de programmeerexpertise van E graag gebruiken. Het begon met 1 module programmeren en vervolgens volgden er snel meer. Op een bepaald moment werd een punt bereikt waarop B zelf geen wijzigingen meer kon

aanbrengen omdat zijn kennis hiervoor tekortschoot. B heeft de server bij hem thuis staan:

> *'Voor mij [E] is zulke hardware alsof je als kind in een speelgoedwinkel bent en overal mee mag spelen. (…) Ondertussen werd er op internet gesproken over [naam forum] op diverse forums. Blijkbaar waren de verwachtingen erg hoog want er werden enkele lovende berichten geplaatst. Als developer gaf mij dit een soort van compliment. Een compliment dat ik op mijn werk zelden ontvang.'* (Casus 152)

De drie kernleden verkopen zelf ook drugs via het forum. Soms versturen ze verkochte waren per post, maar ze zetten ook twee koeriers in (D en F), als de klanten zich bevinden in Nederland of directe buurlanden.
Vertrouwen op het forum wordt op verschillende manieren gefaciliteerd. Ten eerste kan de koper een review van de verkoper geven. Daardoor kunnen andere potentiële kopers inschatten of de verkoper betrouwbaar is. Verder maakt het forum gebruik van een zogenoemde *escrow service*, waardoor veilig kan worden betaald. Zodra een koper een bestelling heeft geplaatst via de website, geeft de koper aan bij de verkoper naar welk adres de bestelling dient te worden verzonden. Het aantal bitcoins dat de koper aan de verkoper is verschuldigd, wordt van het saldo van de koper afgeboekt. Deze gaan echter niet direct naar de verkoper, maar worden in bewaring gehouden door de beheerder van de website. De verkoper krijgt van de beheerder de melding dat zij de verschuldigde bitcoins in bewaring hebben ontvangen. Zodra de bestelling is aangekomen bij de verkoper, zal de verkoper dit doorgeven aan de beheerder. Deze zorgen vervolgens voor de uitbetaling aan de verkoper. Wanneer een bestelling niet aankomt bij de koper, treedt de beheerder op als bemiddelaar en doet een voorstel waar beide partijen mee akkoord gaan. In de praktijk houdt dit in dat er vaak een deel van de in bewaring gegeven bitcoins wordt teruggegeven aan de koper en een deel wordt uitbetaald aan de verkoper.
Tussen de kernleden is geen sprake van wantrouwen of dreigen met geweld, maar uit tapgesprekken en observaties blijkt wel dat A met een aantal leveranciers en afnemers van drugs ruzie maakt om geld en deze personen bedreigt. Zo dreigt hij een afnemer die niet betaald heeft om een paar mannen te sturen die het probleem wel zullen oplossen.
De criminele groepering uit casus 173 houdt zich onder meer bezig met het omwisselen van bitcoins die verkregen zijn door de verkoop van drugs op online criminele markten op het darkweb naar cash geld. De kernleden van de groep bitcoinwisselaars kennen elkaar allemaal via offline sociale relaties. Drie van de kernleden hebben een aantal jaar dezelfde bijbaan gehad bij een groothandel in voedsel. Door gelijke interesse zijn ze daar in contact gekomen met elkaar en is een vriendschap ontstaan. Een van de kernleden zegt hierover:

> *'Ik heb [A] met anderen horen praten over de wereldpolitiek. Je hoort niet vaak dit soort gesprekken op dit soort werk en ik houd van dit soort onderwerpen, daarom ben ik een gesprek met hem aangegaan en zo zijn we begonnen verder met elkaar om te gaan. (…) In het voorjaar van (…)zijn we begonnen over ondernemerschap te praten. Ten eerste heb ik hem verteld welke activiteiten ik verricht in mijn eigen onderneming. Hij werd daar heel erg in geïnteresseerd. Hij was op dat moment geïnteresseerd in actuele politieke onderwerpen en situatie in de wereld. Hij was geïnteresseerd in het concept van bitcoinvaluta: hoe deze valuta functioneert, beheerd wordt en hoe deze valuta de economie beïnvloedt. Hij was ook geïnteresseerd in de mogelijkheden van aanvullende inkomsten. Ik heb hem verteld dat ik hem kennis kon laten maken met handel in bitcoin. Hij nam dat*

aanbod graag aan. Vanaf dat moment werden we nog closer. Geleidelijk begon hij zelf ook goed te begrijpen hoe de bitcoinhandel in elkaar zit en vanaf dat moment ging hij zelf investeren in bitcoinvaluta.' (Casus 173)

De andere twee wisselaars zijn een broer en een jeugdvriend van de drie kernleden. De wisselaars gebruiken (onder andere) de bankrekeningen van katvangers om te cashen. Dader A, die gezien wordt als de coördinator van de wisselaars, maakt daarbij vooral gebruik van mensen uit een specifieke bevolkingsgroep. Ook daar zijn weer duidelijke offline banden te zien.
Het opsporingsonderzoek richt zich daarnaast specifiek op een aantal drugsdealers die gebruikmaken van online markten op het darkweb om hun illegale waar te verkopen. De drugs die worden verkocht op de online markten worden betaald met (onder andere) bitcoins. Voor het omwisselen van deze cryptovaluta voor 'echte' munten maken de verkopers gebruik van de diensten van de bitcoinwisselaars.
De eerste contacten tussen de handelaren in drugs en de bitcoinwisselaars zijn online, de bitcoinwisselaars hadden namelijk advertenties op forums, maar vervolgens volgen al snel ontmoetingen in de fysieke wereld. Tijdens fysieke ontmoetingen, die vaak plaatsvinden in vestigingen van bijvoorbeeld Starbucks of McDonalds, maakt ter plekke de ene partij bitcoins over naar de wallet van de andere partij. Vervolgens wordt cash geld overhandigd. Dat geld heeft de bitcoinwisselaar daarvoor gepind (in meerdere, kleinere bedragen) of al contant bij zich. Om te kijken of nieuwe klanten betrouwbaar zijn, stellen de bitcoinwisselaars vragen en controleren ze reviews en andere beschikbare informatie over de nieuwe klanten. Verder blijkt dat ze langdurig zakendoen met een paar vaste klanten waar ze soms voor tienduizenden euro's per week voor omwisselen.
In de relatie tussen de leden van de groep bitcoinwisselaars is geen sprake van achterdocht of geweld. De leden lijken elkaar te vertrouwen doordat er sprake is van een gedeelte interesse, langdurige vriendschappen, gemeenschapsbanden en familiebanden. In de contacten tussen de bitcoinwisselaars en de verkopers van drugs is wel sprake van enige voorzichtigheid. Bij nieuwe klanten proberen de bitcoinwisselaars erachter te komen of ze met een betrouwbaar persoon te maken hebben. Ze stellen vragen om erachter te komen of de persoon wel weet waar hij of zij mee bezig is (of ze weten hoe bitcoins werken, etc.), ze checken zijn reviews en zoeken andere informatie over de nieuwe klanten. Dader A zegt hierover:

'… Soms bij het verifiëren van de in bitcoinwallet (portemonnee) zijnde accounts van welke de bitcoins afkomstig zijn, kunnen een zeer stabiele en vergelijkbare grote transacties geconstateerd worden. Dat toont handelsactiviteiten aan dat er steeds iets wordt gekocht en verkocht en dat gebeurt op darknet.' (Casus 173)

Bovendien geeft dader A aan vragen te stellen aan nieuwe klanten om te achterhalen of die persoon te vertrouwen is. Iemand die beweert bitcoins te minen, terwijl deze nauwelijks iets weet over de processen van mining, zou snel door de mand vallen. Een andere methode die de partijen hanteren om misbruik tegen te gaan, is dat zij beginnen met kleine transacties en – als het goed gaat – wordt de omvang vergroot. D zegt het volgende hierover:

'… in eerste instantie doe je een kleine transactie. Vaak meerdere kleinere transacties achtereen. Als ik iemand langer ken dan voel ik mij prettiger om met deze persoon ook grotere transacties te doen. Ik geef het geld in een envelop. Het hangt van de persoon af of hij/zij het wil uittellen …' (Casus 173)

Ontmoetingen vinden plaats op openbare plaatsen waar veel mensen komen. Volgens eigen zeggen om te voorkomen dat de bitcoinwisselaars worden overvallen. De bitcoinwisselaars lijken ook bewust voor plekken zoals een koffietentje op een station in een grote stad te kiezen omdat daar openbare wifi-netwerken aanwezig zijn waardoor bitcoins anoniem kunnen worden overgemaakt. Dader A neemt daarnaast vaak iemand mee om een oogje in het zeil te houden. C en F zijn broers die ook vaak samen optrekken. In het dossier wordt één keer een voorbeeld gegeven van een *rip deal*, waarbij A zou zijn overvallen.
Ondanks het mondiale karakter van het darknet en van bitcoins bedienen de bitcoinwisselaars in dit opsporingsonderzoek een beperkte markt. De Nederlandse bitcoinwisselaars werken vooral voor klanten in Nederland, België, Duitsland, Italië, Noord-Frankrijk en Luxemburg.

Georganiseerde cybercriminaliteit: low-tech
Het netwerk uit casus 154 bestaat uit vijf kernleden, een facilitator en een aantal 'uitvoerders'. De kernleden en de uitvoerders zijn aan elkaar verbonden door familie- en vriendschapsbanden. Het gaat hoofdzakelijk om Roemenen die in Nederland verblijven en uit dezelfde regio in Roemenië afkomstig zijn. C en F zijn bijvoorbeeld broers. C, D en H kennen elkaar al langer als vrienden die samen zijn opgegroeid. C heeft bij het arriveren van de broer van D voor I een baan in de bouw geregeld. H en I hebben op dezelfde basisschool gezeten. B, C en H zijn in Roemenië al eens opgepakt wegens traditionele skimactiviteiten (het plaatsen van skimapparatuur bij betaalautomaten). Het enige lid dat geboren en getogen is in Nederland heeft een relatie gehad met een kennis van D.
De leden van deze criminele groep zijn constant bezig met het zoeken naar nieuwe mogelijkheden om geld te verdienen. Een aantal van hen werkt in de bouw, maar ze werkten ook deels al onderling samen op het gebied van mensenhandel, prostitutie en drugshandel. Op een gegeven moment koopt B van een criminele groepering uit Engeland de gegevens van geskimde bankpassen. Deze blijken echter niet te werken. Via contacten in het criminele milieu komt hij in contact met A. A werkt vanuit Engeland voor verschillende lokale groepen die zich bezighouden met skimmen en ontwikkelt zelf software voor skimapparatuur, geeft de kernleden instructies en beheert de database met geskimde gegevens.
Binnen de groep kernleden is geen sprake van geweld. Wel is een aantal gewelds-incidenten te linken aan een van de kernleden. Dit kernlid deinst er niet voor terug om geweld te gebruiken of ermee te dreigen wanneer een medeverdachte niet doet wat het kernlid wil.
Casus 156 betreft een netwerk dat phishingaanvallen uitvoert. Kenmerkend voor dit netwerk is dat de leden elkaar allemaal via-via uit de offline wereld kennen. Dat geldt voor de kernleden maar ook voor de facilitators en katvangers die worden ingezet. Leden kennen elkaar bijvoorbeeld doordat ze familiebanden hebben, uit dezelfde buurt komen en daar rondhangen op straat, of doordat ze op dezelfde school of sportvereniging zitten.
Hoe de acht kernleden elkaar ooit ontmoet hebben is onduidelijk, maar ze komen allemaal uit dezelfde Amsterdamse buurt en zijn al lange tijd actief in het criminele circuit. Uit het opsporingsonderzoek blijkt bijvoorbeeld dat ze in wisselende samenstelling allerlei andere criminele activiteiten uitvoeren of hebben uitgevoerd, bijvoorbeeld drugshandel, skimmen en fraude met telefoonabonnementen.
Facilitators zoals bankmedewerkers die informatie van rekeningen aanleveren en pinlimieten kunnen verhogen en de postmedewerker die aangevraagde inloggegevens kan onderscheppen, zijn gericht geronseld door de kernleden of mensen die de kernleden kennen: ze worden op straat meermaals aangesproken en gevraagd om mee te werken. De bankmedewerkers woonden in de buurten waar de kernleden

ook actief waren. De bankmedewerkers geven tijdens verhoren aan dat hun simpelweg werd gevraagd om informatie te geven over rekeningnummers. Daarbij werd de bankmedewerkers een financiële vergoeding in het vooruitzicht gesteld. Soms werd eerst een smoesje gebruikt om erachter te komen of een bankmedewerker bij gevoelige informatie kon, bijvoorbeeld: 'Ik krijg nog geld van mijn ex. Ze zegt dat ze geen geld heeft, maar dat geloof ik niet. Kan jij dat niet even checken?' Zodra bekend was dat de verdachte inderdaad bij bepaalde informatie kon komen, werd druk uitgeoefend om daadwerkelijk informatie te geven.
Ook het ronselen van katvangers die hun rekening ter beschikking stellen om geld te cashen gaat via-via. Er wordt op schoolpleinen, op sportclubs en tijdens het uitgaan openlijk gevraagd naar pasjes. Ook gebruiken de kernleden en ronselaars waar ze mee werken sociale media om bekenden en onbekenden te benaderen. Verschillende katvangers geven aan dat het vrij normaal is dat ze werden benaderd door mensen om hun pasje af te staan.

Georganiseerde cybercriminaliteit: high-tech
Casus 153 en casus 155 hebben betrekking op criminele groepen die met behulp van malware de online bankrekeningen van klanten van Nederlandse banken proberen leeg te roven. In beide casussen gaat het om Nederlandse kernleden die online forums gebruiken om malware aan te schaffen. De kernleden kennen elkaar via offline en online sociale contacten.
In casus 153 gaat het bijvoorbeeld om vier kernleden die elkaar kennen via sociale contacten. A en B zijn de kernleden die het technische gedeelte van het delict uitvoeren. Ze schaffen de malware aan, passen deze aan en coördineren de aanvallen. Hoe de twee met elkaar in contact zijn gekomen is onduidelijk. Wel studeren ze allebei commerciële economie aan verschillende hogescholen. B en D kennen elkaar van school. A en C kennen elkaar 'uit de rap scene'. Daar wordt openlijk gepraat over het verdienen van geld door het ter beschikking stellen van bankpassen waar dan iemand geld op zet. C geeft aan A in eerste instantie via sociale media te hebben benaderd. De kernleden maken gebruik van een postbode die pakketjes onderschept die zijn aangekocht door middel van frauduleuze overboekingen vanaf rekeningen van slachtoffers. Deze postbode is de buurjongen van een van de kernleden. Katvangers kennen ze ook via offline sociale contacten, maar er worden volgens het dossier ook contacten gelegd via sociale media en online games.
De twee kernleden die verantwoordelijk zijn voor het technische gedeelte van het delict hebben zelf niet de beschikking over genoeg technische expertise om de malware-aanval uit te voeren. Wel hebben twee van de kernleden 'affiniteit met deze materie' en zijn ze actief op forums. Zo weten ze de juiste facilitators te bereiken en geschikte tools aan te schaffen. A heeft bijvoorbeeld via forums contacten met personen die inloggegevens van klanten van Nederlandse banken kunnen leveren. Met deze personen discussieert hij ook over de mogelijkheden om goederen in webwinkels aan te schaffen met gestolen creditkaartinformatie. Twee andere online contacten zijn de ontwikkelaar of verkoper van malware die de groep gebruikt om zelf toegang te krijgen tot online rekeningen en de beheerder van het botnet waar de geïnfecteerde computers onderdeel van uitmaken. Beide contacten krijgen een deel van de opbrengst van de malware-aanvallen. Ten slotte kent A een Rus die identiteitspapieren vervalst. Alle contacten die beginnen op forums worden voortgezet via chatprogramma's waarbij de communicatie is versleuteld.
Casus 155 betreft een netwerk van vijf kernleden die allemaal banden hebben uit de offline wereld. A, die gezien kan worden als de coördinator van dit netwerk, heeft contacten met zowel iemand met een technische achtergrond (E) als personen met een financiële achtergrond (B en C). Al deze personen kent hij omdat ze voor dezelfde bedrijven hebben gewerkt. Het laatste kernlid (D) heeft al een lange criminele

carrière en heeft daardoor contacten met een professionele facilitator die opereert vanuit Engeland en die door middel van bedrijfsconstructies geld kan wegsluizen, een Nederlandse ronselaar van katvangers en een eigen netwerk van katvangers die kunnen worden ingezet om geld te cashen.

2.5 Recapitulatie

In dit hoofdstuk zijn wij nagegaan wat we uit voorgaand empirisch onderzoek weten over criminele samenwerking bij georganiseerde criminaliteit en in hoeverre de literatuur over cybercrime dezelfde of andere beelden oplevert. Daarna hebben wij de criminele samenwerkingsverbanden uit de 30 nieuwe monitorzaken geanalyseerd, waarbij onderscheid is gemaakt tussen de volgende categorieën: traditionele georganiseerde criminaliteit, traditionele georganiseerde criminaliteit waarbij het gebruik van ICT een belangrijk vernieuwend element is, georganiseerde low-tech cybercriminaliteiten en georganiseerde high-tech cybercriminaliteit.
De meeste netwerken binnen de monitorzaken van de vijfde ronde kennen een min of meer vaste groep kernleden die gedurende een langere periode samenwerken. Ook is er binnen de meeste netwerken sprake van meer en minder belangrijke verdachten en afhankelijkheidsrelaties.
Wat opvalt bij de vergelijking met de casussen van traditionele georganiseerde criminaliteit is het belang van technische kennis en technische vaardigheden. Opvallend is dat de betrokken daders zelf vaak niet veel technische kennis bezitten, maar deze kennis wel weten te verkrijgen via facilitators.
Bij de high-tech cybercriminaliteit komen kernleden aan de benodigde technische expertise door het gebruik van forums, bij de low-tech cybercriminaliteit maken daders gebruik van contacten die ze hebben in het criminele milieu. Het zoeken naar technische kennis vindt in het eerste geval dus plaats via online interacties en in het laatste geval door offline interacties.
Over het algemeen is bij de zaken uit de vijfde monitorronde duidelijk dat offline sociale relaties een belangrijke rol spelen binnen de instroom- en doorgroeimechanismen. Met name kernleden kennen elkaar dankzij hun offline sociale netwerken. Er zijn echter ook voorbeelden te zien waarbij sociale-mediaplatformen en online games worden gebruikt om contacten te leggen.
Kenmerkend voor een deel van de netwerken die zich bezighouden met het plegen van cybercrime of die zich bezighouden met traditionele criminaliteit met een vernieuwende ICT-component is dat dergelijke netwerken wat samenstelling betreft vaak een 'mix' zijn. Enerzijds gaat het om personen die hun sporen al hebben verdiend met het plegen van traditionele criminaliteit en allerlei contacten hebben in de onderwereld. Anderzijds zijn er vaak slechts weinig leden met een zekere mate van technische expertise. Met name bij high-tech netwerken spelen online forums daarom een belangrijke rol bij het vinden van facilitators die beschikken over technische expertise die bij de kernleden ontbreekt.
Ten slotte blijkt dat er bij bijna alle casussen sprake is van lokale inbedding. Dat dit zo is bij traditionele offline georganiseerde criminaliteit, wisten we al uit eerdere rapportages op basis van de Monitor Georganiseerde Criminaliteit. Bij andere casussen is deze lokale inbedding minder voor de hand liggend. Netwerken die zich bezighouden met cybercrimes, zowel de high-tech als low-tech varianten, kenmerken zich bijvoorbeeld door kernleden die afkomstig zijn uit Nederland en elkaar hebben leren kennen in de offline wereld. Deze kernleden weten zich te bewegen op forums op het darkweb, maar rekruteren ook facilitators en katvangers binnen hun eigen offline sociale netwerk. Ten slotte lijken de transacties van de Nederlandse online verkopers van drugs zich voornamelijk te richten op klanten in Europese landen.

De bitcoinwisselaars die werken voor mensen die handelen op internationale online drugsmarkten, werkten vooral voor klanten die relatief dichtbij zijn en zich bevinden in Nederland, België, Duitsland, Italië, Noord-Frankrijk en Luxemburg.

3 De logistiek van het criminele bedrijfsproces en het gebruik van ICT

Welke invloed heeft het gebruik van ICT op de logistiek van criminele activiteiten? Zoals in de vorige rapportages op basis van de Monitor Georganiseerde Criminaliteit werd beschreven, kent ieder crimineel bedrijfsproces logistieke bottlenecks; logistieke problemen die moeten worden opgelost om de criminele activiteiten succesvol te laten verlopen (zie voor een overzicht: Kruisbergen et al., 2012, p. 81-152). Welke rol speelt ICT hierbij en welke veranderingen brengt het gebruik van ICT met zich mee?
In paragraaf 3.1 geven we eerst een overzicht van wat er bekend is uit de literatuur over georganiseerde criminaliteit en logistiek. Daarna gaan we in paragraaf 3.2 aan de hand van de literatuur dieper in op ICT en de relatie tussen georganiseerde criminaliteit en ICT. Vervolgens bespreken we de resultaten van de geanalyseerde opsporingsonderzoeken. In paragraaf 3.3 richten we ons op ontmoeten en communiceren, een belangrijk logistiek onderdeel van het criminele bedrijfsproces: hoe vindt dit plaats en welke rol spelen ICT en ontwikkelingen op ICT-gebied daarbij? Daarna bespreken we in paragraaf 3.4 verschillende logistieke bottlenecks in relatie tot ontwikkelingen op ICT-gebied. Het hoofdstuk wordt afgesloten met een recapitulatie (paragraaf 3.5).

3.1 Georganiseerde criminaliteit offline: een overzicht

Criminele logistiek is een brede term voor allerlei problemen die moeten worden opgelost om de succesvolle uitvoering van bepaalde criminele activiteiten mogelijk te maken (zie o.a. Sieber & Bögel, 1993). Voor iedere soort criminele activiteit liggen deze problemen weer anders en deze zijn afhankelijk van de benodigde capaciteiten en de risico's die zijn verbonden aan bepaalde activiteiten. In vorige rapportages is reeds nader ingegaan op de invloed die deze verschillen tussen criminele activiteiten kunnen hebben op de aard van de criminele samenwerking (Kleemans et al., 1998,p. 34-41) en op de betrokkenheid van de legale omgeving (Kleemans et al., 1998, p. 61-91; Kruisbergen et al., 2012, p. 81-152). Hierbij werd benadrukt dat het succesvol uitvoeren van criminele activiteiten sterk afhankelijk is van de bewuste of onbewuste medewerking van de sociale omgeving. Daders moeten elkaar kunnen ontmoeten en heimelijk afspraken kunnen maken of communiceren. Zij hebben infrastructuur nodig voor de productie of het vervoer van drugs en ook rond betalingen, opbrengsten en besteden bestaan er allerlei logistieke bottlenecks die dienen te worden opgelost. In de vierde rapportage worden verschillende aspecten van de afhankelijkheid van de omgeving systematisch op een rij gezet, zoals de keuze tussen het zelf doen of uitbesteden van bepaalde processen en diensten en de manier waarop derden kunnen worden ingeschakeld en wat de relatie is tussen de crimineel en de dienstverlener (Kruisbergen et al., 2012, p. 81-105). Ook kunnen er verschillende soorten contactpunten worden onderscheiden tussen illegaliteit en de reguliere omgeving. Ten eerste op het niveau van personen: bijvoorbeeld financiële specialisten, notarissen en advocaten, luchthavenpersoneel of corrupte ambtenaren. Ten tweede op het niveau van ondernemingen (eigen ondernemingen of externe ondernemingen). Ten derde kan het ook gaan om grotere gemeenschappen, zoals subculturele gemeenschappen (bijvoorbeeld gemeenschappen van (ex-)woonwagenkampbewoners of Outlaw Motorcycle Gangs), etnische gemeenschappen of (delen van) bedrijfstakken. Ten vierde kunnen ook overheidsvoorzieningen ongewild

criminaliteit faciliteren. Voorbeelden daarvan zijn het misbruik van de asielprocedure door mensensmokkelorganisaties en het misbruik van afgeschermde jurisdicties voor witwasdoeleinden (Kruisbergen et al., 2012, p. 107-152).
Een belangrijke constatering over de aard van de georganiseerde criminaliteit in Nederland is dat deze veel sterker wordt gekenmerkt door 'transitcriminaliteit' dan 'racketeering' en afpersing, de traditionele activiteiten van maffiagroepen in landen als Italië en de VS. Het grote belang van logistiek bij transitcriminaliteit zal hieronder nader worden toegelicht.
Een belangrijk deel van de georganiseerde criminaliteit in Nederland bestaat uit transitcriminaliteit: winstgevende, internationale illegale activiteiten, zoals drugshandel, mensensmokkel, mensenhandel, wapenhandel, witwassen en fraude met accijnzen en heffingen, waarbij Nederland kan fungeren als productieland, doorvoerland of bestemmingsland. Winst wordt daarbij behaald door middel van het (illegaal) overschrijden van grenzen en transport neemt een belangrijke plaats in bij het uitvoeren van de criminele activiteiten (Kleemans et al., 2002, p. 139-157). Daders maken bij transitcriminaliteit gebruik van reguliere stromen in de economie en infrastructurele voorzieningen. Zij liften eerder mee op bestaande goederen-, geld- en passagiersstromen dan dat zij zelf onderdelen van de infrastructuur onder controle houden. De positie van Nederland als doorvoerland – met onder meer de Rotterdamse haven, de luchthaven Schiphol en allerlei import- en exportfaciliteiten – biedt ook goede mogelijkheden voor verschillende vormen van transitcriminaliteit. Bedrijven worden daarbij gebruikt om misdrijven te plegen of te verheimelijken.
Omdat er sprake is van transnationale illegale handel en er grote financiële belangen op het spel staan, moeten criminele samenwerkingsverbanden allerlei oplossingen zien te vinden voor logistieke problemen. Hoe vind je bijvoorbeeld betrouwbare leveranciers van cocaïne in Zuid-Amerika? Hoe komen deze drugs ongezien aan boord van een schip of van een vliegtuig? Wie houdt er toezicht op deze kostbare goederen tijdens de reis? Wanneer en waar komen de drugs aan per boot of vliegtuig en hoe krijg je die illegale goederen dan weer van boord? Al deze logistieke aspecten leveren risico's en coördinatieproblemen op.
Een extra probleem dat hierbij speelt is dat de vereiste geheimhouding voor daders extra problemen lijkt te creëren, omdat het riskant is om een boekhouding bij te houden, afspraken schriftelijk vast te leggen of om openlijk met elkaar te communiceren over de uitvoering van illegale activiteiten (Kleemans et al., 1998, p. 93-122). De eerste rapportage op basis van de Monitor Georganiseerde Criminaliteit behandelt enerzijds alledaagse problemen die optreden wanneer daders zelf het transport van illegale goederen ter hand nemen: aangeschafte afhaalboten die bij nader inzien ongeschikt zijn voor hun taak, schepen die door technische mankementen in moeilijkheden raken, meereizende 'controleurs' die plotseling vanwege familieomstandigheden naar huis moeten, problemen met het afzinken van illegale lading op de zeebodem (en het weer terugvinden daarvan) en het ontstaan van onrust of paniek vanwege vermeende politieaandacht. Anderzijds wordt er ook aandacht besteed aan problemen met het 'meeliften' van drugsladingen met reguliere transporten, met of zonder medeweten van de eigenaar van deze legale ladingen of van het transportmiddel. Dit 'meeliften' verkleint weliswaar het risico op ontdekking (en de consequenties daarvan), maar levert hele specifieke coördinatie- en timingproblemen op, zoals een oude casus uit de eerste monitorronde treffend illustreert.

Bij de ontvangst van de partijen cocaïne is er regelmatig sprake van misverstanden door fouten in de communicatie, door spraakverwarring of doordat er bijvoorbeeld een andere koerier wordt gestuurd dan is afgesproken. Ook externe omstandigheden spelen hierbij een rol. Schepen lopen later de haven binnen dan verwacht of zijn alweer vertrokken op het moment dat de afhalers ergens in een

Europese haven zijn gearriveerd. Niet altijd is precies duidelijk waar de cocaïne is verborgen. Niet altijd lukt het om de smokkelwaar van boord te krijgen. En in sommige gevallen durven afhalers het haventerrein niet op, omdat zij te veel controle-activiteiten menen waar te nemen. (Casus 11)

Deze casus geeft goed het belang aan van 'grip' op de vervoersstroom waarop wordt meegelift en op de logistieke knooppunten die worden gepasseerd.
Bij transcriminaliteit is dit 'grip houden' een belangrijke bottleneck, die op drie verschillende manieren kan worden opgelost. Ten eerste, door zelf het gehele vervoer te verzorgen (dit is echter risicovol, omdat de betrokkenheid van daders gemakkelijker kan worden getraceerd). Ten tweede, door mee te liften op een bestaande vervoersstroom, maar de eindlocatie van het vervoer (een ontvangend bedrijf) zelf onder de controle te hebben (dit is echter ook risicovol). Ten derde, door 'mee te liften' op een bepaalde vervoersstroom (bijvoorbeeld containers of luchtvracht) en de illegale goederen voor aankomst bij de eigenaar weer te onderscheppen.
Dit laatste betekent echter vaak dat controle nodig is op logistieke knooppunten, zoals havens en luchthavens, door zelf deze logistieke knooppunten binnen te kunnen komen of door gebruik te maken van personeel dat daar werkzaam is. Op het belang van bepaalde beroepen bij deze vormen van transitcriminaliteit is al in eerdere rapportages op basis van de Monitor Georganiseerde Criminaliteit ingegaan (Van de Bunt & Kleemans, 2007, p. 77-88; Kruisbergen et al., 2012, p. 83-85, 107-152).
Uit een recente analyse van zestien opsporingsonderzoeken uit de Monitor Georganiseerde Criminaliteit gerelateerd aan de luchthaven Schiphol en enkele Europese havens blijkt dat criminele groepen drie verschillende strategieën gebruiken om controles op deze knooppunten veilig door te komen (of te omzeilen) (Madarie en Kruisbergen, 2018). De eerste strategie is om gebruik te maken van de onvolkomenheden van deze controles. Doordat economische belangen en snelheid het onmogelijk maken om alle bagage en alle passagiers voor 100 % te controleren en ook controles beperkingen kennen, kunnen daders gebruikmaken van deze onvolkomenheden. Dit kan bijvoorbeeld door drugskoeriers in te zetten, die de drugs op of in het lichaam of in hun bagage vervoeren, of door drugs zodanig te verbergen dat deze drugs niet zichtbaar zijn op de beelden van scanners. Een tweede strategie is om deze controles geheel te omzeilen door gebruik te maken van personeel, dat er bijvoorbeeld voor zorgt dat tassen met drugs buiten de controles om het land in komen). Een derde strategie is om ontdekkingen bij controles weer ongedaan te maken door het gebruik van corrupt overheidspersoneel.

3.2 Inzichten uit de literatuur op het terrein van 'cybercrime'

Het ligt voor de hand dat traditionele georganiseerde criminaliteit zich meer en meer naar de online wereld beweegt (zie bijvoorbeeld Grabosky, 2007; Europol iOCTA 2016). Toch is er tot op heden op dit gebied nog maar vrij beperkt empirisch onderzoek verricht.
Recent empirisch onderzoek laat zien dat traditionele criminele netwerken die zich met zowel transitcriminaliteit als een meer parasitaire vorm van criminaliteit bezighouden, gebruikmaken van ICT om hun criminele activiteiten beter uit te kunnen voeren (bijvoorbeeld Odinot et al. 2017;[22] Bulanova-Hristova et al. 2016; Leukfeldt 2016; Leukfeldt et al., 2017c; Lavorgna, 2013, 2015a).

[22] Vijf zaken op het terrein van cybercrime/ICT-gerelateerde georganiseerde criminaliteit die in deze vijfde ronde van de monitor zijn opgenomen, maakten ook onderdeel uit van de studie van Odinot et al. (2017).

Traditionele criminele netwerken die zich bezighouden met transitcriminaliteit maken vooral gebruik van ICT om hun delicten beter te kunnen plegen. Netwerken die zich bezighouden met bijvoorbeeld drugshandel en de handel in vervalste goederen, gebruiken Internet om te communiceren, afluisteren te voorkomen, et cetera. In enkele gevallen maken leden van dergelijke netwerken ook gebruik van online ontmoetingsplaatsen om andere criminelen te ontmoeten (Odinot et al. 2017; Bulanova-Hristova et al. 2016; Lavorgna, 2014a, 2014b, 2015a, 2015b).
Traditionele criminele netwerken die zich bezighouden met een meer parasitaire vorm van criminaliteit zoals diefstal, faillissementsfraude of bedrijfsinbraken, maken ook gebruik van ICT om hun delicten beter te kunnen plegen. Daarnaast blijken dergelijke netwerken soms naast hun offline delicten ook cybercrimes te zijn gaan plegen (Odinot et al. 2017; Bulanova-Hristova et al. 2016; Leukfeldt, 2016; Leukfeldt et al., 2017b, 2017c, 2017d, 2017e), bijvoorbeeld phishing, banking malware of ransomware. Dergelijke groepen breiden hun criminele repertoire dus uit met cybercrimes. Het doel van dit soort netwerken is simpelweg snel geld verdienen. De wijze waarop lijkt de leden niet veel uit te maken. ICT biedt nieuwe mogelijkheden voor parasitaire vormen van misdaad, omdat relatief eenvoudig meerdere slachtoffers bereikt kunnen worden. Door de toegenomen verbondenheid van slachtoffers met ICT en Internet, neemt ook de bereikbaarheid van deze slachtoffers toe.
Ten slotte zijn er netwerken die zich alleen bezighouden met een parasitaire vorm van cybercriminaliteit. Deze netwerken voeren dus geen offline delicten uit maar alleen online delicten, bijvoorbeeld phishing (zie bijvoorbeeld Bulanova-Hristova et al. 2016; Leukfeldt et al., 2016, 2017b, 2017c, 2017d, 2017e).

Georganiseerde criminaliteit en toegang tot ICT-expertise
Zoals in hoofdstuk 2 is gebleken, is het een misverstand om te denken dat cybercrime een hoge mate van ICT-expertise bij alle daders vereist. Er is slechts een persoon met ICT-kennis (en/of contacten op forums) nodig om cyberaanvallen uit te kunnen voeren. Veel basale expertise is gemakkelijk verkrijgbaar, ook via forums. Meer geavanceerde expertise moet op een andere manier worden gevonden.
Het sociale kapitaal van mensen in de directe sociale omgeving van criminelen die actief zijn binnen traditionele criminele netwerken zorgt ervoor dat de benodigde ICT-expertise het netwerk binnenkomt. Dat kan doordat dergelijke expertise beschikbaar is bij een lid zelf of iemand binnen diens sociale omgeving, of doordat kennis en kunde online wordt aangekocht. Net als bij traditionele georganiseerde criminaliteit lijkt ook bij georganiseerde cybernetwerken het offline en online sociale netwerk in relatie te staan tot de criminele mogelijkheden.
Ten slotte speelt ook nog het punt dat in hoofdstuk 2 werd gememoreerd. ICT is in zekere zin neutraal en vaak leidt pas de concrete toepassing ervan tot illegale activiteiten. Dat biedt voor daders dus veel meer kansen voor samenwerking met de legale wereld, vooral in de 'grijze zone' tussen legale en illegale toepassingen van ICT. Uit onderzoek van Bijlenga en Kleemans (2017) blijkt dat criminelen soms gemakkelijk ICT-expertise weten te vinden in deze 'grijze zone', omdat bepaalde tools soms geheel legaal worden aangeboden, via internet of via Spyshops (waarbij ook nog extra dienstverlening aan criminele klanten plaatsvindt). Ook bij het aanpassen van tools (voor criminele doeleinden) hoeft voor experts op voorhand niet duidelijk te zijn waarvoor de tools uiteindelijk zullen worden gebruikt. Hierdoor kan gemakkelijk vrij zakelijke samenwerking tot stand komen (op basis van vraag en aanbod), via werkrelaties of via online of offline ontmoetingsplaatsen. Ook kunnen criminelen vrij snel 'to the point' komen, omdat het criminele karakter bij het begin van de samenwerking voor de betrokkene niet duidelijk zichtbaar hoeft te zijn of achteraf kan worden ontkend (Bijlenga & Kleemans, 2017). De neutraliteit van ICT maakt samenwerking in dat opzicht gemakkelijker.

Niet alle traditionele criminele netwerken maken de overstap naar het plegen van cybercrime. Enerzijds zijn bepaalde criminele activiteiten op zichzelf al heel erg lucratief, zoals grootschalige import, export of productie van drugs. Anderzijds laten Lavorgna en Sergi (2014) bijvoorbeeld zien dat Italiaanse maffianetwerken in veel gevallen de overstap naar de virtuele wereld nog helemaal niet hebben gemaakt. De auteurs concluderen dat internet nog geen deel uitmaakt van de sociale gelegenheidsstructuren waar deze netwerken gebruik van maken.

Online forums en darknet markets

Een zeer belangrijke ontwikkeling als gevolg van ICT is het ontstaan van online markten voor illegale goederen en diensten. De voortschrijdende digitalisering van het dagelijks leven brengt voor daders nieuwe technologische mogelijkheden om het hoofd te bieden aan de problemen en risico's waar zij in de uitvoering van hun criminele activiteiten mee worden geconfronteerd. Internet kan in de vorm van zogenoemde *crypto-* of *darknet markets* (Martin, 2014), waarvan Silk Road een van de meest bekende voorbeelden was, de handel in onder meer verdovende middelen faciliteren. Digitale encryptie stelt gebruikers in staat anoniem in te loggen op bepaalde sites en hun (illegale) goederen of diensten te verhandelen, met als voornaamste voordeel dat kopers, verkopers en facilitators nooit hun ware identiteit hoeven prijs te geven. Sterker nog, ze hoeven elkaar nooit in persoon te ontmoeten of zelfs op dezelfde fysieke locatie samen te komen (in beginsel althans). Dergelijke sites worden om die reden vergeleken met legitieme marktplaatsen op internet, zoals eBay, Amazon en Marktplaats (Martin, 2014, p. 353).

Leukfeldt et al. (2017) geven een overzicht van de verschillende typen online markten, in het bijzonder voor drugs, wapens, kinderporno en fraude (creditcards, gehackte accounts, credentials etc.). Ook de functies die dergelijke digitale 'offender convergence settings' hebben worden daarbij besproken: de marktfunctie, de sociale functie en de leerfunctie. Volgens dit artikel blijkt de leerfunctie van forums zeer belangrijk te zijn en is deze voor veel gebruikers goed toegankelijk.

Een verschil met gewone ontmoetingsplaatsen is dat de beperkingen van ruimte en tijd voor een groot deel worden opgeheven. Bilaterale relaties en gesprekken kunnen meteen worden gestart, maar ook bekenden kunnen hier elkaar gemakkelijk 'anoniem' ontmoeten (zonder dat omstanders dit zien). Deze ontmoetingsplaatsen hebben dus veel meer het karakter van een 'vrije markt', maar door de anonimiteit is het opbouwen van vertrouwen met onbekenden lastiger. Voor kleine, zakelijke transacties (zoals kleinere hoeveelheden drugs), hoeft dit geen probleem te zijn. Dit geldt te meer bij het gebruik van 'escrow services', waarbij de beheerder van de website (of een derde partij die samenwerkt met de beheerder) als tussenpersoon functioneert bij betalingen en de verkoper uiteindelijk pas wordt betaald, als de geleverde goederen zijn aangekomen bij de koper. Op deze manier wordt voor zowel koper als verkoper een belangrijk logistiek probleem opgelost: koper en verkoper hoeven elkaar namelijk niet meer fysiek te ontmoeten en tegelijkertijd drugs en geld aan elkaar te overhandigen (met alle risico's op ontdekking, maar ook op opportunistisch gedrag, bedrog, geweld en conflicten).

Sommige forums proberen de toegang (of toegang tot bepaalde onderdelen) selectief te maken door eisen te stellen aan de status van 'aanvragers', relaties die zij hebben met reeds aanwezige leden of de technische capaciteiten van deelnemers (heeft de deelnemer toegevoegde waarde voor de bestaande leden?). Uit een analyse van Dupont et al. (2017) van een exclusief forum blijkt echter dat uiteindelijk zeer veel aanvragers toegang krijgen tot dit 'exclusieve' forum zonder te beschikken over de benodigde technische toegevoegde waarde voor het forum. Een mogelijke verklaring hiervoor is dat de commerciële druk om zo veel mogelijk leden (dat wil zeggen: potentiële klanten en mededaders) toe te laten groter is dan de wens om

'exclusief' en 'veilig' te blijven. Bij verkoop van gestolen data, creditcardgegevens en malware speelt dit probleem nog sterker, omdat deze goederen en diensten gemakkelijk doorverkocht kunnen worden of zelfs 'gelekt', waardoor zij hun commerciële waarde plotsklaps kunnen verliezen.
Hoewel er verschillende soorten darknet markets bestaan, is vooral de ontwikkeling van online drugsmarkten erg belangrijk, qua omvang en qua commerciële waarde. Het anoniem handelen in drugs lost problemen op voor bepaalde consumenten, zoals consumenten in perifere gebieden (ver van offline drugsmarkten) en consumenten die de drempel richting de illegale markt te hoog vinden (in verband met kwaliteit of risico). Verschillende risico's worden voor klanten in beginsel verminderd door onder andere productbeschrijvingen, reviews van andere klanten, 'escrow services' en leveringen via pakketpost. Voor aanbieders van drugs bieden deze darknet markets toegang tot nieuwe klanten.
Als men deze literatuur in ogenschouw neemt, is een belangrijke vraag in hoeverre het vertrouwensprobleem daadwerkelijk wordt opgelost: hoe weet je dat een site te vertrouwen is en niet door de politie wordt beheerd (zoals de Hansa Market die in 2017 door de Nederlandse politie werd overgenomen) of op een gegeven moment door de beheerders zelf uit de lucht wordt gehaald (met medeneming van kredieten en data)? Hoe kunnen klanten en aanbieders elkaar vertrouwen? En hoe worden goederen en diensten afgeleverd en betaald? Nieuwe technische mogelijkheden bieden oplossingen voor bepaalde problemen, maar sommige problemen blijven ook gewoon bestaan of krijgen een andere vorm. Zo zal uit dit hoofdstuk blijken dat fysieke en sociale aspecten van criminele samenwerking en criminele activiteiten ook in de digitale omgeving een rol blijven spelen.
In recente rapporten van het EMCDDA (EMCDDA, 2016; EMCDDA & Europol, 2017) worden deze verschillende ontwikkelingen uitgebreid in kaart gebracht. De situatie in Nederland wordt meer specifiek belicht in een rapport van RAND (Kruithof et al., 2016). Het rapport signaleert dat zowel binnenlandse als buitenlandse opsporingsinstanties rapporteren dat de handel in verdovende middelen plaatsvindt via internet. Nederland blijkt hierbij een voorname rol te spelen als bronland van verdovende middelen die door gebruikers overal ter wereld via internet worden besteld (Kruithof et al., 2016). In het meest recente rapport van EMCDDA en Europol (2017) wordt het aandeel Europese aanbieders geschat op 46% (in termen van inkomsten) en worden Duitsland, Nederland en het Verenigd Koninkrijk binnen dit Europese aanbod als de belangrijkste landen benoemd. Daarnaast wordt geconstateerd dat het aandeel (ten opzichte van de totale drugsmarkt) bescheiden is en dat de transacties vooral kleinere hoeveelheden betreffen. Ten slotte wordt geconcludeerd dat over de rol van traditionele georganiseerde misdaadgroepen ten aanzien van deze online markten nagenoeg niets bekend is en dat dit een belangrijke leemte in de huidige kennis is.

3.3 Analyse van bestudeerde zaken: ontmoeten en communiceren

Een belangrijk onderdeel van de logistiek en van criminele samenwerking betreft het ontmoeten en communiceren. Daders zijn zich bewust van het feit dat openlijk communiceren over criminele zaken risico's met zich meebrengt en dat het handig gebruikmaken van ICT deze risico's deels kan beperken. Andere mogelijkheden om deze risico's te beperken zijn persoonlijke ontmoetingen en communicatie op plekken die niet of moeilijk afgeluisterd kunnen worden. Dit 'kat- en muisspel' tussen daders en opsporingsinstanties is in vorige rapportages van de Monitor Georganiseerde Criminaliteit ook aan de orde gesteld (zie o.a. Kleemans et al., 1998, p. 93-122; Kruisbergen et al., 2012, p. 81-152).

Het logistieke probleem van ontmoeten en communiceren (en kwetsbaarheid voor de opsporing) geldt voor alle typen zaken: traditionele georganiseerde criminaliteit, traditionele georganiseerde criminaliteit met een cybercomponent en ook voor de georganiseerde cybercriminaliteit (low-tech en high-tech). De onderlinge samenwerking en communicatie bij georganiseerde cybercriminaliteit is in hoofdstuk 2 al aan de orde is gekomen. Daarom richten wij ons in deze paragraaf vooral op de traditionele georganiseerde criminaliteit met en zonder cybercomponent. Bij de analyse van deze zaken blijkt dat bij traditionele georganiseerde criminaliteit fysieke ontmoetingen en afgeschermde communicatie een belangrijke rol spelen. Hieronder bespreken we daarom de rol van openbare gelegenheden, woningen, legale ondernemingen en marktplaatsen. Daarnaast bespreken we een belangrijke ontwikkeling ten gevolge van ICT: de nieuwe mogelijkheden tot versleutelde communicatie (paragraaf 3.3.1).

Traditionele georganiseerde criminaliteit (met cybercomponent): ontmoeten en communiceren

De geanalyseerde zaken geven veel voorbeelden van fysieke locaties waar daders in tijd en plaats samenkomen. Openbare plekken worden daarbij nog steeds gebruikt, onder meer omdat op die locaties de kans op afluisteren minder groot is, in elk geval in de perceptie van daders. Al in de eerste rapportage werd beschreven dat leden van criminele samenwerkingsverbanden gelegenheden zoeken om elkaar te spreken (Kleemans et al., 1998, p. 81). Dit zijn over het algemeen plaatsen waar mensen elkaar in het dagelijks leven ook treffen: horecagelegenheden zoals cafés, koffiehuizen en (weg)restaurants, golfbanen, maar ook plekken die een zekere anonimiteit met zich meebrengen, zoals carpoolplaatsen of parkeergarages.
Nog steeds maken leden van criminele samenwerkingsverbanden gebruik van vergelijkbare ontmoetingsplaatsen, zoals bekende fastfoodketens langs de snelweg (casus 151), cafés (casus 151, 164 en 171), een winkel (casus 161), verschillende horecagelegenheden (casus 161 en 171), internationale luchthavens (casus 167), maar ook diverse andere openbare gelegenheden. Sommige verdachten lijken daarbij steeds een andere locatie of gelegenheid te kiezen voor ontmoetingen. Anderen leggen een bijzondere routine aan de dag.

> *Uit observatie, afgeluisterde face-to-face- en telefoongesprekken en bankgegevens bleek dat A op vaste dagen naar dezelfde horecagelegenheden ging en daar ontmoetingen had met andere personen. Deze ontmoetingen hadden veelal te maken met zijn criminele activiteiten. Zo volgde A vaak het onderstaande patroon:*
> *A ontmoette F vaak op zondag in café W.*
> *In een hotel vonden ontmoetingen plaats met X. De bezoeken aan het hotel hielden op, nadat X werd aangehouden in verband met het aantreffen van 300 kg cocaïne in een haven.*
> *Uit een afgeluisterd gesprek blijkt tevens dat C op een vaste dag ontmoetingen had met een persoon. Hij sprak kennelijk iedere dinsdag af in een café.*
> *In een winkelcentrum ontmoette A onder meer D.*
> *In café Z ontmoette A onder meer een persoon met antecedenten op het gebied van de Opiumwet. Maar ook D en R.* (Casus 171)

Naast deze wekelijkse ontmoetingen, kwamen de diverse verdachten samen op een woonwagenkamp waar een van de hoofdverdachten woonachtig was. Tijdens een afgeluisterd gesprek tussen de verdachten valt te horen dat een van de hoofdverdachten zegt dat 'je nooit moet paniekeren als het fout gaat, niet gaan bellen of faxen of zo'. In geval van problemen werd er door dit criminele samenwerkings-

verband teruggegrepen op de routinematige ontmoetingen op vaste tijden en plekken.
Ondanks het feit dat de kans op meeluisteren door de politie op openbare plekken in de perceptie van daders minder groot is, brengt de regelmaat van de ontmoetingen risico's met zich mee. Observatieteams zijn, na enige tijd, immers in staat om de routine goed in kaart te brengen, zoals blijkt uit een van de andere zaken.

> *Men had ontmoetingen op openbare plaatsen, zoals McDonalds. Ook kwamen zeven verdachten samen op een parkeerplaats. Hierbij werd geobserveerd en werden foto's gemaakt, waarna de personen die bij de ontmoeting aanwezig waren later werden geïdentificeerd als A, C, D, E, F en G. Uit verder gerelateerde bevindingen blijkt dat deze ontmoeting in het teken stond van het voorbereiden van een verdovende middelen transport.* (Casus 151)

Een oplossing is om steeds van openbare locatie te veranderen, om zo het in kaart brengen van de modus operandi van ontmoetingen voor de opsporingsdiensten te bemoeilijken. Het constant wisselen van ontmoetingsplaats vergt echter de nodige discipline en levert ook praktische uitdagingen op. Hoe weten mededaders, klanten of afnemers immers waar de ontmoeting zal plaatsvinden? Er zal op de een of andere manier over de concrete locatie gecommuniceerd moeten worden. Omdat sommige verdachten zich bewust lijken te zijn van het feit dat hun telefoon wordt afgetapt, resulteert dit in vage beschrijvingen zoals in casus 159.

> *Verdachten gaven bij een afspraak voor een ontmoeting vaak geen exacte plaats of adres door. Zo wordt gezegd in een afgetapt gesprek: '... ik heb over een kwartier een afspraak bij dinges eeh .... kom maar naar de dinges, ergens bij het ziekenhuis of kom naar een plek ergens in [plaats]'. En even later: 'Ik kom naar de omgeving van je huis. Ik kom naar de bushalte.'* (Casus 159)

Naast openbare gelegenheden en de woonomgeving kunnen ook (eigen) bedrijven fungeren als ontmoetingsplaats. In de vorige rapportage werd ten aanzien van ondergronds bankieren al gewezen op de manier waarop kleine detailhandelsbedrijven fungeerden als 'loket' (Kruisbergen et al., 2012, p. 195-203). In een van de geanalyseerde zaken komt iets soortgelijks naar voren, waarbij de hoofdverdachte verschillende keren afspreekt met contacten in (of in de directe omgeving van) een perceel waar verschillende ondernemingen zijn gevestigd. Deze bedrijven lijken daarbij te worden gebruikt als zogenoemd 'clearinghouse': locaties waar verschillende geldbedragen kunnen worden ingebracht, geregistreerd, bewaard en vervolgens door een andere klant weer opgehaald. In dergelijke gevallen fungeren kleine bedrijven als een 'marktplaats' waar naast klanten ook geldstromen samenkomen. Het voordeel van dergelijke constructies is dat het legale voorkomen van de winkel de aanloop van verschillende mensen niet vreemd of opvallend maakt; anders dan bijvoorbeeld bij een woonhuis of appartement.
Een horecagelegenheid is ook bij uitstek geschikt om dienst te doen als een ontmoetingsplaats, zoals naar voren komt in casus 164.

> *Centraal punt is horecagelegenheid D in [plaats]. Hier vinden veel ontmoetingen plaats met groepsleden. Door hoofdverdachte B wordt daarbij aangegeven dat hij liever geen ontmoetingen heeft buiten de horecagelegenheid en dat, wanneer hij een ontmoeting heeft in de horecagelegenheid, hij altijd kan zeggen dat die personen klanten van de horecagelegenheid zijn en daar niet speciaal zijn gekomen voor een afspraak of ontmoeting met hem. Toch is te merken dat men heel vrij spreekt in de horecagelegenheid.* (Casus 164)

In het dossier staat beschreven dat diverse personen uit binnen- en buitenland die verdacht worden van betrokkenheid bij de (inter)nationale handel in verdovende middelen werden gesignaleerd als bezoeker van de horecagelegenheid. In tegenstelling tot het doorgaans publieke karakter van horecagelegenheden, moesten bezoekers van dit specifieke bedrijf aanbellen om toegang te krijgen. In een andere zaak komt een vergelijkbare verhullende functie van een legale onderneming naar voren.

> *Er werd sinds 2009 gebruikgemaakt van de loods waar bedrijf M gevestigd was op naam van de ex-vrouw van de hoofdverdachte C. Voor de buitenwereld werd dit bedrijf gepresenteerd als legaal bedrijf en zou dit bedrijf horecaspullen en geluidsapparatuur verhuren. Gedurende het onderzoek is van legale activiteiten van het bedrijf niets gebleken. De huur van de loods werd door verdachte D elke maand contant afgedragen aan verdachte C. Deze stortte het ontvangen geld op de bank en maakte de huur over naar de verhuurder. De loods werd gebruikt om kopers en verkopers van precursoren, verdovende middelen, grondstoffen, hardware et cetera te ontvangen. Daarbij werd als dekmantel het bedrijf M gebruikt. Van enige omzet in haar branche is van bedrijf M gedurende het onderzoek niets gebleken.* (Casus 175)

In en rondom de loods van deze op papier legale onderneming konden meer dan 700 personen worden geïdentificeerd, waarvan 200 bezoekers die bij de politie bekend stonden vanwege hun betrokkenheid bij de handel in of productie van verdovende middelen. Het ging hierbij om zowel afnemers, leverancier als tussenpersonen. In de loods, maar ook in het eerder beschreven café, ontstaat een marktplaats.
Grote steden – of specifieke stadsdelen of wijken – kunnen, zoals Huisman et al. (2003) beschreven, eveneens uitgroeien tot een soort marktplaats. Ruggiero (2000) gebruikt hiervoor de metafoor van een stedelijke bazaar. In de geanalyseerde zaken kent de lokale inbedding van de criminele activiteiten een verankering in de wettige wereld omdat deze fysiek samenkomt in een legaal bedrijf. Daders kunnen profiteren van een dergelijk gebruik van legale ondernemingen: het biedt hen afscherming, in het bijzonder omdat ze profiteren van de legale uitstraling van het bedrijf, maar beperkt ook de noodzaak tot communicatie over locaties om elkaar te ontmoeten, zoals een opgenomen gesprek tussen twee van de hoofdverdachten illustreert.

> *A: Als je de mensen maar kan ontvangen, en een beetje kan opslaan.*
> *B: Ja, ja, dat is het hè. Dat is het belangrijkste.*
> *A: Als het dan een beetje loopt, kun je alsnog naar een grotere hal.*
> *B: Ja, maar je moet wel zorgen dat je plek hebt waar mensen naartoe kunnen komen, ja.*
> *A: Anders kun je het vergeten. Anders zou ik het toch rond [plaats] pakken.*
> *B: Want anders, dat is gewoon hoe ik het deed…. Ik zat altijd bij iedereen hè. Ik rij altijd gewoon rond.*
> *A: Je moet een punt hebben, waar ze toch naartoe kunnen komen en waar je van uit kunt werken.*
> *B: Uhu.*
> *A: Dat zie ik hier, dat is gewoon perfect.*
> *B: Ja.*
> (Een van de geanalyseerde casussen)

Dat deze conversatie deel uitmaakt van het opsporingsdossier, geeft aan dat deze modus operandi niet zonder risico is. In beide geanalyseerde zaken waarin een

'marktplaats' wordt beschreven, wisten de opsporingsdiensten namelijk succesvol afluisterapparatuur te plaatsen en bleken de afgeluisterde gesprekken in deze twee zaken een goudmijn, zoals het volgende voorbeeld illustreert.

A: Hij zei dat er twintig samples.
B: Weet ik (NTV).
C: (NTV) zei (NTV) twintig .. samples zei ons chauffeur.
D: Je ken de chauffeur bellen (NTV).
B: Die negenhonderd duizend. Wat moest ik betalen voor de negenhonderd duizend.
A: Ehh vierenvijftig cent.
B: Vierenvijftig cent omdat wat moest ik ook al weer weten.
A: Waar hebben we het nu over.
B: Wat kosten negenhonderd duizend tabletjes maken.
D: (NTV).
(…)
A: Vierenvijftig cent.
D: Vierenvijftig cent (NTV).
B: (NTV) hoeven niks te doen.
A: Alleen aanbetalen.
B: Alleen vijftig ruggen aanbetalen dan maken we pas ehh..
(Een van de geanalyseerde casussen)

De incriminerende details van de opgenomen vertrouwelijke communicatie in de bedrijfsloods en horecagelegenheid doen vermoeden dat zowel de uitbaters als de bezoekers zich binnen veilig en vrij waanden: de verdachten noemen bedragen, hoeveelheden en beschrijven vrij expliciet en openlijk waar ze zich mee bezig-houden.
We zien dus dat bedrijven, net als andere locaties, kunnen fungeren als 'offender convergence settings' (Felson, 2003, 2006): plekken waar daders mededaders en potentiële mededaders en klanten kunnen ontmoeten. De mate waarin deze plekken als privaat, semipubliek of publiek kunnen worden gekarakteriseerd, varieert. We zien dat deze 'offender convergence settings' veelal in de semipublieke sfeer liggen en dat 'toegangscontrole' een belangrijke rol speelt. De plaatsen zijn vaak in principe publiek toegankelijk, maar niet voor iedereen. Bovendien kent de formele en informele toegangscontrole sociale aspecten: mensen worden herkend en worden wel of niet toegelaten of de aard van de activiteiten en gesprekken wordt aangepast. Daardoor is het mogelijk om publieke toegang en heimelijkheid met elkaar te combineren. Soms is er ook sprake van fysieke overgangszones, waarbij een apart gedeelte alleen voor een geselecteerd publiek toegankelijk is.

3.3.1 Versleuteling van communicatie

Verdachten maken zich over het algemeen veel zorgen over de mogelijkheid dat er iemand meeluistert; een reden waarom verdachten in sommige gevallen ofwel bijzonder cryptisch over de telefoon praten ofwel enkel in persoon overleggen. In dit opzicht kunnen zij dankbaar gebruikmaken van technologische ontwikkelingen op het gebied van digitale communicatie, in het bijzonder het gebruik van ge-encrypte telefoontoestellen, ook wel bekend als PGP's. De afkorting PGP staat voor *Pretty Good Privacy*. Deze telefoons, meestal van het merk *Blackberry*, zijn speciaal geprepareerd zodat verschillende functies en services van de telefoon zijn afgesloten, waaronder de camera, internetbrowser, spraakherkenning- en opnames. Het is bovendien met deze telefoons doorgaans niet mogelijk om een normaal telefoon-

gesprek te voeren, zoals een van de verdachten in een van de ons onderzochte zaken via SMS laat weten aan een andere verdachte: *'Its out of the phone, we never call, we only do text and we use pgp'.* Eigenlijk is het enkel mogelijk om berichten te verzenden en te ontvangen via een gesloten bedrijfsnetwerk, waarbij gebruikt wordt gemaakt van een speciaal daarvoor geïnstalleerde applicatie/server. Op deze manier wordt geprobeerd om het risico op interceptie te minimaliseren, in het bijzonder omdat deze manier van communiceren bewerkstelligt dat de opsporingsdiensten dit niet kunnen onderscheppen.
In een van de door ons geanalyseerde zaken legt de ene verdachte aan de andere verdachte het gebruik van deze manier van communiceren uit, maar ook het gevaar dat de politie uiteindelijk toch de communicatie kan achterhalen.

A: Wat is een server?
B: Server? Eh, jouw server, via welke server jij je berichten verstuurt Snap je? Als hun de server pakken, van de bb's, dan kunnen ze elke bericht achterhalen. Snap je? Maar waarom? Ze moeten bij de server wezen.
A: Ja?
B: Kijk, wij hebben nu, zeg maar eh, onze.
A: Nee, dat kunnen ze ook niet achterhalen.
B: Tuurlijk wel.
A: Dan zijn ze alsnog encript.
B: Nee joh gek, als ze de server hebben klaar.
A: Is die dan niet encript?
B: Ja maar dan kunnen ze achterhalen, want dan hebben ze de computer waar alles mee is begonnen. Je kan alles op de wereld kan je hacken zolang je maar die, die, de hoofdbron hebt waar alles op gebeurt. Snap je wat ik bedoel of niet?
A: Ja.
B: Daarom verstoppen mensen die servers. Weet je, ze gaan naar Canada, ze gaan naar Australië, je weet toch? Ze doen die dingen daar allemaal. Snap je wat ik bedoel of niet? Eentje zet hem in fucking Vietnam, of Thailand, wollah. Snap je?
A: Ja ja ja.
B: Waarom? Dan kan de scotoe, die ken niet bij de server komen, dan kunnen ze hun ook niet eh, je weet toch? Bloot leggen, snap je? En ook al hebben ze alle berichten van de server, wie is wie? Snap je wat ik bedoel of niet? Ook dat nog.
A: Ja.
(Een van de geanalyseerde casussen)

In de eerdere 150 door ons bestudeerde opsporingszaken ten behoeve van rapportages van de Monitor Georganiseerde Criminaliteit kwam het gebruik van PGP onder verdachten minder sterk naar voren. In de dertig zaken die in het kader van de huidige rapportage zijn geanalyseerd neemt deze technologie in verschillende zaken een prominente plaats in. In de woning van een verdachte in een van deze zaken werden maar liefst negentig PGP-telefoons aangetroffen. Het gebruik van deze manier van communiceren lijkt een meer recente ontwikkeling te zijn; wat ook door een aantal dienstdoende officieren van justitie werd benoemd. In een van deze zaken kon de opkomst van het gebruik van PGP expliciet worden waargenomen. Waar de verdachten in het begin van het onderzoek veelvuldig communiceerden via wisselende toestellen en telefoonnummers, gingen zij na enige tijd over op PGP om het risico op afluisteren te minimaliseren. Overigens blijft het in beslag nemen van de server wel een groot potentieel gevaar, omdat dan alle geheime gesprekken kunnen worden ontsleuteld (zoals ook o.a. is gebleken in de zaak Ennetcom).

Daders en verdachten proberen op verschillende manieren hun criminele activiteiten, maar ook de communicatie hierover, af te schermen door het opwerpen van (technische) barrières. Naast het gebruik van de mogelijkheden op het gebied van (tele)communicatie, komen in de dossiers ook manieren naar voren waarop verdachten proberen om een veilige, fysieke omgeving te creëren of te bewerkstelligen. Bij ontmoetingsplaatsen werd na doorzoekingen van de locaties diverse apparatuur aangetroffen om de (tele)communicatie te verstoren of afluisterapparatuur te detecteren. Ook zijn er daders die bijvoorbeeld een bedrijfsloods regelmatig 'scannen' op de aanwezigheid van afluisterapparatuur.

3.4 Analyse van bestudeerde zaken: logistieke bottlenecks

In deze paragraaf bespreken we verschillende logistieke bottlenecks in relatie tot ontwikkelingen op ICT-gebied. In een eerste subparagraaf staan traditionele georganiseerde criminaliteit en de doorvoer via (lucht)havens centraal. We bespreken welke bottlenecks daders tegenkomen en welke veranderingen daarin zijn opgetreden als gevolg van ICT-ontwikkelingen. Daarbij analyseren we traditionele georganiseerde criminaliteit en zaken met een cybercomponent. In een tweede subparagraaf richten we ons op een belangrijke ontwikkeling op het gebied van de traditionele drugshandel: de opkomst van online drugsmarkten. Ten slotte behandelen we in een derde subparagraaf een specifieke vorm van georganiseerde cybercriminaliteit: fraude met het betaalverkeer. Het betaalverkeer is de afgelopen jaren sterk veranderd en de cybercrimezaken ('low-tech' en 'high-tech') in deze nieuwe dataverzamelingsronde hebben allemaal betrekking op fraude met het betaalverkeer. Deze kwestie wordt hier vooral op hoofdlijnen besproken, omdat in hoofdstuk 4 uitgebreid wordt ingegaan op het geldverkeer als belangrijk aspect van de logistiek van georganiseerde criminaliteit.

Traditionele georganiseerde criminaliteit en ICT: doorvoer via (lucht-) havens

Een belangrijk deel van de georganiseerde criminaliteit in Nederland bestaat uit transitcriminaliteit: winstgevende, internationale illegale activiteiten, zoals drugshandel, mensensmokkel, mensenhandel, wapenhandel, witwassen en fraude met accijnzen en heffingen, waarbij Nederland kan fungeren als productieland, doorvoerland of bestemmingsland. Winst wordt daarbij behaald door middel van het (illegaal) overschrijden van grenzen en transport neemt een belangrijke plaats in bij het uitvoeren van de criminele activiteiten (Kleemans et al, 2002, p. 139-157).
Bij dit transport speelt het meeliften op bestaande goederen-, geld- en passagiersstromen een belangrijke rol. Dit geldt ook voor logistieke knooppunten, zoals de luchthaven Schiphol (en regionale luchthavens) en de havens van Rotterdam, Antwerpen en andere grote havens. Op deze plekken overschrijden op dagelijkse basis op grote schaal passagiers, bagage en goederen de Nederlandse grens. Dit geldt ook voor het personeel dat betrokken is bij deze grensoverschrijdingen: mensen die werkzaam zijn op Schiphol in het kader van het vervoer van personen en goederen, bagage, catering, onderhoud, schoonmaakbedrijven, et cetera. Vanwege hun werk overschrijden ook deze personeelsleden op dagelijkse basis de grens door van 'landside' naar 'airside' te gaan en andersom. Dit geldt ook voor overheidspersoneel dat met toezicht en opsporing is belast (zoals de Koninklijke Marechaussee, politie en douane) en privaat personeel dat in luchthavens en havens ook een belangrijke rol speelt. Al deze personen kunnen in principe criminele activiteiten verhinderen of juist faciliteren.

Zoals eerder besproken, blijkt uit een recente analyse van zestien opsporingsonderzoeken uit de Monitor Georganiseerde Criminaliteit gerelateerd aan de luchthaven Schiphol en enkele Europese havens dat criminele groepen drie verschillende strategieën gebruiken ten aanzien van deze controles (Madarie & Kruisbergen, 2018). De eerste strategie is om gebruik te maken van de onvolkomenheden van deze controles. Doordat economische belangen en snelheid het onmogelijk maken om alle bagage en alle passagiers voor 100 % te controleren en ook controles beperkingen kennen, kunnen daders gebruikmaken van deze onvolkomenheden. Dit kan bijvoorbeeld door drugskoeriers in te zetten, die de drugs op of in het lichaam of in hun bagage vervoeren, of door drugs zodanig te verbergen dat deze drugs niet zichtbaar zijn op de beelden van scanners. Een tweede strategie is om deze controles geheel te omzeilen door gebruik te maken van personeel op de luchthaven (of in de haven). Een derde strategie is om ontdekkingen bij controles weer ongedaan te maken door het gebruik van corrupt overheidspersoneel.
Belangrijke logistieke problemen die bij het meeliften met bestaande vervoersstromen een rol spelen zijn timing- en 'uithaal'-problemen. Wanneer komen personen en/of goederen aan en hoe kunnen deze personen en/of goederen tijdig op het logistieke knooppunt worden onderkend en door de controle worden geloodst? Het controle houden op kostbare lading en het tijdig uithalen van de lading of door de controles loodsen is dus altijd een punt van zorg. Daarom is hulp van (lucht)havenpersoneel of een andersoortige greep op de logistiek van de haven of luchthaven voor daders van groot belang. Met hulp van personeel kunnen verschillende logistieke problemen worden opgelost.
Een relevante ontwikkeling daarbij is de toegenomen automatisering van de logistiek en de toegenomen beveiliging van havens en luchthavens. Tegenwoordig is het bijvoorbeeld voor niet-personeelsleden veel minder gemakkelijk om binnen het beveiligde gebied van luchthavens te komen dan vroeger (dit geldt overigens ook voor havens). Zo ging tijdens een opsporingsonderzoek uit de eerste ronde van de Monitor Georganiseerde Criminaliteit een mensensmokkelaar vaak de beveiligde zone op Schiphol binnen om daar klanten te 'coachen', weg te brengen, op te halen of te helpen met overstappen. Ook de hulp van schoonmakers, die poortjes en deuren tussen 'airside' en 'landside' open lieten staan, faciliteerde de mensensmokkel. Deze situatie is sinds die tijd ingrijpend veranderd.
In eerdere rapportages beschreven we ook hoe contacten op luchthavens, zoals personen werkzaam in de bagagekelder of schoonmakers van vliegtuigen op Schiphol, dienstbaar waren aan de internationale handel in verdovende middelen. Omdat dergelijke facilitators een belangrijke schakel vormen in het criminele bedrijfsproces, zijn bepaalde beroepsgroepen of specifieke werkplekken onderhevig aan strenge vormen van screening en toezicht. Dat geldt in het bijzonder voor Schiphol.
Van Sluis en Bekkers (2009, p. 84-85) beschrijven dat Schiphol verschillende security-gebieden kent. Om toegang te krijgen tot deze gebieden is een zogenoemde Schipholpas vereist die personeelsleden ontvangen na een veiligheidsonderzoek. Bovendien zijn de meeste personeelsdoorgangen op Schiphol voorzien van apparatuur waarmee de biometrische gegevens op de Schipholpas kunnen worden gecontroleerd. Er is, ten slotte, een 100% controle op al het personeel.
In een van de geanalyseerde zaken lijkt een crimineel samenwerkingsverband een succesvolle manier te hebben gevonden om zich toch aan dit toezicht te onttrekken:

> *Bedrijf Y maakte vliegtuigen schoon. In de vliegtuigen kon op verschillende plaatsen cocaïne verstopt worden, zoals (o.a.) in het vrachtruim, of in het passagiersgedeelte of in de watertanks. Tot het criminele samenwerkingsverband behoorden personen die de verdovende middelen van de vliegtuigen konden halen en via*

schoonmaakbedrijf Y kon de cocaïne van 'air-' naar 'landside' worden gebracht.
(Een van de onderzochte casussen)

In deze zaak was een van de hoofdverdachten als voormalig bestuurder van het schoonmaakbedrijf het contact buiten Schiphol naar de organiserende partijen.

A wordt gebeld door K:
A: Euh ... kijk ... op de vijfde van de maand zou toch onze grote ezel naar de garage gaan?
K: Wat zeg je Abi?.
A: De grote ezel.
K: Ja?
A: Die zou op de vijfde van de maand naar de garage gaan.
K: Okay.
A: Ha .. morgen is het de vijfde van de maand.
K: Ja.
A: Ha ... als ie naar de garage gaat zeg dat hij (een derde persoon) de banken/stoelen even grondig dinges doet .... hij moet ze losmaken en schoonmaken.
K: Is goed
(Een van de onderzochte casussen)

Ook in havens hebben daders met timing- en 'uithaal'-problemen te maken. Zij kunnen deze problemen deels oplossen door medewerking van personeel dat werkzaam is op haventerreinen en/of dat toegang heeft tot deze haventerreinen. Een belangrijke ontwikkeling in dit opzicht is de sterk toegenomen automatisering van het containertransport en de toegenomen beveiliging van haventerreinen. Bij havens is een belangrijke rol weggelegd voor de diensten van zogenoemde 'uithalers': medewerkers die weten waar en wanneer een lading verdovende middelen de haven bereikt en die de (veilige) uitvoer van de partij verzorgen of faciliteren.
Zo heeft een hoofdverdachte in een van de zaken het over 'topmannen om die dingen weg te laten halen'. Het summum van een dergelijk corrupt contact op een logistiek knooppunt was echter een 'platte' medewerker van de douane. Zijn functie bestond uit het aan de hand van risicoprofielen onderzoeken of een (fysieke) controle bij specifieke zendingen of containers noodzakelijk was.

A: Ik heb nu 100% controle over alle zendingen. Tenzij de FIOD er is.
B: Ja.
A: Maar nu heb ik echt 100% controle.
B: Dat weet niemand?
A: Dat weet niemand
(Een van de geanalyseerde casussen)

De bovengenoemde douanier zorgde ervoor dat ladingen niet werden gecontroleerd. In andere gevallen nemen daders echter bewust het risico op controle en laten zij illegale goederen meeliften met ladingen die wel of niet zullen worden gecontroleerd. In dat geval is er, zoals gezegd, echter een belangrijk 'timing-' en 'uithaal-' probleem, omdat de illegale goederen op tijd uit deze lading moeten worden gehaald, voordat de lading als geheel – dat wil zeggen de reguliere lading en de smokkelwaar – de legale afnemer bereikt.
In zaken in eerdere rondes van de Monitor Georganiseerde Criminaliteit zagen we dat daders zelf haventerreinen betraden, zegels van containers verbraken en de illegale lading zelf uit deze containers haalden. Ook zagen we dat het heel belangrijk

is om te weten waar een specifieke lading op welk moment is. Zo hield de verdachte in casus 11 al via een track & trace systeem bij waar een schip met zijn illegale lading zich op welk moment bevond, zodat uithalers op tijd in de haven ter plekke zouden kunnen zijn.
Ook hier zijn sterke veranderingen opgetreden: toegang krijgen tot haventerreinen is moeilijker geworden en zowel de beveiliging als de containerafhandeling zijn sterk geautomatiseerd. Ook is het steeds moeilijker om een container in de haven zonder hulp van 'insiders' en zonder toegang tot geautomatiseerde systemen te lokaliseren en deze container ook daadwerkelijk te bereiken, omdat containers soms wel in lagen van vijf, zes of zeven containers worden opgestapeld. Ten slotte is er altijd sprake van tijdsdruk, mede omdat de container moet worden bereikt voordat de vervoerder de container komt ophalen.
Dat deze automatisering ook kwetsbaarheden oplevert, wordt treffend geïllustreerd door casus 151.

> *Op [datum] wordt vastgesteld door het IT-personeel van rederij/containerterminal D dat hun portaalsite [http//www.xxxx] werd gehackt vanuit Nederland. De portaalsite werd recentelijk vervangen door een nieuwe webomgeving, maar is nog steeds actief. Op bedoeld portaalsysteem kunnen de klanten van de terminal nagaan welke container met welk schip wordt aangevoerd en of het schip reeds is aangekomen/gelost. Het gaat uiteindelijk om een soort track & trace systeem betreffende containers behandeld door D. De klanten die hier toegang toe hebben zijn rederijen, expediteurs en diensten als de douane, (veterinaire) keuringsdiensten, et cetera. Deze klanten hebben ten behoeve van deze externe toegang een door D bepaalde gebruikersnaam en wachtwoord gekregen, teneinde in het portaalsysteem dergelijke zoekingen te doen.*(Casus 151)

De bedrijven in de haven werden aangevallen op twee manieren. Allereerst werden zogenoemde keyloggers gebruikt om de toetsaanslagen van medewerkers te kunnen registeren. Deze hardware werd fysiek geplaatst tussen toetsenborden en computers, nadat de verdachten onder valse voorwendselen het bedrijf waren binnengelopen. Daarnaast werden er e-mails met malware verstuurd aan de rederijen, waardoor medewerkers uiteindelijk zelf de systemen infecteerden. Voor de hackers was het daarna op afstand mogelijk om de benodigde gegevens binnen te halen, waarna leden van het criminele samenwerkingsverband in staat waren om te bepalen waar de containers met de verdovende middelen zich bevonden. Om deze containers vervolgens op te halen maakten ze gebruik van de daarvoor benodigde, fraudeleus verkregen 'pincodes'.
Het onderzoek richtte zich primair op de meer traditionele offline invoer van verdovende middelen, maar de modus operandi van dit criminele samenwerkingsverband laat zien dat de cybercomponent in deze zaak een belangrijke rol speelde. Door manipulatie van computersystemen wisten de daders waar een container zich bevond en waren ze in staat deze container af te halen voordat een chauffeur van het legale bedrijf waarvoor de container was bestemd dat kon doen.[23] Toch werden met deze geavanceerde manier van toegang krijgen tot containers niet de fundamentele problemen van het meeliften met ander vrachtvervoer opgelost. Het probleem met het meeliften met andermans lading is namelijk dat dergelijke containers weer moeten afgeleverd bij de uiteindelijke klant en dat een vervoerder is ingeschakeld om deze klus te klaren. In deze zaak zien we dus ook dat deze contai-

[23] Bijzonder is eveneens de betrokkenheid van een oude bekende uit een eerdere rapportage van de Monitor Georganiseerde Criminaliteit, die in deze zaak de kennis en kunde inhuurde van jonge(re) specialisten op het gebied van ICT.

ners uiteindelijk altijd door iemand worden 'gemist' en dat dat vervolgens vragen en reacties oproept. Als de container wel bij de klant wordt afgeleverd, is er een chauffeur van een vervoersbedrijf die de container mist. Als de container niet bij de klant wordt afgeleverd, zal de klant denken dat de container is vermist of is gestolen. Op deze manier kwam deze zaak overigens ook aan het rollen, omdat er onder meer containers zoek waren met een inhoud van hoge waarde. De zaak bleek echter niet te gaan om ladingdiefstal, maar om de drugs die werden verstopt in deze containers.

Traditionele georganiseerde criminaliteit met cybercomponent: online drugsmarkten

In paragraaf is 3.3 duidelijk geworden dat fysieke ontmoetingsplaatsen nog steeds belangrijk zijn voor daders, al dan niet in combinatie met het afschermen of versluieren van communicatie door het gebruik van moderne ICT-middelen. Een belangrijke achtergrond hiervan is het grote belang van bestaande sociale relaties en het opbouwen van vertrouwen bij criminele samenwerking.
Sinds het verschijnen van de laatste rapportage (Kruisbergen et al., 2012) zijn er echter nieuwe ontwikkelingen waar te nemen, zoals de opkomst van *crypto*- of *darknet markets*, meer in het bijzonder op het terrein van de handel in de verdovende middelen en andere illegale goederen en diensten.
Mede om deze reden is in een van de zaken het OM uit eigen initiatief een onderzoek gestart naar de rol van een specifieke website waarop zowel verdovende middelen als vuurwapens werden aangeboden.

> *Door een digitaal rechercheur werd onderzoek verricht naar de activiteiten van de gebruiker A op de website X. A is een van de vijf moderators van de forums op de website. Daarnaast is A actief als verkoper op de website. Hij biedt onder meer de volgende producten op de website te koop aan: cocaïne, hasj, heroïne, xtc en amfetamine. Er waren in totaal 178 feedbackreacties op verkooptransacties van A. De feedbackreacties waren afkomstig van verschillende gebruikersnamen.*
> (Casus 152)

De site in kwestie was enkel te benaderen via een zogenoemd TOR-netwerk, waarbij het oorspronkelijke IP-adres verborgen blijft. Net als in het geval van Silk Road en andere darknet markets, vielen de interacties en transacties door het gebruik van TOR en betalingen in de vorm van bitcoins moeilijk te traceren (in hoofdstuk 2 wordt deze casus meer uitgebreid besproken).

Een groot deel van de handel en communicatie in deze zaak verliep via internet, onder meer via TOR, chat, mail, Skype en VPN-verbindingen. Maar tegelijkertijd was men slordig met communiceren en maakten de (hoofd)verdachten vergelijkbare 'bedrijfsfouten' die ook tijdens de meer traditionele vormen van georganiseerde criminaliteit vallen waar te nemen. Zo werd er niet consequent gebruikgemaakt van encryptie, maar werd er in sommige gevallen openlijk en tot in detail gesproken over leveringen.
De genoemde TOR-netwerken bieden daders belangrijke faciliteiten. Een TOR-netwerk is een netwerk van computers en servers binnen het bestaande internet. TOR stelt gebruikers in staat om hun IP-adres te verbergen, omdat er verbindingen worden gelegd met andere servers binnen het bredere netwerk. Bovendien worden de gegevens protocollair versleuteld, wat het aftappen van de verbinding bemoeilijkt en in veel gevallen in het geheel onmogelijk maakt. Hierdoor is het onmogelijk, zoals in een van de door ons onderzochte zaken naar voren komt, om de fysieke locatie van een server te achterhalen. Ook het gebruik van een exotische server,

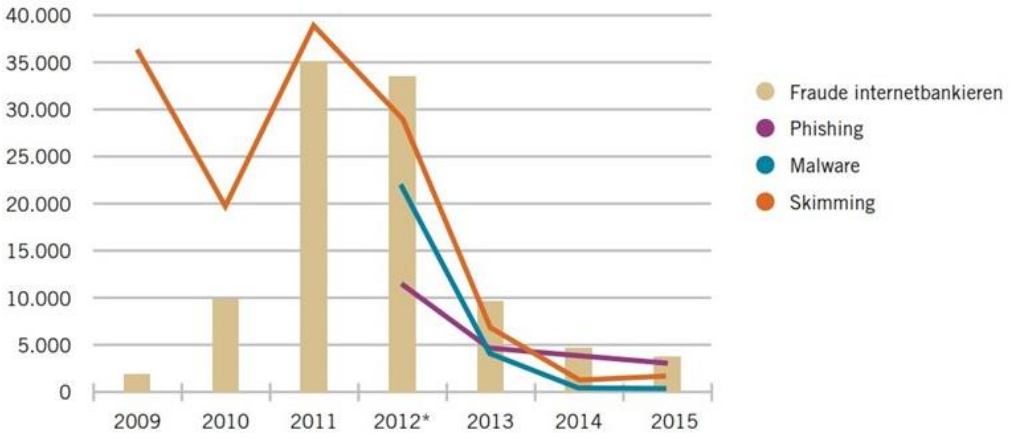
zoals een server uit Ho Chi Minh City, of het gebruikmaken van open wifi-verbindingen bewerkstelligt dat er een rookgordijn wordt opgetrokken rondom de daadwerkelijke fysieke locatie van een verdachte.
De bovenstaande beschrijving illustreert dat internet nieuwe mogelijkheden biedt om het hoofd te bieden aan risico's en problemen die inherent zijn aan het uitvoeren van criminele activiteiten. Toch vielen de (hoofd)verdachten ook terug op werkwijzen die overeenstemmen met meer traditionele vormen van georganiseerde criminaliteit. De daders in casus 152 kenden elkaar persoonlijk en woonden bij elkaar in de buurt. Bij de handel in gebruikershoeveelheden hadden koper en verkoper geen fysiek contact en werden deze leveringen geseald en per post verstuurd. Grotere partijen werden echter door de hoofdverdachten zelf verhandeld en per auto afgeleverd in Nederland, België, Frankrijk en Duitsland. In het algemeen lijkt vooral geleverd te worden aan klanten in Europese landen.
In dit geval, maar ook in (de andere) gevallen van georganiseerde vormen van cybercriminaliteit (zie ook hoofdstuk 2), wordt niet het gehele criminele bedrijfsproces gedigitaliseerd, maar faciliteren of vervangen technologische (hulp)middelen slechts een bepaald onderdeel of een specifieke (deel)taak. Naast online aspecten kennen deze criminele activiteiten nog steeds belangrijke offline aspecten, waarvoor digitalisering geen oplossing biedt.

Georganiseerde cybercriminaliteit: fraude met het betaalverkeer
Vier geanalyseerde zaken uit deze nieuwe ronde van de Monitor Georganiseerde Criminaliteit hebben betrekking op georganiseerde cybercriminaliteit ('low-tech' en 'high-tech'; zie voor meer details hoofdstuk 2). Men zou deze zaken op twee manieren kunnen karakteriseren: als cybercriminaliteit 'pur sang' of als een vergevorderde verschijningsvorm van traditionele diefstal en/of fraude. In de kern komen deze criminele activiteiten namelijk neer op het mensen afhandig maken van geld, er met de buit vandoor gaan en de buit – voordat dit ontdekt wordt – te cashen.
De nieuwe mogelijkheden om mensen geld afhandig te maken zijn gerelateerd aan de manieren waarop mensen betalingen doen. Op dit terrein is de afgelopen tijd sprake geweest van twee belangrijke ontwikkelingen. In de eerste plaats is het aantal contante betalingen aan de kassa sterk gedaald en vervangen door betalingen met een pinpas (het aantal betalingen met creditcards is redelijk stabiel (ongeveer 0,5 %) en is minder omvangrijk dan in landen als de Verenigde Staten). Zo is de omvang van contante betalingen tussen 2010 en 2016 met bijna een derde afgenomen van 4,37 miljard in 2010 tot 2,95 miljard euro in 2016 (DNB, 2017). In de tweede plaats vindt het betalingsverkeer in toenemende mate plaats via internetbankieren. Tegenwoordig verloopt ongeveer 92% van de overboekingen via internetbankieren (Nederlandse Vereniging van Banken (NVB), 2017).
Door deze ontwikkelingen zijn de mogelijkheden om mensen geld afhandig te maken veranderd. Een bekende manier om misbruik te maken van betalingen met traditionele creditcards is 'skimming': het op onrechtmatige wijze bemachtigen en kopiëren van betaalkaartgegevens (van creditcards en/of pinpassen). Vooral de magneetstrips van betaalkaarten waren gemakkelijk te kopiëren. Een veel gebruikte modus operandi was dan ook om een kopie te maken van deze betaalkaarten en daarmee betalingen te gaan doen in het buitenland. Het duurde in de regel enige tijd voordat deze fraude werd ontdekt, vooral bij creditcards, omdat de klant in de beginperiode vaak slechts eens per maand een papieren overzicht van de afgeschreven bedragen kreeg. Kwetsbaarheid van het betaalsysteem en de late ontdekking van de fraude vormden hierbij de hoekstenen van het 'verdienmodel' van de fraudeurs. Ook de directe dader-slachtofferconfrontatie, die kenmerkend is voor traditionele diefstal, neemt hierbij meer indirecte vormen aan.

Dit geldt ook voor de fraude met online bankieren. Omdat steeds meer betalingen plaatsvinden via online bankieren, kunnen daders hier misbruik van maken, wanneer zij bijvoorbeeld door middel van phishing of malware kennis weten te krijgen van de inloggegevens van burgers of bedrijven. Hoewel deze fraudevormen vaak worden ingedeeld aan de hand van kenmerken van nieuwe werkwijzen van daders (skimming, phishing, malware en de verschillende vormen daarvan), vallen deze vormen van fraude in de kern uiteen in twee categorieën: fraude door gebruik te maken van de ontwikkeling naar het gebruik van creditcards en pinpassen in het dagelijkse betalingsverkeer en fraude door gebruik te maken van de verschuiving naar online bankieren. Beide ontwikkelingen, die te maken hebben met de voortschrijdende digitalisering van het betalingsverkeer, gaan gepaard met nieuwe mogelijkheden van daders, maar gaan ook weer gepaard met nieuwe ontwikkelingen op het gebied van beveiliging en controle.
De voortschrijdende digitalisering van het betalingsverkeer zien we ook terug in de zaken uit de Monitor Georganiseerde Criminaliteit. In oude zaken zagen we bijvoorbeeld fraude met creditcards (bijvoorbeeld: casus 49) die bestond uit het fysiek 'skimmen' van creditcards (bijvoorbeeld in restaurants of winkels), het klonen van de creditcards en het op pad sturen van mededaders (of het verkopen van deze creditcards en/of creditcardgegevens) om – vaak in het buitenland – te cashen; door het doen van betalingen of het aankopen van goederen en diensten. Deze fraude wordt uiteindelijk altijd ontdekt – door de creditcardmaatschappij, de bank of de klant, maar de modus operandi maakt gebruik van het feit dat er vaak veel tijd verstrijkt tussen het daadwerkelijk cashen in het buitenland en het moment van ontdekking.
We zien echter ook dat deze betaalkaartfraude (creditcards en/of pinpassen) tegenreacties heeft opgeroepen. In de eerste plaats is de beveiliging van betaalkaarten verbeterd, onder meer door de introductie van een beter beveiligde chip en/of een pincode. In de tweede plaats is er sprake van 'geoblocking': consumenten moeten voor gebruik van hun betaalkaart buiten Europa in de regel expliciet toestemming vragen, waardoor de standaard modus operandi van daders (die vaak buiten Europa cashten) rechtstreeks wordt gedwarsboomd. In de derde plaats is de fraudecontrole vanuit de bedrijven die betaalkaarten uitgeven ook sterk verbeterd. Het gevolg is dat het schadebedrag van fraude met betaalkaarten de laatste jaren zeer sterk is gedaald. Figuur 1 laat de ontwikkeling van twee verschillende vormen van schade zien (NVB, 2017): schade door fraude met betaalkaarten (skimming: de oranje lijn) en schade door fraude met internetbankieren (de lichtbruine balken, waarbij die schade vanaf 2012 ook wordt onderverdeeld in de subcategorieën phishing (de paarse lijn), malware (de blauwe lijn) en overige vormen van fraude). De schade ten gevolge van skimming is sinds 2011 zeer sterk gedaald: van iets minder dan 40 miljoen euro in 2011 naar grofweg 2 miljoen euro. Een soortgelijke, zeer sterke daling zien we vanaf 2012 bij de fraude met internetbankieren en de subcategorieën phishing en malware (NVB, 2017).[24]

[24] De beschreven daling omvat alleen de schade die bij de banken bekend is en dus niet noodzakelijkerwijs alle gevallen van door individuen geleden schade.

Figuur 1 Schade door fraude met internetbankieren (x € 1.000)



* Sinds 2012 wordt in de frauderapportage een onderscheid gemaakt tussen phising, malware en overige fraudevormen.

Bron: NVB (2017)

De opkomst van phishing, malware en overige vormen van fraude met internetbankieren is gerelateerd aan het sterk toegenomen gebruik van het online betalingsverkeer. Het gemak van online betalen gaat ook gepaard met een toegenomen kwetsbaarheid van consumenten, omdat zij online kunnen worden benaderd of gebruikmaken van technische hulpmiddelen die door anderen kunnen worden gehackt en/of geïnfecteerd (bijvoorbeeld via emails die leiden tot geslaagde phishing of infectie met malware).
De beveiliging van de consument (en van de bank) bepaalt hoe gemakkelijk cybercriminelen toegang kunnen krijgen tot een bankrekening. Daarbij spelen naast digitale beveiliging ook sociale aspecten een rol: is de phishingemail overtuigend en in de juiste bewoordingen (en in de juiste taal) opgesteld? En hoe geloofwaardig is de website waar de consument naar toe wordt geleid? Ook de beveiliging door banken (bijvoorbeeld door middel van 2-stapsauthenticatie, waarbij een unieke code wordt toegestuurd die vervolgens binnen een kort tijdsbestek moet worden ingevoerd) speelt een belangrijke rol bij de vraag hoeveel moeite cybercriminelen moeten doen om een cliënt te misleiden en vervolgens 'uit te melken'.
Wat internet heeft veranderd, is dat veel consumenten via internet benaderd kunnen worden door cybercriminelen en dat deze cybercriminelen heel veel slachtoffers tegelijk kunnen benaderen en in principe ook kunnen afwachten wie wel en niet 'hapt' op een 'phishing-mail' of malware-aanval. Het potentiële bereik voor daders is dus veel groter geworden, al zijn geloofwaardige 'phishing-mails' en websites wel gebonden aan taalgrenzen en lokale kennis over bijvoorbeeld banken. Het delict draait uiteindelijk nog steeds om het afhandig maken van geld, dat digitaal kan worden overgemaakt, maar uiteindelijk nog steeds vaak fysiek 'gecasht' wordt, al dan niet door een money mule. De snelheid van ontdekking van de fraude door de consument of door de bank speelt daardoor ook een belangrijke rol.
Het daadwerkelijk cashen van het geld is nog steeds een risicovolle actie, met bijvoorbeeld een grote kans op ontdekking voor mensen die hun bankrekening laten gebruiken en het geld cash (laten) opnemen. Waar de voorkant van deze criminele processen dus steeds meer wordt gedigitaliseerd, is het einde van het proces nog steeds vaak heel fysiek het cashen van geld. Het rekruteren en gebruiken van bij-

voorbeeld money mules is een logistieke bottleneck en het risico van deze money mules blijft – ook door de toegenomen beveiliging en fraudedetectie – hoog.[25] Digitalisering heeft positieve en negatieve kanten, zowel vanuit het perspectief van daders als vanuit het perspectief van slachtoffers. Digitalisering kan de kwetsbaarheid van burgers en bedrijven enerzijds verhogen, maar kan anderzijds ook weer nieuwe beveiligingsmogelijkheden bieden voor banken en hun klanten. Zo kunnen banken digitale transacties beter gaan monitoren en fraudedetectiesystemen ontwikkelen. Ook hebben klanten een beter en actueler inzicht in hun eigen transacties dan vroeger het geval was en is inmiddels een breed publiek zich bewust van kwetsbaarheden die het online betalingsverkeer met zich meebrengt.
Concluderend kan dus worden gesteld dat de digitalisering van het betalingsverkeer nieuwe mogelijkheden heeft gecreëerd voor daders. Maar bepaalde onderdelen van het criminele proces, zoals het cashen van het afhandig gemaakte geld, zijn nog steeds vaak heel fysiek, herkenbaar en risicovol. Ook heeft de digitalisering tegenreacties opgeroepen in de vorm van verbeterde beveiliging en fraudedetectie (zie ook Schuppers et al., 2016). De netto-uitkomst van deze ontwikkelingen is dat het schadebedrag van de bovengenoemde nieuwe vormen van fraude de laatste jaren niet is gestegen, maar juist zeer sterk is gedaald (althans voor zover dit blijkt uit de gepubliceerde cijfers van de Nederlandse Vereniging van Banken (NVB, 2017)).

3.5 Recapitulatie

In dit hoofdstuk werd ingegaan op de vraag welke rol ICT speelt bij logistieke problemen die moeten worden opgelost om criminele activiteiten succesvol te laten verlopen en welke veranderingen het gebruik van ICT met zich meebrengt. Naast een overzicht van de literatuur werd in dit hoofdstuk specifiek ingegaan op ontmoeten en communiceren (paragraaf 3.3) en op logistieke bottlenecks (paragraaf 3.4): bij traditionele georganiseerde criminaliteit en de doorvoer via (lucht)havens, de ontwikkeling van online drugsmarkten en fraude met het betaalverkeer.
Bij ontmoeten en communiceren speelt afscherming en vertrouwen een grote rol. Daders zijn zich bewust van het feit dat openlijk communiceren over criminele zaken risico's met zich meebrengt en dat het handig gebruikmaken van ICT deze risico's deels kan beperken. Andere mogelijkheden om deze risico's te beperken zijn persoonlijke ontmoetingen en communicatie op plekken die in de perceptie van daders niet of moeilijk afgeluisterd kunnen worden: auto's, woningen, horecagelegenheden, bedrijven of andere 'offender convergence settings', plekken waar daders mededaders en potentiële mededaders en klanten kunnen ontmoeten. De mate waarin deze plekken als privaat, semi-publiek of publiek kunnen worden gekarakteriseerd, varieert. We zien dat deze 'offender convergence settings' veelal in de semipublieke sfeer liggen en dat 'toegangscontrole' een belangrijke rol speelt. De plaatsen zijn vaak in principe publiek toegankelijk, maar niet voor iedereen. Bovendien kent de formele en informele toegangscontrole sociale aspecten: mensen worden herkend en worden wel of niet toegelaten of de aard van de activiteiten en gesprekken wordt aangepast. Daardoor is het mogelijk om publieke toegang en heimelijkheid met elkaar te combineren.
ICT heeft nieuwe mogelijkheden gecreëerd, meer in het bijzonder ten aanzien van de versleuteling van communicatie. Zo speelt het gebruik van telefoontoestellen met PGP-encryptie een belangrijke rol. Naast het gebruik van mogelijkheden op het

[25] Behalve via money mules kan ook via identiteitsfraude geld van slachtoffers worden doorgesluisd. Dit komt erop neer dat via de persoonlijke gegevens van een derde een betaaldienst wordt afgenomen. Die betaaldienst wordt bijvoorbeeld vervolgens gebruikt om het ontvangen geld van het slachtoffer verder door te sluizen.

gebied van (tele)communicatie, komen in de dossiers ook manieren naar voren waarop verdachten proberen om een anonieme fysieke omgeving te creëren. Zo zagen we in onderzochte zaken dat bij doorzoekingen van locaties apparatuur wordt aangetroffen om (tele)communicatie te verstoren of afluisterapparatuur te detecteren.

De laatste paragraaf van dit hoofdstuk had betrekking op logistieke bottlenecks bij verschillende criminele activiteiten. ICT heeft de mogelijkheden voor controle op goederen en luchtvaart- en haventerreinen vergroot. Daardoor is voor daders het belang van toegang tot geautomatiseerde systemen toegenomen. Die toegang kunnen zij krijgen door medewerking van personeel of, zoals in een zaak gebeurde, door in te breken op de desbetreffende computernetwerken. Bij het laten meeliften van goederen op bestaande vervoersstromen is de kern van deze logistieke bottleneck echter niet veranderd: om de lading te volgen en op tijd de illegale goederen uit deze legale lading te halen, moet men nog steeds zelf toegang hebben, moet men gebruikmaken van insiders of moet men deze insiders misleiden.

Bij de opkomst van online drugsmarkten zien we dat ICT nieuwe mogelijkheden biedt om het hoofd te bieden aan risico's en problemen die inherent zijn aan het uitvoeren van criminele activiteiten, zoals anonieme ontmoetingen tussen aanbieders en afnemers van (vooral kleinere hoeveelheden) verdovende middelen en de overdrachts- en betalingsproblemen die daarbij horen. Toch zien we dat niet het gehele criminele bedrijfsproces wordt gedigitaliseerd. Naast online aspecten kennen deze criminele activiteiten nog steeds belangrijke offline aspecten, waarvoor digitalisering geen oplossing biedt, zoals bijvoorbeeld het onderhandelen over en overdragen van grotere hoeveelheden verdovende middelen.

Bij fraude met het betalingsverkeer zien we dat door de digitalisering van het betalingsverkeer de directe dader-slachtofferconfrontatie, die kenmerkend is voor traditionele diefstal, meer indirecte vormen aanneemt, zoals 'skimmen' van creditcards, phishing, malware en andere vormen van fraude met internetbankieren.[26] In de kern komen deze criminele activiteiten echter neer op het mensen afhandig maken van geld. Wat internet heeft veranderd, is dat veel consumenten via internet benaderd kunnen worden door cybercriminelen en dat deze cybercriminelen heel veel slachtoffers tegelijk kunnen benaderen en in principe ook kunnen afwachten wie wel en niet 'hapt' op een 'phishing-mail' of malware-aanval. Het potentiële bereik voor daders is dus veel groter geworden. Aan de andere kant is het cashen van het buitgemaakte geld nog steeds een risicovolle actie, met bijvoorbeeld een grote kans op ontdekking voor mensen die hun bankrekening laten gebruiken en het geld cash (laten) opnemen. Waar de voorkant van deze criminele processen dus steeds meer wordt gedigitaliseerd, is het einde van het proces nog steeds vaak heel fysiek het cashen van geld. Het rekruteren en gebruiken van bijvoorbeeld money mules is een logistieke bottleneck en het risico van deze money mules blijft – ook door de toegenomen beveiliging en fraudedetectie – hoog. Ten slotte blijkt dat digitalisering het ook voor banken en slachtoffers gemakkelijker kan maken om beveiliging en fraudedetectie te verbeteren (zie ook Schuppers et al., 2016). In de afgelopen jaren is het schadebedrag ten gevolge van de genoemde fraudevormen dan ook niet gestegen, maar juist zeer sterk gedaald (althans voor zover dit blijkt uit de gepubliceerde cijfers van de Nederlandse Vereniging van Banken (NVB, 2017)).

[26] Hoewel er ook bij cybercrime wel degelijk een dader-slachtoffercontact kan zijn, bijvoorbeeld wanneer een dader een specifiek slachtoffer telefonisch benadert om hem te bewegen bepaalde gegevens af te geven (Schuppers et al., 2016).

4 Criminele geldstromen en het gebruik van ICT

Georganiseerde criminaliteit is vaak gericht op het behalen van financieel voordeel.[27] Maar het genereren van criminele verdiensten stelt een dader ook voor problemen. Hoe kan hij over zijn geld beschikken zonder onder de aandacht van de autoriteiten te komen? Ook het beheren van geldstromen vormt met andere woorden een flessenhals in het criminele bedrijfsproces. Criminele geldstromen en de rol die ICT daarbij speelt vormen het onderwerp van dit hoofdstuk. Daarbij komen, voor zover de beschikbare informatie dat toelaat, de verdiensten zelf, de besteding ervan en het afschermen van criminele inkomsten aan bod. Net als in de vorige hoofdstukken beginnen we met een bespreking van inzichten die de bestaande literatuur ons biedt (paragrafen 4.1 en 4.2). In de paragrafen 4.3 en 4.4 komen de resultaten aan bod van de empirische analyse van de dertig zaken uit de vijfde ronde van de Monitor Georganiseerde Criminaliteit. Waar dat relevant is, zal daarbij afzonderlijk worden ingegaan op respectievelijk traditionele georganiseerde criminaliteit (casus 157-172, 174-180), traditionele georganiseerde criminaliteit waarbij het gebruik van ICT een belangrijk vernieuwend element in de modus operandi is (casus 151, 152 en 173), georganiseerde low-tech cybercriminaliteit (casus 154 en 156) en georganiseerde high-tech cybercriminaliteit (casus 153, 155). Paragraaf 4.5 biedt een recapitulatie.

4.1 Georganiseerde criminaliteit offline: een overzicht

Hieronder volgt een overzicht van de literatuur over geldstromen in de traditionele, dat wil zeggen offline uitgevoerde, georganiseerde criminaliteit. Daarbij putten we uit eerdere rapportages van de Monitor Georganiseerde Criminaliteit en enkele andere bronnen.

Criminele verdiensten

De omvang van criminele verdiensten is voor een belangrijk deel onbekend. Er is met andere woorden sprake van een *dark number*. Uit de aard der zaak is het een grootheid die zich alleen laat schatten. Dat geldt op macro-niveau, dat wil zeggen op landelijk of internationaal niveau, maar vaak ook op het micro-niveau van individuele zaken of daders.

Schattingen van de wereldwijde omzet van georganiseerde criminaliteit verschillen sterk. Afzonderlijke schattingen kennen bovendien vaak grote onzekerheidsmarges. Die wereldwijde omzet zou volgens schattingen in ieder geval honderden miljarden Amerikaanse dollars bedragen (Buehn & Schneider, 2013, p. 172-174; Schneider & Windischbauer, 2008, p. 391-392). Voor Nederland maakten Kazemier en Rensman (2015) een schatting van de bijdrage van een aantal illegale activiteiten aan het nationaal inkomen van Nederland. Zij schatten dat drugshandel, prostitutie, smokkel van sigaretten, heling, illegaal kopiëren en illegaal gokken in totaal voor 2,6 miljard euro bijdragen aan ons nationaal inkomen, met een geschatte ondergrens van 2,0 en een bovengrens van 3,4 miljard euro.[28] In de monitorrapportage van 2012 (en

[27] Ook andere drijfveren kunnen een rol spelen, zoals de zucht naar een 'spannend' leven of de wens om indruk te maken op de omgeving (Naylor, 1999, p. 11).

[28] Criminele activiteiten die vooral bestaan uit gedwongen vermogensoverdracht zijn in de schattingen niet meegenomen omdat ze niet bijdragen aan het nationale inkomen. Prostitutie zijn wel in de schattingen meegenomen ondanks de opheffing van het bordeelverbod.

eerder in andere bronnen) is al geconstateerd dat ook in individuele opsporingsonderzoeken er vaak geen volledig beeld bestaat van de opbrengsten van georganiseerde criminaliteit. Vaak wordt maar een (klein) deel van de verdiensten die aan daders worden toegeschreven ook daadwerkelijk aangetroffen (Kruisbergen et al., 2012, p. 229-256; Meloen et al., 2003, p. 12-13, 23, 343-344; Kleemans et al., 2002, p. 124-125). Vanwege deze informatiebeperking en omdat het verzamelde materiaal zich daarvoor niet leent, is het niet mogelijk om op basis van de bestudeerde zaken een schatting te maken van de verdiensten van de Nederlandse georganiseerde criminaliteit als geheel. Wel werd in het laatste monitorrapport ter illustratie een bandbreedte aangegeven voor de hoogte van het veronderstelde wederrechtelijk verkregen voordeel. Voor de zaken waarin er een berekening was gemaakt van de totale criminele winsten van een criminele groepering, varieerden de bedragen van minder dan enkele duizenden tot vele miljoenen euro's (Kruisbergen et al., 2012, p. 159-160). Ten slotte is in het laatste monitorrapport ook ingegaan op de verdeling van criminele verdiensten binnen een crimineel samenwerkingsverband. Daarin werd een tweedeling beschreven tussen aan de ene kant een kern van twee tot vier hoofdrolspelers die meestal het overgrote deel van de verdiensten krijgen en aan de andere kant een categorie van vooral uitvoerenden die meestal een veel kleiner deel ontvangen. Ook werd voor drugsproductie/-handel beschreven dat de scheefheid van de verdeling van de winsten verschilt per drugsmarkt en lijkt samen te hangen met de logistieke aard van de handelsketen. Zo verdienen de importeurs van cocaïne, die zorgen dat de cocaïne vanuit Zuid-Amerika de Europese markt bereikt, veel meer dan degenen die zorgen voor de distributie. Daarnaast geldt dat de verdeling van criminele winsten geen statisch gegeven is; daders kunnen natuurlijk proberen hun eigen aandeel in de opbrengsten te vergroten. Dit gebeurt ook, zo bleek uit de analyse destijds, en in het geval van drugshandel lijkt dat vooral neer te komen op het passeren, bedriegen of bestelen van 'zakenpartners' (zie Kruisbergen et al., 2012, p. 161-176).

Besteding van criminele verdiensten

Empirisch onderzoek naar wat daders doen met hun geld is relatief schaars (Malm & Bichler, 2013; Verhage, 2011, p. 172; Fernández Steinko, 2012, p. 909; Levi, 2012). In de monitorrapportage van 2012 en in een aantal verdiepende publicaties is echter uitgebreid ingegaan op besteding, afscherming en het opsporen en afpakken van criminele inkomsten.[29] De besteding valt uiteen in consumptie en investeringen. Voor het consumptiepatroon geldt dat in ieder geval een deel van het casusmateriaal daders laat zien met een (zeer) luxe levensstijl. In die zaken wordt veel geld uitgegeven aan bijvoorbeeld dure auto's, horloges, juwelen, woninginrichting, vakanties en uitgaan. Er zijn echter ook zaken waarin daders er voor zover bekend een sober uitgavenpatroon op nahouden (Kruisbergen et al., 2012, p. 176-177).

Blijft er na de consumptie, de kosten van het levensonderhoud en de financiering van criminele activiteiten nog geld over, dan kan een dader ervoor kiezen geld te investeren in de legale economie. Investeringen van daders in de reguliere economie blijken enerzijds vooral uit onroerend goed te bestaan, dat wil zeggen woningen, zakelijk onroerend goed en grond. Anderzijds gaat het om bedrijven. Uit bestudering van 150 zaken uit de eerste vier rondes van de monitor bleek dat het daarbij, vooral bij daders binnen drugs-, mensenhandel-, mensensmokkel- en illegale-wapenhandelzaken, vaak gaat om bedrijven in de sector groot-/detailhandel (bijvoorbeeld bedrijven die fruit of andere goederen importeren/exporteren) en bedrijven als hotels, bars en restaurants, transportbedrijven, bordelen, en bedrijven

[29] Voor een bespreking van een aantal andere studies op dit terrein, zie Kruisbergen et al. (2015a, p. 239-241).

die behoren tot de financiële dienstverlening. Bij de laatstgenoemde bedrijven gaat het niet zo zeer om banken, maar om management-/investmentsbedrijven of holdings die vooral worden gebruikt om ander bezit, onroerend goed bijvoorbeeld, onder te brengen.[30] Verder bleken investeringen vooral te worden gedaan in het woonland of het land van herkomst. Voor meer dan de helft van de bedrijven waarin daders hebben geïnvesteerd, werd in het zaakdossier informatie aangetroffen die indiceert dat het bedrijf een functie vervult binnen de criminele activiteiten van de dader.[31]
Veel daders lijken al met al een vrij conservatief investeringspatroon te hebben, waarbij de afstand tussen hen en hun investering vrij klein is, zowel in fysieke als in sociale zin. Ze lijken immers vooral te investeren in hun land van herkomst of hun woonland, vooral in goederen en bedrijven waarmee ze vanuit het dagelijks leven bekend zijn (huizen en ander vastgoed en bedrijven uit bekende sectoren als groot-/detailhandel, horeca en transport), en bedrijven worden vaak gebruikt ter ondersteuning van de criminele activiteiten. Puur financiële investeringen daarentegen, zoals obligaties, opties en aandelen in bedrijven waarin daders níét persoonlijk betrokken zijn, bijvoorbeeld in beursgenoteerde bedrijven, werden in maar een klein aantal zaken gezien (Kruisbergen et al., 2012, 2015a, 2015b; zie ook Bruinsma 1996; Bruinsma & Bovenkerk 1996; Kleemans et al. 2002; Van Duyne & Levi 2005).

Afschermen en witwassen van criminele verdiensten
In de 150 zaken die tot en met de vierde ronde van de Monitor Georganiseerde Criminaliteit zijn bestudeerd, werd een breed scala aan werkwijzen aangetroffen waarmee daders hun criminele inkomsten proberen af te schermen. De meest basale werkwijze is het simpelweg verstoppen van geld, bijvoorbeeld door het te begraven. Maar daders kunnen hun geld ook verplaatsen, bijvoorbeeld naar landen waar het toezicht op het financiële verkeer minder stringent is. Dat verplaatsen kan onder meer via geldkoeriers plaatsvinden, via money transfer-instellingen of via een zogenoemde ondergrondse bankier (Kruisbergen et al., 2012, p. 187-228).
Verder zijn er manieren om de inkomsten afgeschermd in Nederland uit te geven. In de vierde monitorrapportage noemden we dit 'afgeschermd consumeren'. Het kan betekenen dat een dader contant geld besteedt aan het gebruik van een voertuig of woonruimte zonder dat deze goederen naar hem zijn te herleiden, bijvoorbeeld door de inschakeling van een facilitator of katvanger. Daarnaast zijn er meer complexe witwasconstructies. Zo kan de herkomst van misdaadgeld worden verhuld door bijvoorbeeld het fingeren van een lening (aan jezelf, 'loan back') of het fingeren van een inkomen uit een dienstbetrekking of winst uit een kansspel of bedrijf/handel. Ook het doorsluizen van geld via een reeks van transacties naar vennootschappen of personen is een beproefde methode (Kruisbergen et al., 2012, p. 187-228).[32]
Wanneer een dader niet voldoende in staat (of bereid) is om zelfstandig zijn geld wit te wassen, kan daarvoor een facilitator worden ingeschakeld (Soudijn, 2017). Facilitators bij witwassen kunnen onder meer bestaan uit ondergrondse bankiers

[30] In fraude- en witwaszaken zien we deels een ander investeringspatroon. Investeringen die in die zaken werden aangetroffen, betreffen vaker vastgoedbedrijven en de zojuist genoemde holdings.

[31] Die functie kan liggen op het terrein van de logistiek (opslag, transport, ontmoetingen etc.), legitimering (een bedrijf verschaft bijvoorbeeld de klading of een legitieme reden om bepaalde stoffen aan te kopen) of witwassen (zie Bruinsma & Bovenkerk, 1996).

[32] Het verhullen van de herkomst van misdaadgeld via rechtspersonen wordt mogelijk moeilijker door implementatie van de vierde anti-witwasrichtlijn van de Europese Unie. Deze richtlijn schrijft voor dat lidstaten in een register bijhouden wie de uiteindelijke belanghebbenden zijn van juridische entiteiten (zie ook Soudijn, 2017).

en geldsmokkelaars (die geld fysiek de grens overbrengen). Ook kan het gaan om personen met (toegang tot) posities in de formele economie die bijvoorbeeld via het opzetten van constructies helpen bij het wegsluizen van vermogen en eventueel het fingeren van een legitieme herkomst van dat vermogen. Het eindresultaat van deze verhullingen kan zijn dat het crimineel verdiende geld is geïnvesteerd in de 'bovenwereld', bijvoorbeeld in onroerend goed of bedrijven (Kruisbergen et al., 2012, p. 87; Soudijn, 2014).
De meest recente editie van de Criminaliteitsbeeldanalyse Witwassen constateert dat contant geld nog steeds een cruciale rol speelt binnen de georganiseerde criminaliteit, en mogelijk zelfs een grotere rol vanwege de striktere regulering van de legale financiële sector. Ook wordt in het rapport beschreven dat de belangrijkste witwasmethoden de laatste vijf jaar niet wezenlijk zijn veranderd. Relatief nieuw is wel het gebruik van *bitcoins* en *crowdfunding*, waarop we in de volgende paragraaf terugkomen (Soudijn, 2017).

4.2 Inzichten uit de literatuur op het terrein van 'cybercrime'

Hier bespreken we de inzichten die de literatuur biedt in de geldstromen bij cybercrimezaken. We bespreken achtereenvolgens de criminele verdiensten, de besteding van criminele verdiensten en het onderwerp afscherming en witwassen.

Criminele verdiensten
Er zijn verschillende schattingen in omloop van cybercrimemarkten en de schade als gevolg van cybercrime. Zo zijn er schattingen gemaakt van de omzet op darknet markets zoals Silk Road, Black Market Reloaded en Hansa, bijvoorbeeld door Aldridge en Decary-Hetu (2014; zie ook EMCDDA, 2016), Christen (2012), Kruithof et al. (2016) (zie EMCDDA & Europol, 2017). Verder schatte bijvoorbeeld een computerbeveiligingsbedrijf in 2014 de wereldwijde economische verliezen als gevolg van cybercrime op honderden miljarden Amerikaanse dollars.[33] Los van het feit dat economische schade iets anders is dan de verdiensten van daders, geldt net als bij offline criminaliteit dat het om schattingen gaat waarbij onderliggende gegevens verre van compleet zijn.[34] Ook zijn er pogingen ondernomen om de omvang van specifieke online cybercrimemarkten te schatten (bijvoorbeeld Dhanjani & Rios, 2008; Holz et al., 2009), maar lijkt dit door de verscheidenheid aan aangeboden waar, de onduidelijkheid over verschillen tussen vraagprijs en verkoopprijs (de deal wordt gesloten buiten het forum) en het ontbreken van adequate data of instrumenten een moeilijke zo niet onmogelijke opgave (Holt & Smirnova, 2014; Herley & Florencio, 2009).
Ook opsporingsonderzoeken naar cybercrime geven lang niet altijd inzicht in criminele verdiensten, zo blijkt bijvoorbeeld uit onderzoek op grond van Zweedse (Werner & Korsell, 2016) en Nederlandse zaken (Odinot et al., 2017[35]). De (veronderstelde) verdiensten in de elf Nederlandse zaken die Odinot en anderen onderzochten varieerden van meer dan een miljoen euro tot nul of onbekend, omdat geen informatie over verdiensten beschikbaar was (Odinot, et al., 2017, p. 80). Onderzoek

[33] Uitgedrukt als percentage van het Bruto Binnenlands Product zou volgens de schattingen van McAfee de schade als gevolg van cybercrime in Duitsland (1,60) en Nederland (1,50%) het grootste zijn (McAfee Center for Strategic and International Studies, 2014, p. 2, 9-10).

[34] In het aangehaalde geval geldt bovendien dat een computerbeveiligingsbedrijf zekere belangen heeft bij de 'vaststelling' van schade als gevolg van cybercrime.

[35] Vijf zaken op het terrein van cybercrime/ICT-gerelateerde georganiseerde criminaliteit die in deze vijfde ronde van de monitor zijn opgenomen, maakten ook onderdeel uit van de studie van Odinot et al. (2017).

naar Duitse zaken liet zien dat de 'schade' in achttien zaken in totaal 115 miljoen euro zou bedragen (Bulanova-Hristova & Kasper, 2016, p. 207). Over de verdeling en besteding van criminele inkomsten in cybercrimezaken is (eveneens) weinig bekend.

Besteding van criminele verdiensten
Net als in zaken van offline georganiseerde criminaliteit die bijvoorbeeld voor eerdere monitorrapporten zijn bestudeerd, zijn er ook in sommige cybercrimezaken aanwijzingen (zoals inbeslagnames) dat in ieder geval door een deel van de daders veel geld wordt uitgegevens aan een dure levensstijl (Odinot et al., 2017, p. 64; Leukfeldt, 2014; Leukfeldt et al., 2017c).

Afscherming en witwassen van criminele verdiensten
Ook daders die online opereren dienen hun inkomsten af te schermen wanneer ze willen voorkomen dat die inkomsten en zijzelf in handen van justitie vallen. De aard van verschillende vormen van cybercrime of door internet gefaciliteerde criminaliteit brengt met zich mee dat de directe opbrengsten vaak digitaal van aard zijn. Dit geldt bijvoorbeeld voor phishingaanvallen, banking malware en ransomware, maar ook voor online drugshandel. Oerlemans et al. (2016) onderzochten de geldstromen die in verband staan met banking malware en ransomware. Bij banking malware (waarvan de schade de laatste jaren sterk is afgenomen) wordt vaak gebruikgemaakt van *money mules*, personen die tegen vergoeding bijvoorbeeld hun bankrekening beschikbaar stellen aan criminelen. In eerste instantie wordt via banking malware het geld vanaf de rekening van het slachtoffer overgemaakt naar een rekening van zo'n money mule. Die money mule neemt vervolgens het bedrag zo snel mogelijk op bij een geldautomaat. Na het *cashen* (of de *cash-out*) kan het geld bijvoorbeeld via geldtransferkantoren naar het buitenland worden overgemaakt, waarna het weer door een (andere) money mule in het buitenland wordt opgenomen. Een andere werkwijze is dat met het via banking malware verkregen geld direct goederen of diensten worden aangekocht, zoals (luxe) goederen bij fysieke of webwinkels of bitcoins (Oerlemans et al., 2016).
Bij ransomware bestaan de opbrengsten – het losgeld – vaak uit bitcoins of tegoeden van online vouchers. Wanneer bitcoins zijn ontvangen kunnen de daders, al dan niet na het gebruik van bijvoorbeeld een 'mixing service', de bitcoins besteden of omwisselen voor bijvoorbeeld een contant bedrag aan euro's bij een fysieke bitcoinhandelaar of een bitcoin exchange (online wisselkantoor). Zijn de opbrengsten verkregen uit door het slachtoffer aangekochte vouchers, dan wordt de waarde van de vouchers bijgeschreven op een online account van een e-wallet-dienst[36], waarna eventueel andere afschermingsmethoden kunnen worden toegepast (Oerlemans et al., 2016).
Naast parasitaire vormen van online criminaliteit, zoals de toepassing van banking malware en ransomware, zijn er ook symbiotische vormen. Online drugshandel is daar een van de belangrijkste voorbeelden van. Online marktplaatsen als Silk Road, Agora, Black Market Reloaded, Nucleus, The Armory en Evolution opereren (of opereerden) als zogenoemde *darknet markets*, wat wil zeggen dat ze onderdeel uitmaken van een 'verborgen' deel van internet dat niet toegankelijk is voor standaard browsers. Dergelijke websites zijn doorgaans alleen toegankelijk via een browser als TOR (The Onion Router), die het IP-adres van een gebruiker verbergt en daarmee anoniem gebruik van internet mogelijk maakt. Naast het gebruik van TOR zijn ver-

[36] Een e-wallet is een online betalingsdienst (zoals PayPal) waarbij geld op een persoonlijk account kan worden geparkeerd, waarna bijvoorbeeld betalingen kunnen worden gedaan bij webwinkels (Oerlemans et al., 2016, p. 107-108).

sleutelde communicatie tussen koper en verkoper en betalingen via bitcoin de belangrijkste pijlers onder het functioneren van deze marktplaatsen, waar behalve drugs ook andere goederen (en diensten) worden verhandeld (EMCDDA, 2016; Kruithof et al., 2016).[37] Op bitcoins, vouchers en enkele andere nieuwe ontwikkelingen gaan we nu verder in.

Bitcoin is een *cryptocurrency*, oftewel een cryptografische munteenheid. In tegenstelling tot de dollar en euro wordt bitcoin niet uitgegeven, centraal beheerd of gecontroleerd door een bank, overheid of een andere centrale partij. Het gebruik van bitcoins is dan ook relatief ongereguleerd en niet onderworpen aan enige vorm van financieel toezicht.[38] Naast bitcoin zijn er overigens verschillende andere cryptocurrencies, waarvan Ethereum, Litecoin en Dogecoin enkele voorbeelden zijn. Bitcoin is wat marktwaarde betreft (al) lange tijd de belangrijkste cryptomunt (geweest) (Oerlemans et al., 2016; EMCDDA, 2016), hoewel het marktaandeel van bitcoin wel is afgenomen.[39]

Het aanmaken van bitcoins (*mining* (delven)) verloopt decentraal, en wel via een netwerk van computers van gebruikers. Bitcoins ontstaan door toepassing van een algoritme, een wiskundige formule. Iemand kan een bitcoin zelf aanmaken, maar daar is een enorme rekenkracht van computers voor nodig, en daarmee tevens een enorme hoeveelheid energie. Bitcoins kunnen daarom, via een online *bitcoin exchange*, een wisselkantoor, ook simpelweg worden aangekocht tegen betaling van reguliere muntheden. Voor het bewaren van bitcoins wordt gebruikgemaakt van een *wallet* (portemonnee), een bestand dat is opgeslagen op de eigen computer, in de cloud of op een smartphone (Oerlemans et al., 2016).

Voor personen met criminele bedoelingen biedt bitcoin in potentie belangrijke voordelen. Zoals gezegd is bitcoin niet onderworpen aan toezicht en verplichtingen die voor de reguliere financiële sector gelden, zoals de meldingsplicht met betrekking tot ongebruikelijke transacties. Daardoor is het in beginsel mogelijk om van achter je bureau bitcoins over te maken ten gunste van een andere partij waar dan ook ter wereld zonder tussenkomst van een instelling die aan toezicht is onderworpen. Een hiermee samenhangend voordeel is dat transacties met bitcoins een bepaalde mate van anonimiteit kennen (of kunnen hebben) (Oerlemans et al., 2016; Kruisbergen & Soudijn, 2015).

Het ongereguleerde karakter en de anonimiteit van bitcoin kent echter beperkingen. Zoals gezegd, geschiedt de aan- en verkoop van bitcoins, dat wil zeggen het omwisselen van bijvoorbeeld euro's in bitcoins en omgekeerd, (onder andere) bij bitcoin exchanges. Hoewel deze wisselkantoren in Nederland niet onder financieel toezicht vallen, voeren zij op vrijwillige basis soms toch een anti-witwasbeleid waarbij gebruikers worden geïdentificeerd. Verder vallen bitcoin exchanges in bijvoorbeeld de Verenigde Staten wel onder toezicht (Oerlemans et al., 2016, p. 108-109). Daarnaast worden alle transacties die met bitcoins worden gedaan, zoals de aankoop van drugs op een website als (het voormalige) Silk Road, opgeslagen in een soort logboek, de *block chain*. De transacties zijn in die zin volledig transparant want voor iedereen te volgen. Een bitcointransactie bestaat uit een overboeking van het ene bitcoinadres naar het andere, en dat is dan ook wat in de block chain is na te gaan. De herkomst van elke bitcoin kan daarmee worden getraceerd, maar in beginsel kan de identiteit van de personen achter de transacties verborgen blijven. Transacties zelf kunnen echter tot op zekere hoogte aan elkaar worden gekoppeld en bovendien

---

[37] Verschillende van deze marktplaatsen zijn offline gehaald, waarna echter vaak weer alternatieven ontstaan. Naast *darknet market* wordt ook de term *cryptomarket* gebruikt (EMCDDA, 2016; Kruithof et al., 2016).

[38] Dit verandert mogelijk nu Bitcoin in sommige landen als officieel betaalmiddel wordt gezien, zoals in Japan (https://fd.nl/beurs/1200322/bitcoin-bereikt-nieuw-hoogtepunt-op-goed-nieuws-uit-japan-en-vs).

[39] Zie de historische reeksen op: https://coinmarketcap.com/historical/.

slagen gebruikers er niet altijd in hun identiteit verborgen te houden. Meiklejohn et al. (2013) hebben dan ook aangetoond dat via technieken om netwerkdata te analyseren en vanwege het 'onveilige' gedrag van gebruikers, transacties soms wel degelijk naar personen herleid kunnen worden. Vooral wanneer iemand grote bedragen aan bitcoins in bezit heeft, zou het moeilijker zijn anonimiteit te handhaven (Meiklejohn et al., 2013; Ron & Shamir, 2013; Oerlemans et al., 2016; Kruisbergen & Soudijn, 2015). Een bitcoingebruiker staan verschillende diensten ter beschikking die de herleidbaarheid van transacties verkleinen. Hierop gaan we straks nader in.

Behalve het feit dat de anonimiteit van bitcoingebruikers zeker geen gegeven is, kent bitcoin ook een aantal specifieke nadelen. Zo brengt het vrije karakter van bitcoin met zich mee dat gebruikers niet worden beschermd door waarborgen die in de formele financiële sector wel gelden. Zo verdwenen enkele jaren geleden honderdduizenden bitcoins via de erg populaire bitcoin exchange Mt. Gox[40] en in de zomer van 2017 hebben hackers grote hoeveelheden van de cryptomunteenheid Ethereum buitgemaakt.[41]

Een ander risico dat verbonden is aan bitcoin is het nogal grillige koersverloop. Ten slotte is de acceptatie van de bitcoin als betaalmiddel in de offline wereld nog beperkt, hoewel het aantal bedrijven en personen dat bitcoins als betaling accepteert toeneemt (Kruisbergen & Soudijn, 2015; Oerlemans et al., 2016).

In de opsporingspraktijk wordt het gebruik van bitcoins de laatste jaren vaker aangetroffen, zo wordt in de meest recente editie van de Criminaliteitsbeeldanalyse Witwassen geconstateerd. De in de opsporingsonderzoeken aangetroffen bitcointransacties hebben vaak betrekking op relatief kleine bedragen.[42] Wel is het zo dat sommige daders zijn te relateren aan vele kleine transacties die samen flink optellen. De criminaliteitsbeeldanalyse spreekt de verwachting uit dat het gebruik van bitcoins op criminele marktplaatsen zal toenemen.

Zoals gezegd, wordt bitcoin niet centraal beheerd. Een voorbeeld van centraal beheerd virtueel 'geld' is *WebMoney*. Webmoney is een online systeem dat wordt gebruikt voor het bewaren en uitwisselen van waarde-eenheden. Voor het openen van een Webmoneyrekening is geen bankrekening of creditcard nodig. Een rekening, of *purse*, kan in verschillende eenheden worden aangehouden, zoals euro's, Amerikaanse dollars, Russische roebels en bitcoins. Webmoney kan onder meer worden gebruikt om bij sommige online winkels te betalen (Oerlemans et al., 2016, p. 54).[43]

Het gebruik van bitcoins is een van de weinige veranderingen op het terrein van witwassen die in de Criminaliteitsbeeldanalyse Witwassen worden beschreven. Het toegenomen gebruik van *vouchers* en/of *prepaidkaarten* is eveneens 'nieuw'. Deze worden in vergelijking met de eerdere editie van de Criminaliteitsbeeldanalyse Witwassen vaker in opsporingsonderzoeken in beslag genomen. De kaarten die in Nederland worden uitgegeven zijn echter aan limieten gebonden. Bovendien is bij het aanvragen van een kaart of het storten van geld vaak identificatie vereist. Dit zijn twee belangrijke beperkingen voor het gebruik voor witwasdoeleinden. Er zijn

---

[40] Zie Moore en Christin (2013) voor een bespreking van de risico's die zijn verbonden aan bitcoin exchanges (hun publicatie verscheen overigens voordat het verdwijnen van de bitcoins bij Mt. Gox aan het licht kwam).

[41] http://datanews.knack.be/ict/nieuws/7-miljoen-dollar-aan-ethereum-gestolen-in-online-overval/article-normal-879833.html

[42] Individuele betalingen van miljoenen euro's werden niet aangetroffen. Wel bedroegen sommige bitcointransacties tienduizenden euro's tot meer dan honderdduizend euro (Soudijn, 2017).

[43] Zie www.wmtransfer.com (laatst geraadpleegd op 16 november 2017).

echter ook buitenlandse kaarten in omloop die minder beperkingen kennen.[44] Ten slotte beschrijft de criminaliteitsbeeldanalyse ook het gebruik en opzetten voor witwasdoeleinden van een *payment service provider* (PSP), een online betaaldienstverlener die betalingen bij winkeliers kan afhandelen (Soudijn, 2017).[45]
De veranderingen die in de Criminaliteitsbeeldanalyse Witwassen worden beschreven hangen voor een belangrijk deel samen met het gebruik van internet: vaker gebruik van bitcoins en prepaidkaarten (hoewel doorgaans relatief kleine bedragen); het (zeer beperkte) gebruik van crowdfunding; en het gebruik van een PSP voor witwasdoeleinden. Er hebben echter geen veranderingen op grote schaal plaatsgevonden en al met al lijkt witwassen redelijk traditioneel plaats te vinden. De meest in het oog springende overeenkomst, tussen meer actuele en iets oudere witwaszaken, maar ook tussen witwassen bij respectievelijk offline en online criminele activiteiten, is misschien wel het grote belang van contant geld (Soudijn, 2017). In de vorige paragraaf merkten we op dat contant geld een cruciale rol speelt binnen de offline georganiseerde criminaliteit. Hetzelfde lijkt te gelden voor daders die zich met cybercrime bezighouden, zo blijkt uit verschillende bronnen. Zo belandt het geld verkregen via banking malware en ransomware uiteindelijk, via tussenstappen/-personen, vaak contant in de handen van de daders (Leukfeldt, 2014; Leukfeldt et al., 2017a, 2017b, 2017c; Odinot et al., 2017, p. 38; Oerlemans et al., 2016). Zowel bij criminele betalingen als bij witwassen heeft contant geld nog steeds de voorkeur, ook bij cybercriminelen (Europol, 2015a). Het gebruik van virtuele munten en prepaidkaarten biedt nieuwe mogelijkheden voor criminelen, maar in de praktijk worden ze vooral in combinatie met contant geld gebruikt. Europol spreekt in dit verband van een symbiose tussen traditionele methoden en nieuwe technologie (Europol, 2015a). Mogelijk is de rol van contant geld zelfs groter geworden, vanwege het feit dat veel digitale betaalmethoden vaak sporen nalaten en vanwege de striktere regulering van de legale financiële sector (Europol, 2015a; Soudijn, 2017). Heeft de cybercrimineel zijn verdiensten eenmaal (omgezet in) in contant geld, dan kan hij gebruikmaken van dezelfde middelen om zijn verdiensten af te schermen als die andere daders ook ter beschikking staan, zoals het verplaatsen van zijn geld (fysiek of via bijvoorbeeld money transfers of een ondergrondse bankier), de (verhulde) aankoop van kostbare goederen of witwassen door bijvoorbeeld het fingeren van inkomen of winst uit bedrijfsactiviteiten (zie ook Europol, 2015a, p. 370-378).
Bij het afschermen van de criminele inkomsten die online zijn gegenereerd, wordt gebruikgemaakt van verschillende (nieuwe) soorten dienstverleners die gewild of ongewild bij de criminele geldstromen zijn betrokken.[46] Een belangrijke categorie van professionele facilitators die doelbewust diensten aan criminelen leveren vormen de malafide *bitcoinhandelaren*. Dit zijn personen die tegen een prijs ver boven de reguliere marktprijs bereid zijn grote bedragen om te wisselen. Zij opereren vaak in openbare gelegenheden waar zij in bijzijn van een klant op een computer een

[44] Weer een andere nieuwe ontwikkeling is het, weliswaar zeer beperkte, gebruik van *crowdfunding* als variant binnen een *loan back*-witwasconstructie. Een verdachte richtte zich via internet tot de *crowd* ter financiering van een vastgoedobject. Daarop werd ingegaan door tientallen (fictieve) personen, die vermoedelijk door de verdachte zelf van geld werden voorzien (Soudijn, 2017).

[45] Een PSP stuurt vaak verschillende transacties in een grote batch op, waardoor de transacties niet meer op consumentenniveau zijn uit te splitsen en de bank minder controles kan uitoefenen (Soudijn, 2017).

[46] We noemen hier alleen die dienstverleners die in de literatuur specifiek in relatie tot online activiteiten worden genoemd.

transactie uitvoeren.[47] *E-walletdiensten* spelen een centrale rol bij het aan- en verkopen van bitcoins. Daarbij worden ook varianten aangeboden die specifiek zijn ingericht op het verhullen van het spoor tussen zend- en ontvangstadres van een bitcoin (en het beschermen van de identiteit van de zender of ontvanger). Voor het verbreken van dat spoor zijn op het darknet ook verschillende afzonderlijke diensten beschikbaar, zogenoemde *mixing* of *tumbler services* als bitcoin fog en helix. Daarnaast werden hierboven al *payment service providers* en *prepaid*kaarten *en voucherdiensten* besproken. Verder zagen we bijvoorbeeld dat katvangers, *money mules*, een belangrijke rol spelen bij banking malware en phishing (voor een analyse van de achtergrondkenmerken van money mules zie Oerlemans, et al., 2016). Uit de studie van Oerlemans en anderen blijkt dat deze mules vooral geronseld worden uit jongvolwassenen tussen de 18 en 22 jaar uit armere wijken in vooral de grote steden (Oerlemans et al., 2016; zie ook Mauritz, 2014). Ten slotte spelen ook *banken* een belangrijke rol in de modus operandi van veel daders, aangezien zij de infrastructuur verzorgen waar bijvoorbeeld bij banking malware of door bitcoinwisselaars gebruik van wordt gemaakt. Door (onder andere) verschillende maatregelen die banken hebben genomen is de schade van banking malware de laatste sterk afgenomen (EMCDDA, 2016; Odinot et al., 2017; Oerlemans et al., 2016; Soudijn, 2017; zie hoofdstuk 3).

4.3 Analyse van bestudeerde zaken: criminele verdiensten en besteding

Criminele verdiensten

In deze en de volgende paragraaf komen de resultaten aan bod van een analyse van de geldstromen in de dertig zaken uit de vijfde ronde van de Monitor Georganiseerde Criminaliteit. Hieronder gaan we eerst vooral in op de criminele verdiensten en de besteding van die verdiensten. Omdat er wat betreft verdiensten en bestedingen geen grote verschillen zijn gevonden tussen de verschillende categorieën van zaken, zullen traditionele georganiseerde criminaliteit en georganiseerde cybercriminaliteit in één paragraaf (en dus niet in aparte subparagrafen) worden besproken.

In de tweede monitorrapportage werd beschreven dat vragen naar (besteding van) criminele verdiensten tot de moeilijkste onderzoeksvragen op het terrein van de georganiseerde criminaliteit behoren, omdat een goed zicht op de financiële positie van daders vaak ontbreekt (Kleemans et al., 2002, p. 124). Ook in de dertig meest recente zaken van Monitor Georganiseerde Criminaliteit is lang niet altijd (volledig) zicht op de criminele verdiensten. Dit kan enerzijds het gevolg zijn van succesvolle pogingen van daders om hun verdiensten en vermogen aan het zicht van de opsporing te onttrekken. Een mogelijk voorbeeld hiervan vinden we in een drugszaak die maar weinig zicht geeft op de geldstromen (casus 164). De desbetreffende zaaksofficier vermoedt dat veel criminele verdiensten naar het land van herkomst van de daders zijn gestroomd. Anderzijds is er in sommige zaken informatie die erop kan wijzen dat daders simpelweg (nog) weinig verdiensten of vermogen hebben gegenereerd. Daarnaast zijn er verschillende zaken waarbij het duidelijk is dat de daders op zijn minst op enig moment veel geld onder zich hebben gehad, maar waarbij het onduidelijk blijft wat de daders zelf hebben verdiend en/of waar het (grootste deel van het) geld is gebleven. Zo ontstaat er in een onderzoek naar een groepering die wordt verdacht van het faciliteren van moorden in het criminele milieu maar weinig zicht op concrete geldstromen (casus 165). Er worden ook

[47] Soudijn constateert verder dat sommige facilitators die zich met virtuele witwastrajecten bezighouden ook met contante geldsmokkel in verband zijn te brengen (Soudijn, 2017). Overigens kunnen criminelen ook reguliere bitcoin exchangers gebruiken, waarbij de mogelijkheden voor afscherming echter doorgaans minder groot zijn.

relatief weinig vermogensbestanddelen aangetroffen. De goederen die wel in beslag zijn genomen, tonen echter aan dat er wel degelijk omvangrijke geldstromen zijn te relateren aan de daders. Zo wordt er een boekhouding gevonden waarin inkomsten uit drugshandel en uitgaven waren bijgehouden, opgeteld bijna 20 miljoen euro, is er een opslagplaats aangetroffen met vele tientallen (automatische) wapens en zijn er bij een enkel persoon tientallen zogenoemde PGP-telefoons in beslag genomen. Verder is van belang hier op te merken dat in verschillende zaken het (financieel) onderzoek nog niet volledig was afgerond op het moment dat de zaak in het kader van de Monitor Georganiseerde Criminaliteit werd bestudeerd.
Zaken waarin op het moment van bestuderen wel berekeningen waren gemaakt van de criminele verdiensten van een samenwerkingsverband, beslaan een grote bandbreedte; van een ton of enkele tonnen tot (vele) miljoenen. De door ons bestudeerde zaken op het terrein van cybercriminaliteit laten op dit punt geen opvallende verschillen zien. Zo werden de verdiensten van een dadergroepering die zich bezighield met phishing voorlopig berekend op meer dan twee miljoen euro (casus 156). Voor de dadergroepering die skimmingoperaties uitvoerde wordt op basis van informatie van een Nederlandse bank de criminele omzet op meer dan miljoen euro berekend (casus 154). Bij een crimineel samenwerkingsverband dat computers en mobiele telefoons met malware besmette om banktransacties te manipuleren lag het op ongeveer € 500.000 (casus 153). Overigens hebben verschillende cybercrimezaken vanuit het perspectief van de opsporing het voordeel dat hierbij het reguliere elektronische betalingsverkeer is betrokken, waardoor er een relatief toegankelijke informatiebron voorhanden is voor het afleiden van de criminele verdiensten. Zo kan er bij daders die zich bezighouden met phishing- of banking-malware-aanvallen worden afgegaan op frauduleuze banktransacties vanaf de rekeningen van slachtoffers en de daarop volgende opnames of overboekingen.

Verdeling van criminele verdiensten
Over de verdeling van criminele verdiensten binnen een crimineel samenwerkingsverband is maar voor een deel van de dertig zaken iets bekend en die informatie is zelden of nooit eenduidig en volledig. Toch besteden we er hier aandacht aan omdat de verdeling van de criminele verdiensten iets zegt over de verhoudingen binnen een crimineel samenwerkingsverband en over het relatieve belang van verschillende onderdelen van het criminele bedrijfsproces. We richten ons hier vooral op zaken met een ICT-component waarin informatie aanwezig is over de verdeling van misdaadgeld (voor een uitgebreide analyse van verdeling in andere zaken: Kruisbergen et al., 2012, p. 161-176).
In de casus die zich richt op de online handel in drugs en wapens via een darknet market (152) zien we een moderator/administrator die verklaart dat hij van de eigenaar van de ondergrondse marktplaats in de laatste drie maanden dat de marktplaats actief was, een vergoeding in bitcoins kreeg waarvan de totale waarde destijds op ruim een halve ton in euro's lag. In casus 154 en 153 is wat meer bekend over de winstverdeling tussen verschillende daders. Interessant is dat in beide casussen technische expertise door de kernleden wordt ingekocht tegen betaling van een fors deel van de totale opbrengst. In casus 154 houdt een dadergroepering zich bezig met het manipuleren van kaartlezers van een grote Nederlandse bank die worden gebruikt voor het inloggen bij het internetbankieren (skimmen). Interessant in deze casus is dat de kernleden, die via familie- en vriendschapsrelaties aan elkaar zijn verbonden en deels uit dezelfde streek in Roemenië afkomstig zijn, voor de technische uitvoering van hun criminele operaties volledig afhankelijk zijn van een facilitator die voor verschillende criminele groepen werkt en software voor skimapparatuur maakt en een database met geskimde gegevens beheert. De kernleden zelf sturen in feite vooral de uitvoerenden aan. De exclusiviteit van de diensten van

de facilitator blijkt uit het aandeel van de winst dat hij opstrijkt, dat op 50% zou liggen volgens het opsporingsdossier. Hoofdverdachte B is degene die namens de kernleden contact onderhoudt met de facilitator en krijgt 20%. De andere kernleden en de uitvoerenden krijgen lagere percentages.
In de casus (153) waarin daders computers en mobiele telefoons met malware besmetten om banktransacties te manipuleren, wordt er in onderschepte communicatie tussen de daders ingegaan op de verdeling van inkomsten. Ook is er binnen het opsporingsonderzoek vanuit het Team Criminele Inlichtingen (TCI) informatie over de verdeling binnengekomen. Hoofdverdachte A in deze casus stuurt de banking-malwareoperaties (samen met een andere hoofdverdachte) grotendeels aan. A bespreekt met andere verdachten de ontwikkeling en distributie van de malware en draagt zorg voor de vertaling van buitenlandse teksten die in de malware gebruikt kunnen worden. Enerzijds werkt hij samen met andere, Nederlandse daders met wie hij samen de kern van het samenwerkingsverband vormt en die elkaar kennen vanuit sociale, offline contacten. Daarnaast werkt A onder meer samen met onbekend gebleven, vermoedelijk buitenlandse personen, bijvoorbeeld om bepaalde technische faciliteiten te verkrijgen. Ook hier zien we dat het belang van ingekochte technische kennis en instrumenten tot uitdrukking komt in het aandeel van de opbrengst. In onderstaande communicatie bespreekt A de winstverdeling met een leverancier (NN) van een botnet.

A: 'We understand each other? So later no problems?'
NN X: 'YES!!'.
A: '35% you, 15% … (Name), 50% I share with my man and people. OK'
(Casus 153)

Met een andere buitenlandse partner (NN Y) bespreekt A andere percentages.

NN Y: 'If we divide our profit like this: 40% your, 40% mine, 10% coder, 10% traffer'.
A: 'Yes, it's good'.
NN Y: 'OK'.
(Casus 153)[48]

Gemaakte afspraken over verdeling van opbrengsten worden zeker niet altijd nagekomen. Individuele daders kunnen hun aandeel in de winst vergroten, onder andere door mededaders te bedriegen. Dat gebeurt in drugszaken, zo zagen we eerder (Kruisbergen et al., 2012, p. 174-176), en we zien hetzelfde gedrag in enkele van de voor de vijfde ronde onderzochte zaken op het terrein van cybercriminaliteit. Zo komt in het onderzoek naar een crimineel samenwerkingsverband dat zich bezighoudt met phishingaanvallen naar voren dat personen die zijn geronseld om bepaalde diensten te verlenen, zoals bankmedewerkers of money mules, vergoedingen worden aangeboden die zij uiteindelijk lang niet altijd krijgen (casus 156). Ook in de zojuist aangehaalde casus die zich richt op banking malware (casus 153) wordt het eigen aandeel in de winst vergroot door mededaders hun aandeel te onthouden. Uit communicatie tussen hoofdverdachten A en B blijkt dat zij regelmatig partners benadelen, bijvoorbeeld door hen voor te houden dat transacties niet gelukt zijn of dat een bankrekening is leeggehaald door een derde.

[48] Zoals ook al uit bovenstaande gesprekken blijkt, geven de verschillende bronnen in deze casus geen eenduidig beeld van de verdeling. De verdachten zelf willen tijdens hun verhoren bovendien niets verklaren over de winstverdeling.

Besteding van criminele verdiensten
Wat doen daders met hun geld? Net als in eerdere publicaties maken we bij de uitgaven van daders een onderscheid tussen consumptie en investeringen (Kleemans, et al., 2002, p. 124-136; Kruisbergen et al., 2012, p. 176-183). Ook in deze ronde zien we in verschillende zaken voorbeelden van daders die er een uitbundig(e) levensstijl en navenant uitgavenpatroon op nahouden. Zo zien we bij een dadergroepering die zich bezighoudt met internationale drugstransporten dat er veel over de wereld wordt gereisd met eerste klas-vliegtickets, wordt verbleven in luxe hotels en dure evenementen worden bezocht (casus 167). In een zaak die zich richt op drugshandel en corruptie zien we een hoofdverdachte die, naast onroerend goed, dure auto's, twee boten en tientallen horloges van exclusieve merken bezit en tevens tienduizenden euro's besteedt aan business seats bij een voetbalclub (casus 163).
Maar er zijn ook daders bij wie er weinig of geen opvallende uitgavenposten worden vastgesteld. Sommige daders lijken zelfs moeite te hebben om rond te komen. Dit valt bijvoorbeeld uit afgeluisterde gesprekken af te leiden voor twee verdachten in een vrij omvangrijke drugszaak (casus 175).
De beschikbare informatie voor de zeven zaken van cybercrime of traditionele georganiseerde criminaliteit met een vernieuwende ICT-component, laten voor het consumptiepatroon grofweg hetzelfde patroon zien als de 23 zaken van traditionele georganiseerde criminaliteit. Enerzijds zijn er zaken waarin maar weinig bekend is over bijzondere bestedingen. Anderzijds staan daar zaken tegenover waarin daders uitbundig van hun inkomsten lijken te genieten.

> *Het criminele samenwerkingsverband houdt zich bezig met het omwisselen van bitcoins voor euro's, waarschijnlijk ten dienste van personen die als drugshandelaar actief zijn op een darknet market. Bij verdachte A worden verschillende auto's in beslag genomen. Voor verdachte C is er informatie die erop wijst dat hij in vier maanden tijd twee auto's van het merk Mercedes koopt. Verder boekt hij twee helikoptervluchten, huurt hij voor duizenden euro's een Maserati en geeft hij een Gucci horloge en duizenden euro's voor gebitsherstel aan zijn vriendin.* (Casus 173)

In de casus waarin daders bankkaartlezers manipuleren die worden gebruikt voor het inloggen bij het internetbankieren (skimmen), zien we dat daders geld uitgeven aan prostitutie, drugs en een nieuwe BMW (casus 154). In een van de casussen die zich op banking malware richt wordt gezien dat meer dan twee ton wordt uitgegeven aan boten (casus 155). Dure auto's zien we ook bij een netwerk dat zich bezighoudt met phishing.

> *De daders binnen dit criminele samenwerkingsverband houden zich bezig met phishingaanvallen op klanten van Nederlandse banken. De hoofdverdachten komen uit dezelfde buurt en zijn al lange tijd actief in het criminele circuit. Op de geldstromen in deze zaak bestaat maar beperkt zicht. Wel blijken de daders een dure levensstijl te hebben. Ze rijden in dure auto's en geven veel geld uit in het uitgaanscircuit. Er zijn aanwijzingen dat een deel van de criminele verdiensten is geïnvesteerd in drugshandel. Verder is er mogelijk sprake van investeringen in vastgoed in Suriname, het land waar verschillende verdachten hun wortels hebben liggen. Daarnaast is vermoedelijk geld geïnvesteerd in een eethuisje, dat op naam staat van een familielid van een van de hoofdverdachten.* (Casus 156)

In bovenstaand casusfragment komen verschillende soorten bestedingen samen. Naast een uitbundig consumptiepatroon gebruiken de daders hun geld voor investe-

ringen, zoals investeringen in criminele activiteiten (drugshandel). Wanneer er na consumptie, levensonderhoud en het continueren of opzetten van nieuwe criminele activiteiten geld overblijft, kan dat worden geïnvesteerd in de reguliere economie, waarvan het bovenstaande fragment ook voorbeelden bevat.
Voor de dertig zaken uit de vijfde ronde van de monitor is er gekeken naar bezittingen in de legale economie die aan daders zijn te relateren. Daarbij gaat het concreet om (gedeeltelijk) bezit van bedrijven en onroerend goed (al dan niet afgeschermd door bijvoorbeeld het gebruik van katvangers). De analyses zijn gebaseerd op de aanwezige informatie in opsporingsdossiers over investeringen en bezittingen. Daarbij zijn niet alleen de inbeslagnames meegenomen maar ook informatie afkomstig uit andere bronnen, zoals bijvoorbeeld verhoren, observaties en undercoveroperaties.[49]

Zoals in paragraaf 4.1 is besproken, zijn eerder voor de 150 zaken uit de eerste vier rondes van de Monitor Georganiseerde Criminaliteit uitgebreide analyses gemaakt van investeringen (bezittingen) van daders in de legale economie. Wanneer we naar de aard, omvang, plaats en het gebruik van de bezittingen in de legale economie kijken, zien we in het grootste deel van de dertig nieuwste zaken op hoofdlijnen hetzelfde patroon als bij die eerdere analyses (Kruisbergen et al., 2012, 2015a, 2015b). Een enkele zaak laat een ander beeld zien. Dit laatste geldt voor casus 168, die zich richt op witwasactiviteiten (volledig offline) van een dader met sporen in de drugshandel. Onder meer de omvang van zijn vermogen, tientallen miljoenen, en het sterke internationale karakter van zijn investeringsportfolio geven deze zaak een ander aanzien dan de meeste andere zaken. Omdat ICT in deze zaak (in relatie tot witwassen) geen rol lijkt te spelen, gaan we er op deze plaats niet verder op in.
Het overgrote deel van de andere zaken laat over het algemeen het eerder beschreven patroon zien: het investeringspatroon lijkt vrij conservatief waarbij de fysieke en/of sociale afstand tussen een dader en zijn bezittingen vaak klein is. Daders investeren veel in het land waarin ze wonen en/of het land waar ze via een migratieachtergrond (van hun ouders) mee verbonden zijn. Daarnaast investeren ze vooral in tastbare, 'bekende' vermogensbestanddelen, dat wil zeggen huizen en ander onroerend goed en bedrijven uit sectoren als groot-/detailhandel, horeca en transport. Ten slotte worden hun bedrijven vaak gebruikt ter ondersteuning van de criminele activiteiten. Minder tastbare, puur financiële bezittingen, zoals obligaties, opties en aandelen in bedrijven waarin daders níet persoonlijk betrokken zijn (bijvoorbeeld in beursgenoteerde bedrijven), lijken veel minder vaak voor te komen.
We maken hierbij de kanttekening dat deze analyses, net als alle andere in dit rapport, zijn gebaseerd op informatie uit opsporingsdossiers. Het gebruik van opsporingsdossiers draagt het risico in zich dat bepaalde resultaten verborgen blijven, niet omdat de feiten er niet zijn maar simpelweg omdat de politie ze niet kon vinden.[50]
We richten ons nu vooral op de zeven zaken met een sterke ICT-component (cybercrime of traditionele georganiseerde criminaliteit waarin ICT een vernieuwend element inbrengt). In casus 151 zien we daders die voor het logistieke aspect van hun drugssmokkel gebruikmaken van een vernieuwende modus operandi: ze breken in op het computernetwerk van een haventerminal om de afhandeling van binnenkomende containers te manipuleren. Wanneer we naar de bezittingen van deze daders in de legale economie kijken, zien we dat ze deze 'moderne' handelswijze

[49] Meestal is onbekend of de bezittingen zijn verkregen met criminele verdiensten.

[50] Verder concentreren we ons op het feitelijk bezit van bijvoorbeeld onroerend goed en niet op formeel eigendom. Daarnaast hebben we wat betreft investeringen het aanhouden van contant geld en spaartegoeden niet meegenomen in onze analyses (zie Kruisbergen, 2017, p. 84-85, 180-181).

combineren met een traditionele: het gebruik van eigen bedrijven of bedrijven van relaties voor logistieke of legitimeringsdoeleinden. Het gaat dan bijvoorbeeld om groothandels- en/of import- en exportbedrijven die fungeren als verzender of ontvanger van een container en soms ook de deklading verzorgen, bijvoorbeeld fruit. Overigens is voor tenminste één bedrijf bekend dat dit nauwelijks reguliere economische activiteiten onderneemt.
Ook in de zaak van de bitcoinwisselaars ligt er informatie die wijst op gebruik van eigen bedrijven voor de uitvoering of ondersteuning van de criminele activiteiten. Ook biedt de zaak informatie over investeringen in onroerend goed.

> *Aantekeningen in een aangetroffen notitieblok lijken erop te wijzen dat verdachte C in totaal meer dan anderhalve ton besteedt aan een appartement in het land waar zijn familiewortels liggen, de inrichting van een woning in een Nederlandse stad en een investering in een onderneming. Voor verdachte K is uit tapgesprekken op te maken dat hij vermoedelijk een auto en een stuk grond bezit in een Zuid-Amerikaans land (waar hij is geboren). Verdachte M bezit een woning in een Zuid-Europees land. Verschillende verdachten hebben ten slotte een bedrijf. Zo hebben verdachte A en C bedrijfjes die vooral voor witwasdoeleinden lijken te worden gebruikt; ze gebruiken de bankrekeningen van de bedrijven voor het ontvangen, overboeken en opnemen van gelden uit de handel in bitcoins.* (Casus 173)

Ook in de casus waarin daders skimmingoperaties uitvoeren hebben verschillende verdachten bedrijfjes die worden gebruikt ten behoeven van het criminele samenwerkingsverband. Dit geldt onder meer voor verdachte E.

> *Verdachte E heeft een technische opleiding op HBO-niveau gevolgd en beschikt over expertise op het terrein van ICT. Ook heeft hij een eigen elektronicabedrijf. E was al actief met dit bedrijf voordat hij betrokken raakte bij de skimmingoperaties die de dadergroepering uitvoert. Eenmaal betrokken bij het criminele samenwerkingsverband, gebruikt E echter zijn bedrijf om de skimmingactiviteiten te ondersteunen, door de levering van telefoons, simkaarten en chips.* (Casus 154)

De zeven zaken van georganiseerde criminaliteit met een duidelijke ICT-component laten al met al geen grote verschillen zijn met de andere zaken. Een verschil is mogelijk het type bedrijf waaraan verdachten zijn te relateren. Behalve in de zojuist aangehaalde casus (154) zien we hier ook een voorbeeld van in casus 155, die zich richt op daders van banking malware. In die zaak is een hoofdverdachte betrokken bij een bitcoin exchange service (waarbinnen overigens weinig activiteiten lijken te hebben plaatsgevonden). Gezien de cybercriminele activiteiten van deze dader, ligt een dergelijk bedrijf echter duidelijk in zijn werk- en levenssfeer, waarmee de zaak goed past in het eerder beschreven patroon in de bezittingen van de algehele daderpopulatie binnen onze zaken.

4.4 Analyse van bestudeerde zaken: afscherming van criminele verdiensten

In deze paragraaf gaan we na hoe de verschillende criminele samenwerkingsverbanden omgaan met de afscherming van hun verdiensten. We maken hierbij onderscheid tussen traditionele georganiseerde criminaliteit (casus 157-172, 174-180), traditionele georganiseerde criminaliteit waarbij het gebruik van ICT een belangrijk vernieuwend element is (casus 151, 152 en 173), georganiseerde low-tech cyber-

criminaliteit (casus 154 en 156) en georganiseerde high-tech cybercriminaliteit (casus 153 en 155). Ook gaan we in een aparte subparagraaf in op een rode draad die wat betreft criminele geldstromen door alle, zowel traditionele als ICT-gerelateerde, zaken heen loopt: het grote belang van contant geld.

Traditionele georganiseerde criminaliteit
In de 23 zaken van traditionele georganiseerde criminaliteit uit de vijfde monitorronde zien we een brede variatie in werkwijzen waarmee daders hun criminele inkomsten proberen af te schermen, zoals dat ook naar voren kwam in de analyses die bij de vierde ronde zijn gemaakt. Bij een aantal van deze werkwijzen is geen sprake van het doorlopen van de drie fasen – plaatsing, versluiering en integratie – die zo vaak in de literatuur worden beschreven. Het gaat om hele eenvoudige en vaak voorkomende werkwijzen om criminele geldstromen af te schermen: het verstoppen, verplaatsen of het afgeschermd consumeren van veelal contant geld. Deze basale vormen bespreken we als eerste. Vervolgens gaan we kort in op meer complexe witwasconstructies. Ten slotte bespreken we of en zo ja hoe in de 23 zaken van traditionele georganiseerde criminaliteit gebruik is gemaakt van zogenoemde *new payment methods*. Het blijkt dat de 23 zaken al met al geen grote verschillen laten zien ten aanzien van de analyses die in de vierde monitorrapportages zijn gedaan.
Veel traditionele, dat wil zeggen, offline uitgevoerde vormen van georganiseerde criminaliteit genereren contant geld. De meest eenvoudige manier om criminele inkomsten af te schermen is dit contante geld te *verbergen*. Dit zien we in verschillende zaken, waarbij de inbeslagname van contanten varieert van enkele duizenden (casus 174) tot bijna zes miljoen euro (casus 171).

> *Het criminele samenwerkingsverband houdt zich bezig met hennepteelt. Bij doorzoekingen op verschillende plaatsen wordt grofweg 1,2 miljoen euro aan contant geld gevonden, verborgen in onder meer een tuin (begraven), schuur, een pilaar, in een waterput en in een kluis van een bank.* (Casus 169)

Daders kunnen om verschillende redenen hun geld *verplaatsen*, bijvoorbeeld omdat ze denken dat het toezicht op geldstromen in een ander land minder scherp is en/of omdat ze een bepaalde band hebben met een ander land, bijvoorbeeld het land van herkomst. Geld kan enerzijds worden overgeboekt via reguliere kanalen, met name via money transferinstellingen (bijvoorbeeld casus 159 en 176). Anderzijds gebruiken daders ondergrondse kanalen voor internationaal financieel verkeer. Zo kan het geld worden 'overgemaakt' via ondergronds bankieren of fysiek de grens over worden gesmokkeld. Beide vormen komen in verschillende zaken voor. In verschillende zaken zien we dat geld vanuit Nederland naar een ander land wordt vervoerd of overgemaakt, waarbij het land van bestemming bijvoorbeeld het land van herkomst is van de opdrachtgever van de geldtransactie. Er zijn echter ook zaken waarin daders dergelijke financiële dienstverlening gebruiken om geld te ontvangen, bijvoorbeeld betalingen in relatie tot verzorgde drugstransporten (casus 161).

Behalve verplaatst kunnen criminele verdiensten ook simpelweg in Nederland worden geconsumeerd. Zeker bij grotere bedragen die contant worden afgerekend bestaat echter het risico dat aanbieders van goederen en diensten vragen gaan stellen, een melding doen van een ongebruikelijke transactie bij de FIU-Nederland (Financial Intelligence Unit) of de contante betaling weigeren. Om *afgeschermde consumptie* mogelijk te maken kan een dader gebruikmaken van een katvanger die bijvoorbeeld een auto op zijn of haar naam laat zetten. Ook kan een dader gebruikmaken van bijvoorbeeld de creditcard van een katvanger. Daarnaast wordt afge-

schermde consumptie mogelijk gemaakt door aanbieders van goederen en diensten bij wie grote bedragen zonder problemen contant kunnen worden afgerekend. Ook in deze ronde zien we in verschillende zaken daders die hun verdiensten op deze wijze consumeren. In casus 161, waarin daders actief zijn op het terrein van verschillende soorten drugsproductie/-handel, zien we onder andere een hoofdverdachte die de huur van € 20.000 voor een Nederlands huis contant betaalt. Verder betaalt hij meer dan € 20.000 contant voor de aankoop van een Mercedes, rekent hij vele duizenden euro's contant af voor de aanschaf van scooters en een waterscooter en boekt hij een vakantiereis waarvan de prijs, bijna € 9.000, door een relatie contant wordt voldaan. En zo zijn er meer voorbeelden te geven.

Verder zien we in de 23 zaken van traditionele georganiseerde criminaliteit uit de vijfde monitorronde verschillende van de vaak wat *meer complexe constructies* om criminele inkomsten af te schermen of van een legaal voorkomen te voorzien. Zo zien we in veel zaken dat een inkomen uit een reguliere dienstbetrekking of winst uit een legaal bedrijf of handel wordt gefingeerd. Daarbij wordt dan gebruikgemaakt van legale (dekmantel)bedrijven van de dader zelf of een relatie (bijvoorbeeld casus 161 en 163, 164, 167, 168, 170, 171, 172, 175, 176, 177 en 179). Een mogelijke loan-backconstructie in verband met onroerend goed zien we bijvoorbeeld in casus 170. Ook het doorsluizen van geld via (een serie van) overboekingen van/naar buitenlandse rechtspersonen komt in verschillende zaken terug, zoals in casus 163, 168 en 170 waarbij daders (onder andere) rekeningen van rechtspersonen gevestigd in de Verenigde Arabische Emiraten gebruiken, en in casus 180 waarin bedrijfsrekeningen worden gebruikt uit China, de Verenigde Staten, Luxemburg, Frankrijk en andere Europese landen.
Bij deze vormen van witwassen komt, in tegenstelling tot wanneer daders hun geld bijvoorbeeld verstoppen, de verwevenheid tussen daders en de reguliere economie duidelijk naar voren. Die verwevenheid zien we ook wanneer we kijken naar de dienstverleners waarvan gebruik wordt gemaakt. Zo zien we (vermoedens van) het gebruik van onder andere een derdengeldrekening van een advocaat (casus 158), een financieel adviesbureau (casus 163), een dienstverlener op het gebied van trustdiensten (casus 168), een juridisch adviseur (casus 170) en een boekhouder (casus 172).

Behalve de hierboven besproken 'traditionele' manieren die daders gebruiken om hun criminele verdiensten af te schermen, kunnen zij ook gebruikmaken van door ICT mogelijk gemaakte *new payment methods*, zoals bitcoins en prepaidkaarten. Een cryptomunteenheid als bitcoin is in beginsel niet alleen van belang voor daders die zich met cybercrime of ICT-gerelateerde misdrijven bezighouden. Een dader zou de aanschaf van bitcoins bijvoorbeeld kunnen gebruiken in een constructie om zijn geldstromen af te schermen of als investering waarbij wordt gespeculeerd op koersstijging. In de 23 zaken van traditionele georganiseerde criminaliteit zien we echter nergens het gebruik van bitcoins of andere cryptomunteenheden. Daarbij tekenen we aan dat een deel van deze opsporingsonderzoeken liep in een periode waarin bitcoin niet bij een groter publiek bekend was (het jaar waarin in deze onderzoeken aanhoudingen werden verricht varieert van 2009 (één zaak) tot 2016). Overigens werden ook andere, iets oudere vormen van innovatieve, digitale financiële dienstverlening, zoals Liberty reserve en e-gold, in deze zaken niet gezien. Mogelijke redenen waarom in deze zaken nergens het gebruik van bitcoins werd gesignaleerd: daders hebben bitcoins of andere cryptomunteenheden simpelweg niet nodig; de nadelen die aan bitcoins zijn verbonden werpen een drempel op (begrensde anonimiteit, grote koersschommelingen, geringe bestedingsmogelijkheid in de offline wereld en het risico van diefstal of 'kwijtraken'); virtuele valuta staan te ver af van

de belevingswereld van veel daders (vergelijk de uitkomsten wat betreft de bezittingen van daders in de reguliere economie); de politie wist dit niet op te sporen. Wel wordt in één van de zaken geconstateerd dat daders gebruikmaken van prepaidkaarten.

> *Het criminele samenwerkingsverband wordt verdacht van het faciliteren van moorden in het criminele milieu. Binnen de dadergroepering wordt gebruikgemaakt van cash passports. Dit zijn prepaid creditcards waarmee, na storting van een geldbedrag, betaald en geld opgenomen kan worden. Er waren kaarten afgegeven aan verdachten A en H. Ook waren er onbekenden op wiens naam kaarten stonden. De bedragen kwamen niet boven de € 5.000 uit.* (Casus 165)

Traditionele georganiseerde criminaliteit met cybercomponent
Een belangrijk verschil tussen veel zaken op het terrein van traditionele georganiseerde criminaliteit enerzijds en cyberzaken (breed opgevat) anderzijds betreft de primaire geldstroom. Delicten die onder traditionele georganiseerde criminaliteit vallen genereren vaak fysiek, dat wil zeggen contant geld. Dit geldt bijvoorbeeld voor offline drugshandel en mensenhandel in de seksindustrie.[51] Zaken met een belangrijke cybercomponent genereren juist vaak digitale valuta. In deze vijfde ronde van de monitor scharen we zoals gezegd drie zaken onder de noemer 'traditionele georganiseerde criminaliteit met cybercomponent'. In één van die zaken bestaat de primaire geldstroom uit contant geld. Dit is de zaak (casus 151) waarin daders hackers inzetten om containers met daarin een partij drugs ongehinderd de haven uit te krijgen. In casus 152 draait het om online drugs- en wapenhandel via een darknet market. Hier is (een deel van) de primaire geldstroom wel digitaal; online afgesloten drugstransacties worden betaald met bitcoins.

> *Het criminele samenwerkingsverband is betrokken bij het opzetten en beheren van een marktplaats op het darknet. Op deze marktplaats worden drugs en wapens verhandeld. Wanneer koper en verkoper tot overeenkomst waren gekomen, stort de koper een bedrag in bitcoins op een bitcoin wallet van de beheerder. Die beheerder verleent een zogenoemde escrow service, dat wil zeggen dat hij als tussenpersoon fungeert tussen de kopende en verkopende partij en de betaalde bitcoins doorboekt naar een wallet van de verkoper zodra de koper meldt dat hij de bestelde waar heeft ontvangen. A is een van de moderators van de marktplaats. Ook handelt A zelf in drugs. Bij doorzoekingen wordt beslag gelegd op honderden bitcoins, ter waarde van grofweg een half miljoen euro.* (Casus 152)

In het dossier wordt gemeld dat deze A contacten heeft waar hij bitcoins kan omwisselen in fysieke euro's. A gaf er blijkbaar de voorkeur aan in ieder geval een deel van zijn verdiensten in euro's aan te houden. Het omwisselen gebeurde bij individuele bitcoinwisselaars waarmee op openbare plekken werd afgesproken. Er zijn ook verschillende, gemakkelijk toegankelijke online *bitcoin exchanges* maar wisseltransacties verlopen daar vaak via herleidbare kanalen. Dergelijke wisseltransacties brengen voor drugshandelaren die hun bitcoins willen omruilen voor euro's natuurlijk risico's met zich mee. Er is dan ook behoefte aan financiële dienstverleners die een grotere mate van anonimiteit bieden. De eerder aangehaalde casus 173 richt zich op professionele facilitators die daarin voorzien.

---

[51] Verschillende vormen van bijvoorbeeld fraude genereren juist digitaal geld. Denk hierbij aan BTW-fraude, beleggingsfraude of aan zaken waarin met vastgoedtransacties wordt gefraudeerd.

De hoofdverdachten houden zich bezig met het opkopen van bitcoins, dat wil zeggen dat ze tegen betaling van een commissie aangeleverde bitcoins omwisselen voor contante euro's. Het vermoeden bestaat dat in ieder geval een deel van de door hen opgekochte bitcoins afkomstig is van handel in onder meer drugs op het zogenoemde dark web. Zo zijn bij klanten van de bitcoinwisselaars drugs aangetroffen en voorwerpen die in verband staan met verzending van drugs. Ook is een bitcoin wallet van een klant te relateren aan online drugshandel. Een andere belangrijke aanwijzing voor de criminele herkomst van de bitcoins is de prijs die de klanten moeten betalen voor het omwisselen van hun cryptovaluta, bijvoorbeeld 7 %, een veel hogere prijs dan die reguliere, online bitcoin exchangers rekenen.
De bitcoinwisselaars ontmoeten hun klanten met name in lokale vestigingen van hamburger- of koffieketens (met wifi). Deze ontmoetingen vonden vooral plaats in Nederland en in nabijgelegen landen. Nadat een klant zijn bitcoins heeft overgemaakt naar een door de wisselaar gecontroleerde bitcoin wallet, ontvangt de klant contant geld. Met het opkopen en omwisselen van uit criminaliteit afkomstige bitcoins maken de wisselaars zich schuldig aan witwassen. De grote hoeveelheid bitcoins die zij op deze wijze verkrijgen, creëert voor henzelf echter ook een omwissel- en witwasprobleem. Een deel van de aangekochte bitcoins wordt omgewisseld voor euro's bij reguliere bitcoin exchangers als Kraken en Bitonic. Laatstgenoemden storten de euro's op bankrekeningen die onder controle staan van de hoofdverdachten. Dit geld wordt weer contant opgenomen en gebruikt voor de aankoop van bitcoins. In totaal wordt voor miljoenen euro's op de bankrekeningen bijgeschreven / opgenomen. Om de opgekochte bitcoins om te wisselen en wit te wassen, lijkt verder (onder andere) gebruik te worden gemaakt van de goudhandel. Met aangekochte bitcoins wordt goud ingekocht. Vervolgens wordt het goud bij een andere goudhandelaar met verlies tegen contante betaling verkocht. (Casus 173)

De bitcoinwisselaars in deze casus maken voor hun transacties met klanten dus gebruik van lokale voorzieningen, zoals een vestiging van een hamburgerketen met wifi. Ze kennen daarmee een zekere lokale inbedding én begrenzing. De geografische actieradius van hun transacties is dan ook niet onbeperkt; de meeste klanten waren afkomstig uit Nederland of nabijgelegen landen.
Deze bitcoinwisselaars profiteren dus van de behoefte aan contant geld onder online drugshandelaren. We zien dat ook zij op hun beurt een deel van hun virtuele munten omwisselen in contante euro's (om opnieuw bitcoins te kunnen omwisselen). In deze zaak wordt dan ook op verschillende plaatsen ongeveer € 200.000 aan contanten in beslag genomen.
De belangrijke rol die een cryptomunteenheid als bitcoin speelt op darknet markets, de uiteindelijke voorkeur van een deel van de handelaren op die ondergrondse markten voor fysieke euro's, en de rol en werkwijze van een bitcoinwisselaar, zijn wat betreft witwassen de belangrijkste specifieke inzichten die de drie zaken van traditionele georganiseerde criminaliteit met een cybercomponent bieden (casus 151, 152 en 173). Enkele van de 'klassieke' manieren om criminele geldstromen af te schermen zien we echter ook in deze drie zaken. Zo zien we in de zaak van het drugssmokkelnetwerk dat hackers gebruikt (casus 151) dat een verdachte huishoudelijke elektronica van grofweg € 3.000 contant betaalt met € 500-biljetten (in dezelfde zaak maken daders overigens ook gebruik van money transfers en ondergronds bankieren en wordt ongeveer anderhalve ton aan contant geld in beslag genomen). Een andere vorm van afgeschermde consumptie zien we in de casus (173) betreffende de bitcoinwisselaars. Daar zien we dat een verdachte in korte tijd twee luxe auto's koopt en die op naam van een familielid laat zetten. Een andere

verdachte doet iets soortgelijks. In dezelfde zaak komt ook een wat meer complexe witwasconstructie voor, waarbij een legaal inkomen uit handelsactiviteiten wordt gefingeerd. Dit zagen we in het zojuist weergegeven casusfragment, waarin een bitcoinwisselaar de goudhandel gebruikte om de schijn van een legaal inkomen te creëren.

Georganiseerde cybercriminaliteit: low-tech

Eén van twee zaken die we scharen onder georganiseerde low-tech cybercriminaliteit betreft een dadergroepering die kaartlezers van een grote Nederlandse bank manipuleert om gegevens van rekeninghouders af te lezen (skimmen, casus 154). Vervolgens wordt met zelfgemaakte betaalpassen door verschillende zogenoemde cashteams in meer dan tien verschillende landen bij geldautomaten geld opgenomen. Het opgenomen geld wordt daarna fysiek vervoerd, maar ook wordt gebruikgemaakt van money transfers (bij een hoofdverdachte wordt ook nog bijna anderhalve ton euro in beslag genomen).

Het contant opnemen van geld speelt ook een centrale rol in de andere zaak van low-tech cybercriminaliteit, casus 156, waarin daders phishingaanvallen uitvoeren. Een belangrijk verschil is echter dat na het skimmen het geld contant wordt opgenomen, direct van de rekening van de slachtoffers, terwijl bij een phishingaanval het geld van de rekening van een slachtoffer eerst via internetbankieren wordt overgeboekt naar een rekening die onder controle staat van de daders, waarbij vaak zogenoemde money mules worden gebruikt. Pas daarna wordt het geld, vanaf de rekening van een money mule, contant opgenomen.

> *De kernleden van het netwerk dat zich bezighoudt met phishingaanvallen op Nederlandse bankrekeninghouders, gebruikt money mules voor het ontvangen van de frauduleus overgemaakte gelden. Nadat het geld van een slachtoffer is gestort op een rekening van een money mule, haalt deze bijvoorbeeld zelf het geld van de rekening of geeft de pas en pincode af aan een ronselaar.* (Casus 156)

Net als bij de casus van online drugshandel (casus 152) en de casus van de bitcoinwisselaars (casus 173) zien we dus dat ook in deze phishingzaak digitale valuta, in dit geval euro's, worden omgewisseld in fysieke, contante euro's. Daarbij wordt gebruikgemaakt van katvangers, zogenoemde money mules, die met het beschikbaar stellen van hun rekening de frauduleuze overboekingen en opnames mede mogelijk maken. Op deze money mules komen we later nog terug.

Het gebruik van bitcoin, vouchers en/of prepaidkaarten of andere, innovatieve financiële dienstverlening zien we niet in de twee zaken van low-tech cybercriminaliteit (casus 154 en 156).[52]

De twee zaken bevatten wat betreft het afschermen van criminele verdiensten informatie over één andere werkwijze, te weten afgeschermde consumptie. Dit zien we bij het netwerk dat zich bezighoudt met phishing.

> *Op de rekening van een familielid van verdachte A wordt contant geld gestort. Die rekening wordt vervolgens gebruikt voor het huren van auto's en een buitenlandse reis. A huurt ook auto's op zijn eigen naam, waarbij hij de huur contant betaalt.* (Casus 156)

[52] Daarbij tekenen we aan dat casus 156 zich afspeelde in een periode dat bitcoin nog maar kort bestond.

Georganiseerde cybercriminaliteit: high-tech
In casus 153 worden door de daders verschillende methoden toegepast om de criminele verdiensten af te schermen.[53]

> *Leden van dit criminele samenwerkingsverband besmetten computers en mobiele telefoons met banking malware om banktransacties te manipuleren. De criminele geldstroom bestaat uit drie hoofdelementen. Ten eerste wordt het geld afkomstig van bankrekeningen van slachtoffers gebruikt om onder meer bitcoins, Webmoney of vouchers aan te kopen. De bitcoins worden (ten dele) omgewisseld voor euro's. Dit verloopt via een individuele bitcoinwisselaar met wie op een online forum contact is gemaakt. Bitcoins worden (bijvoorbeeld) door een hoofdverdachte naar een wallet van de wisselaar overgemaakt. De wisselaar wisselt de bitcoins om voor euro's bij een money transferkantoor, waar ze door een andere verdachte worden opgehaald. Een tweede geldstroom bestaat eruit dat geld van de slachtoffers wordt aangewend voor de online aankoop van goederen zoals computers en telefoons, waarbij een adres van een katvanger als afleveradres wordt gebruikt. De goederen worden vervolgens verkocht of gebruikt door de hoofddaders. Ten derde wordt geld van de rekeningen van slachtoffers overgeboekt naar rekeningen van money mules, waarna het contant wordt opgenomen.* (Casus 153)

In casus 155 (eveneens gericht op banking malware) zien we ook dat (persoonlijke of bedrijfs)rekeningen van money mules worden gebruikt en dat vervolgens wordt *gecashed*. In die zaak wordt bovendien ook meer dan € 300.000 contant geld in beslag genomen. Ook zien we, net als in de zojuist aangehaalde casus 153, dat bitcoins worden aangekocht. Het aankopen van vouchers kwam voor zover bekend alleen voor in casus 153. In deze twee zaken van cybercrime met een sterkere technische component worden dus wel ' nieuwe' betaalmethoden zoals bitcoins, Webmoney en/of vouchers gebruikt. Ten slotte zien we in het aangehaalde casusfragment ook een voorbeeld van een 'online variant' van afgeschermde consumptie; de daders kopen via katvangers online goederen zoals computers en telefoons, die ze vervolgens zelf gebruiken of doorverkopen.

De digitale geldstroom die er in veel ICT-gerelateerde zaken is, brengt behoefte aan en mogelijkheden voor 'nieuwe' soorten van dienstverlening met zich mee. Zo zien we in casus 155 dat daders een zogenoemde bitcoin 'mixing service' gebruiken, om het spoor tussen zend- en ontvangstadres van een bitcoin te verhullen en aldus de identiteit van (in dit geval) de ontvanger te beschermen. Verder vervullen money mule[54] en bitcoinwisselaars (voor zover bitcoins worden omgewisseld) een belangrijke functie voor daders die zich bezighouden met , respectievelijk, fraude met het internetbetalingsverkeer of illegale handel op darknet markets. Aan de hand van casus 173 zijn we al ingegaan op bitcoinwisselaars die als professionele facilitators verschillende klanten bedienen die hun, vermoedelijk met online drugshandel verdiende, cryptovaluta willen inwisselen voor contante euro's. Deze wisselaars gebruikten lokale voorzieningen, zoals vestigingen van hamburger- of koffieketens met wifi, om hun klanten te ontmoeten en transacties te verrichten. De bitcoinwisselaar in het aangehaalde fragment uit casus 153 lijkt op een andere, minder lokaal

[53] Zie ook de publicatie van Oerlemans en anderen voor een beschrijving van de werkwijze in deze zaak (2016, onder andere p. 78-79).

[54] Behalve via money mules kan ook via identiteitsfraude geld van slachtoffers worden doorgesluisd. Dit komt erop neer dat via de persoonlijke gegevens van een derde een betaaldienst wordt afgenomen. Die betaaldienst wordt bijvoorbeeld vervolgens gebruikt om het ontvangen geld van het slachtoffer verder door te sluizen.

gebonden wijze te opereren (waarbij een money transferkantoor als tussenschakel wordt gebruikt). Een andere categorie 'facilitators' vormen de money mules die worden gebruikt voor het overboeken en opnemen van geld. Zij zijn eerder katvangers dan professionele facilitators en opereren in de periferie van criminele netwerken. Bij de bespreking van de literatuur in paragraaf 4.2 zagen we al dat uit onderzoek blijkt dat money mules vooral worden gerekruteerd onder jongvolwassenen uit armere wijken in stedelijke gebieden (Oerlemans et al., 2016; zie ook Mauritz, 2014). In aansluiting hierop komt uit communicatie tussen daders in casus 155 naar voren dat zij money mules vooral zoeken onder gemakkelijk beïnvloedbare personen, die bijvoorbeeld kampen met schulden, psychische problemen of drugsverslaving. In hoofdstuk 2 is voor casus 156 en 155 al beschreven dat money mules vooral worden geronseld in de sociale en lokale nabijheid van de kernleden van de desbetreffende criminele netwerken. In de eigen buurt bijvoorbeeld, bij het uitgaan of via oproepen op de sociale media, worden contacten aangeboord, waarbij de werving via de sneeuwbalmethode zich voor kan zetten.
De werkwijze en de positie van de bitcoinwisselaars en money mules verschillen dus. De bitcoinwisselaars, in ieder geval in de door ons onderzochte zaak, zijn professionele witwassers die hun diensten aanbieden aan verschillende klanten. De money mules daarentegen lijken een meer inwisselbare, ongelijkwaardige positie in te nemen ten opzichte van hun opdrachtgevers; zij worden 'gebruikt'. Toch is er ook een belangrijke overeenkomst tussen de bitcoinwisselaars en money mules: de lokale inbedding.

4.4.1 Het belang van contant geld

Een essentieel kenmerk van criminele geldstromen is de prominente rol van contant geld. Veel criminele activiteiten, zoals drugshandel, genereren contant geld. In veel opsporingsonderzoeken wordt dan ook contant geld aangetroffen (en soms geldtelmachines), niet zelden in grote hoeveelheden. Contant geld stelt daders echter ook voor problemen, problemen die zij oplossen dankzij de directe of indirecte hulp vanuit hun omgeving. Zo wordt, ten eerste, het belang dat contant geld speelt binnen de georganiseerde criminaliteit benut door financiële dienstverleners die zich gespecialiseerd hebben in het (al dan niet fysiek) *verplaatsen of omwisselen van criminele verdiensten*. Deze dienstverleners spelen een cruciale rol in verschillende criminele bedrijfsprocessen. Zij lossen problemen op die bijvoorbeeld drugshandelaren hebben wanneer zij grote hoeveelheden geld genereren, geld dat zij in een andere valuta willen hebben, in andere coupures en/of op een andere plaats.
Het wisselen van reguliere valuta speelde natuurlijk een grote rol voor de komst van de euro, maar is nog steeds voor bepaalde criminele handelsstromen van belang, bijvoorbeeld wanneer transacties plaatvinden met partners in het Verenigd Koninkrijk. Behalve het wisselen van valuta kan ook het wisselen van coupures van groot belang zijn. Het omwisselen van valuta en/of coupures speelt vaak ook een rol bij een andere vorm van financiële dienstverlening waar daders in de georganiseerde criminaliteit gebruik van maken, het ondergronds bankieren, ook bekend als *hawala*. Bij ondergrondse bankiers kunnen daders contant geld afgeven dat, uiteraard tegen een vergoeding, vervolgens in een ander land in een gewenste valuta aan een op te geven begunstigde wordt uitgekeerd (voor een uitgebreide bespreking zie Kruisbergen et al., 2012, p. 195-203; Soudijn, 2015; Van de Bunt & Siegel, 2009). Een ander type dienstverlener heeft zich toegelegd op de fysieke smokkel van contant geld. In Nederlandse opsporingsonderzoeken is dit onder andere bekend van Zuid-Amerikaanse dadergroeperingen. In het voorafgaande zijn al kort twee van dergelijke zaken besproken. In de Nederlandse opsporingspraktijk zijn hier echter veel meer voorbeelden van te geven, zeker sinds de opsporing van ondergrondse

bankiers en contant-geldsmokkel de laatste vijf à tien jaar meer prioriteit heeft gekregen (zie Soudijn & Reuter, 2016). Ten slotte zien we ook in zaken in deze vijfde ronde dat een deel van de daders gebruikmaakt van money transferkantoren. Dat geldt zowel voor zaken van traditionele georganiseerde criminaliteit als cybercrimezaken.[55]
Verder zagen we in onze zaken dat daders van ICT-gerelateerde delicten hun digitale valuta – euro's op een bankrekening in het geval van phishing- of banking-malware-aanvallen en bitcoins in het geval van online drugshandel – vaak willen omwisselen voor fysieke, contante euro's.[56] Dit omwisselen van digitale in fysieke, contante valuta is ook in andere studies vastgesteld (zie bijvoorbeeld Leukfeldt, 2014; Leukfeldt et al., 2017a, 2017b, 2017c; Oerlemans et al., 2016; Europol, 2015a). Voor het omwisselen van digitale in fysieke valuta kunnen daders van verschillende katvangers of facilitators gebruikmaken. In het geval van phishingaanvallen en banking malware kan daarbij gebruik worden gemaakt van money mules, die de op hun rekening gestorte euro's contant (laten) opnemen. Daders die (een deel van) hun bitcoins willen omwisselen voor euro's, zoals drugshandelaren die op een darknet market actief zijn, kunnen terecht bij een bitcoinwisselaar.
De waarde die de genoemde dienstverleners – van ondergrondse bankiers tot bitcoinwisselaars – hebben voor hun criminele clientèle, blijkt ook uit de prijs die klanten bereid zijn te betalen. Informatie hierover is schaars, maar de informatie die er is wijst uit dat die prijs vrij hoog kan zijn. Bij ondergrondse bankiers kunnen percentages van grofweg 9% worden gerekend voor criminele klanten, hoewel er ook voorbeelden zijn van ondergrondse bankiers die lagere provisies rekenen (casus 177, 178; Kruisbergen et al., 2012, p. 172-173; Kleemans et al., 2002, p. 123).[57]
Voor contant-geldsmokkel is door Soudijn en Reuter (2016) een grondige analyse gedaan op basis van zes opsporingsonderzoeken naar Colombiaanse smokkelnetwerken. Deze netwerken zouden vooral grote hoeveelheden contant geld vervoeren ten behoeve van cocaïnehandelaren. Soudijn en Reuter berekenden de totale kosten van deze dienstverlening op 10% à 17%.[58] Bitcoinwisselaars zien we in ons casusmateriaal in casus 153 en 173. Laatstgenoemde casus draait volledig om professionele bitcoinwisselaars. De vergoeding die hun klanten moeten betalen voor het omwisselen van bitcoins in contante euro's lijkt te variëren en ligt bijvoorbeeld op 7%, een stuk hoger dan bij reguliere bitcoin exchangers. In casus 153 wordt gesproken over 8% die daders van banking-malware-aanvallen betalen aan een bitcoinwisselaar.[59]

Naast het verplaatsen en wisselen van criminele verdiensten is het *accepteren van betalingen met contant* geld een tweede soort van 'dienstverlening' waar daders gebruik van maken. Het zonder vragen te stellen accepteren van betalingen van

---

[55] Oerlemans en anderen zagen in de literatuur, gerechtelijke uitspraken en opsporingsdossiers dat daders van banking malware vaak gebruikmaken van money transferkantoren (Oerlemans et al., 2016, p. 74, 104).

[56] In een aantal bestudeerde cyberzaken werd een grote hoeveelheid contant geld in beslag genomen.

[57] Ondergronds bankieren bestaat al eeuwenlang en wordt ook gebruikt voor het verplaatsen/overmaken van niet-criminele inkomsten (Van de Bunt & Huisman, 2009, p. 113-115; Van de Bunt, 2008a, p. 113-120; Kleemans et al., 2002, p. 113-114; Kruisbergen et al., 2012, p. 195-200).

[58] Dit zijn de totale kosten voor het versturen van geld; het gaat dus niet om de vergoeding voor een individuele betrokkene.

[59] Volgens Europol ligt de vergoeding die money mules krijgen voor het cashen van de verdiensten van daders van bijvoorbeeld phishing- of banking-malware-aanvallen op 5% (Europol, 2015b, p. 41). In paragraaf 4.3 zagen we dat geronselde money mules hun vergoeding echter lang niet altijd krijgen (casus 156). Het genoemde percentage omvat voor zover bekend niet de vergoeding voor degene (indien aanwezig) die het ronselen en de activiteiten van de money mules coördineert.

(zeer) grote bedragen in contant geld, stelt daders in staat om hun criminele verdiensten *afgeschermd* te *consumeren*. In deze en in eerdere rondes van de monitor zien we aanbieders van goederen diensten in de reguliere economie die daders hierbij, bewust of onbewust, van dienst zijn. Het kan gaan om autobedrijven, aanbieders van woonruimte, elektronicawinkels, aannemers, reisbureaus en andere aanbieders van (kostbare) goederen en diensten. Deze aanbieders vervullen een belangrijke functie voor daders, soms vanuit onwetendheid, soms vanuit een passieve houding van 'geen vragen stellen' en soms is sprake van doelbewust meewerken of zelfs van een professionele facilitator (Kruisbergen et al., 2012, p. 93-99). Sommige aanbieders gaan er simpelweg van uit dat hun klanten grotere bedragen contant afrekenen, mogelijk gezien de aard van de verkochte goederen of diensten. In een nummer van Justitiële Verkenningen zien we hier een voorbeeld van. Daarin wordt een eigenaar van twee spyshops aangehaald: *'Wij hebben geen limiet aan contante betalingen', 'Ik vind € 4.400 geen groot bedrag om op zak te hebben als je bij ons komt' en 'Bij ons wordt alles contant betaald. € 4.400 is geen bijzondere transactie en geen bijzonder groot bedrag'* (De Korte, 2017, p. 39).[60]

De prominente rol die contant geld speelt binnen traditionele en ICT-gerelateerde georganiseerde criminaliteit, biedt aanknopingspunten voor beleid en de opsporing. Hier gaan we in de slotbeschouwing van dit rapport op in (hoofdstuk 5).

4.5 Recapitulatie

In dit hoofdstuk zijn we ingegaan op de criminele geldstromen in de dertig zaken uit de vijfde ronde van de Monitor Georganiseerde Criminaliteit, met name in relatie tot het gebruik van ICT.
Recapitulerend kunnen we op basis van de literatuur en de door ons geanalyseerde zaken zeggen dat financiële aspecten relatief onderbelicht blijven in de opsporing van en het wetenschappelijk onderzoek naar cybercriminaliteit, zoals dat in meer of mindere mate ook geldt voor traditionele (georganiseerde) criminaliteit. Criminele verdiensten blijven met andere woorden nogal eens buiten het zicht van de opsporing (en van onderzoekers). Toch leveren de dertig zaken samen een aantal interessante inzichten op.
Over de verdeling van criminele verdiensten binnen criminele samenwerkingsverbanden is weinig bekend. Interessant daarbij is wel dat de summiere informatie die hierover wel beschikbaar is, goed aansluit bij bevindingen uit hoofdstuk 2. In dat hoofdstuk kwam naar voren dat in sommige netwerken op het gebied van cybercrime kernleden vrij sterk afhankelijk zijn van (offline of online) facilitators met technische expertise, hetgeen bevestigd wordt door in enkele cybercrimezaken aangetroffen informatie over de verdeling van de inkomsten. De analyse van de dertig zaken laat op het punt van besteding van criminele inkomsten geen grote verschillen zien ten opzichte van de analyses uit eerdere monitorrondes en ook geen grote verschillen tussen traditionele en ICT-gerelateerde criminaliteit. Zowel wat betreft consumptie van inkomsten als investeringen (aangetroffen bezittingen) in de legale economie passen de uitkomsten op hoofdlijnen bij eerder gevonden resultaten (hoewel een enkele zaak een ander beeld laat zien). Bij die investeringen gaat het vaak om huizen en ander onroerend goed en (dekmantel)bedrijven, waarbij deze bedrijven vaak worden gebruikt bij de criminele activiteiten van daders. Dat in enkele cybercrimezaken daders betrokken zijn bij ICT-gerelateerde bedrijven past

[60] De spyshopeigenaar is geïnterviewd ten behoeve van scriptie-onderzoek van de De Korte.

in het eerder geschetste beeld; de afstand tussen daders en hun bezittingen is in fysieke en/of sociale zin vaak klein.
Bij het afschermen van criminele inkomsten zien we wel belangrijke verschillen tussen traditionele georganiseerde criminaliteit enerzijds en ICT-gerelateerde criminaliteit anderzijds. Binnen de 23 zaken op het terrein van traditionele georganiseerde criminaliteit zagen we de verschillende modaliteiten zoals die in de vorige monitorronde zijn beschreven: het verbergen en verplaatsen van contant geld, het afgeschermd consumeren van criminele inkomsten in Nederland en meer complexe witwasconstructies zoals het fingeren van legale inkomsten uit dienstbetrekking of bedrijf, loan-backconstructies of het doorsluizen van geld via buitenlandse rechtspersonen. Het gebruik van bitcoins hebben we in deze 23 zaken van traditionele georganiseerde criminaliteit niet gezien (waarbij werd aangetekend dat een deel van de opsporingsonderzoeken liep in een periode waarin bitcoin nog niet bekend was bij een groter publiek). Wel zagen we in een zaak het gebruik van een andere 'nieuwe' betaalmethode, prepaidkaarten. Al met al zijn de traditionele zaken van georganiseerde criminaliteit ook wat betreft witwasactiviteiten dus nog steeds vrij 'traditioneel'.
Meer klassieke witwasmethoden, zoals afgeschermde consumptie of het fingeren van een legaal inkomen uit bedrijf, kwamen we ook tegen in de zaken met een ICT-component. Belangrijker zijn hier echter de relatief nieuwe, financiële modi operandi die deze zaken kenmerken. Bij ICT-gerelateerde criminaliteit zijn de opbrengsten, in tegenstelling tot veel vormen van traditionele georganiseerde criminaliteit, vaak digitaal van aard. Verkopers van drugs die handelen op een darknet market ontvangen de opbrengsten van hun handelswaar vaak in een cryptomunteenheid zoals bitcoin. Plegers van phishing- en malware-aanvallen verkrijgen door hun fraudeleuze handelingen de controle over het online betalingsverkeer van hun slachtoffers, dat in digitale euro's verloopt. In de cyberzaken die we hebben geanalyseerd werden deze euro's vervolgens contant opgenomen en/of ze werden gebruikt voor de aanschaf van onder andere bitcoins, webmoney, vouchers en/of goederen (die vervolgens werden verkocht of door de daders zelf werden gebruikt). Het gebruik van bitcoin is een belangrijke nieuwe ontwikkeling. Cryptovaluta zoals bitcoin zijn op darknet markets een belangrijk (of hét) betaalmiddel. Verder zagen we dus ook in twee banking-malwarezaken dat daders met een deel van de gestolen euro's bitcoins aankopen (die deels weer worden omgewisseld). Ten behoeve van de criminele geldstromen in ICT-gerelateerde criminaliteit wordt verder gebruikgemaakt van 'nieuwe' soorten van dienstverlening, zoals bitcoin 'mixing services', money mules en bitcoinwisselaars. In de zaken die wij analyseerden had het opereren van zowel de money mules als een deel van de bitcoinwisselaars een lokale dimensie; de money mules werden geronseld binnen het sociale netwerk van kernleden en sommige bitcoinwisselaars maakten gebruik van lokale voorzieningen om hun klanten te ontmoeten (een andere bitcoinwisselaar opereerde op een andere minder lokaal gebonden wijze).
De centrale rol van contant geld is een overheersend, gemeenschappelijk kenmerk van veel van de door ons bestudeerde zaken, zowel op het terrein van traditionele als ICT-gerelateerde georganiseerde criminaliteit. Daders verbergen contant geld, zorgen dat contant geld in andere landen terechtkomt, wisselen digitale valuta (bitcoins of euro's) om in contant geld en kopen kostbare goederen en diensten met contant geld. Daarbij maken zij gebruik van een breed scala aan dienstverleners, die onbewust, zonder veel vragen te stellen, of doelbewust daders helpen hun financiële zaken te regelen. In hoofdstuk 5 komen we bij de bespreking van mogelijke beleidsconsequenties terug op criminele geldstromen en het belang van contant geld.

5 Slotbeschouwing

Het doel van dit deelrapport van de Monitor Georganiseerde Criminaliteit is het vergroten van het inzicht in hoe daders binnen de georganiseerde criminaliteit ICT gebruiken en welke invloed dat gebruik heeft op hun criminele bedrijfsprocessen. Daarbij kijken we niet uitsluitend naar cybercrime, maar verkennen we het gebruik van ICT én de consequenties daarvan voor een breder scala van soorten georganiseerde criminaliteit. In de drie voorafgaande empirische hoofdstukken hebben we het gebruik van ICT onderzocht in relatie tot de volgende deelthema's: het ontstaan en groeien van criminele samenwerkingsverbanden; de logistieke keten van criminele processen; en criminele geldstromen. Het empirisch materiaal dat is gebruikt bestaat uit de dertig zaken die zijn geanalyseerd in de meest recente, vijfde ronde van de Monitor Georganiseerde Criminaliteit. Die dertig zaken beslaan gevallen van traditionele georganiseerde criminaliteit, traditionele georganiseerde criminaliteit waarbij het gebruik van ICT een belangrijk vernieuwend element is, georganiseerde low-tech cybercriminaliteit en georganiseerde high-tech cybercriminaliteit. Dit slothoofdstuk bevat een synthese van de belangrijkste bevindingen (paragraaf 5.1). Ook bespreken hier nog eens de reikwijdte van ons onderzoek (paragraaf 5.2). Ten slotte gaan we in op de mogelijke beleidsimplicaties van onze onderzoeksuitkomsten (paragraaf 5.3).

5.1 Synthese van de belangrijkste bevindingen

Wat opvalt bij de analyse van criminele samenwerkingsverbanden is dat de meeste netwerken een min of meer vaste groep kernleden kennen die gedurende een langere periode samenwerken. Verder is er binnen de meeste netwerken sprake van meer en minder belangrijke verdachten en afhankelijkheidsrelaties. Binnen de cybercrimezaken zijn technische kennis en vaardigheden voor de uitvoering van de delicten van groot belang. De kernleden van deze netwerken hebben deze expertise echter vaak niet zelf in huis. Deze expertise wordt dan gevonden op online forums (in het geval van high-tech cybercriminaliteit) of via offline contacten in het criminele milieu (low-tech cybercriminaliteit).
Wat betreft de instroom- en doorgroeimechanismen zien we over het algemeen ook in deze vijfde monitorronde dat sociale relaties een belangrijke rol spelen. Kernleden, ook in cybercrimezaken, kennen elkaar met name dankzij hun offline sociale netwerken, hoewel ook internet wordt gebruikt om contacten te leggen.

Verder zijn we ingegaan op de rol die ICT speelt bij het oplossen van logistieke problemen die criminele activiteiten met zich meebrengen. Ontmoetingen en communicatie met mededaders zijn een belangrijke logistieke vereiste binnen veel criminele processen. ICT speelt daarbij een belangrijke rol, vooral door de mogelijkheden van bijvoorbeeld versleutelde communicatie, maar ook door bijvoorbeeld technische middelen die daders gebruiken om fysieke ruimten te beschermen tegen afluisteren.
Een belangrijke logistieke flessenhals bij verschillende vormen van transitcriminaliteit bestaat uit het veilig passeren van grenzen. Door de essentiële rol die ICT speelt binnen controles en afhandeling van vervoersstromen op lucht- en zeehavens, is het voor daders belangrijker geworden om toegang te hebben tot geautomatiseerde systemen, via personeel of anderszins. Het is echter de vraag of daarmee het logistieke proces van smokkeloperaties wezenlijk is veranderd. Om bijvoorbeeld tijdig en

veilig de in een container verstopte drugs in handen te krijgen, moeten daders vaak nog fysiek aanwezig zijn of daarvoor insiders gebruiken of misleiden.
Voor criminele markten heeft ICT tot belangrijke innovaties geleid: vragers en aanbieders van bijvoorbeeld drugs kunnen elkaar anoniem 'ontmoeten' en, eveneens tot op zekere hoogte anoniem, transacties verrichten (vooral voor kleinere hoeveelheden).
Bij fraude met het betalingsverkeer ten slotte heeft de digitalisering ertoe geleid dat het bereik van daders veel groter is geworden. Het cashen van de opbrengsten, de laatste schakel in de logistieke keten van bijvoorbeeld phishing- of banking-malware-aanvallen, is echter nog steeds een grotendeels fysiek proces.

Criminele geldstromen lijken zowel in zaken van traditionele georganiseerde criminaliteit als in gevallen van cybercrime nogal eens buiten het zicht van de opsporing te blijven. Toch genereren de dertig geanalyseerde zaken ook hier belangrijke inzichten. Op het punt van besteding van criminele inkomsten laten de analyses geen grote verschillen zien ten opzichte van eerdere monitorrondes en ook geen grote verschillen tussen traditionele en cybercriminaliteit.
Verder zien we ook bij het afschermen van criminele inkomsten (witwassen) de in eerdere rapportages beschreven varianten veelvuldig terugkomen in de onderzochte zaken. Een wezenlijk verschil tussen traditionele en ICT-gerelateerde criminaliteit is er wel bij het gebruik van nieuwe betaalvormen. Op ondergrondse, online marktplaatsen wordt betaald met cryptovaluta, zoals de bitcoin, die samen met onder andere prepaidkaarten of vouchers ook een rol spelen bij bijvoorbeeld banking malware.
Opvallend blijft echter ook de prominente rol van contant geld binnen de onderzochte zaken, zowel bij traditionele georganiseerde criminaliteit als cybercriminaliteit. Daders verbergen contant geld, zorgen dat contant geld in andere landen terechtkomt, wisselen digitale valuta (bitcoins of euro's) (deels) om in contant geld en kopen kostbare goederen en diensten met contant geld (afgeschermde consumptie). Vooral bij het verplaatsen, omwisselen en kunnen besteden (accepteren) van contant geld, spelen verschillende actoren uit de omgeving van daders, al dan niet bewust, een belangrijke rol.

ICT biedt daders dus nieuwe mogelijkheden op het terrein van criminele samenwerking, met betrekking tot logistieke aspecten van het criminele bedrijfsproces en wat betreft criminele geldstromen. Zo verlegt ICT de horizon voor daders die zoeken naar slachtoffers, mededaders, hulpmiddelen of klanten. Daders die slachtoffers geld afhandig willen maken, kunnen dankzij internet een groot vangnet uitwerpen. Daders die specifieke kennis of instrumenten zoeken, kunnen die vinden via criminele ontmoetingsplaatsen op internet. ICT leidt zo tot nieuwe vormen van samenwerking. En ook aanbieders en consumenten van drugs vinden op het dark web marktplaatsen die in beginsel vrij zijn van fysieke en sociale begrenzingen. Contacten in de offline wereld en hechte sociale verbanden lijken daardoor minder belangrijk, omdat het gemakkelijker is om mensen, expertise en hulpmiddelen te vinden. Vertrouwen in de capaciteiten van bijvoorbeeld een online aanbieder van drugs is daarbij nog steeds essentieel, waarbij gebruik wordt gemaakt van de mogelijkheden die internet biedt om de reputatie van hulpbronnen na te gaan (Holt et al., 2015; Decary-Hétu & Dupont, 2013; Dupont et al., 2016; Soudijn & Monsma, 2012; Lu et al., 2010; Yip et al., 2013; Holt, 2013; Holt & Smirnova, 2014; Lusthaus, 2012; Schuppers et al., 2016).

Verder zien we dat daders dankbaar gebruikmaken van mogelijkheden om afgeschermd met elkaar te communiceren. Technologische ontwikkelingen hebben ver-

sleutelde communicatie voor iedereen toegankelijk gemaakt, ook voor daders die actief zijn in traditionele, offline vormen van georganiseerde criminaliteit (zie ook Schuppers et al., 2016). Vrij toegankelijke hardware en software voor afgeschermde communicatie bieden een belangrijk voordeel voor daders die onderling zaken willen afstemmen zonder dat de politie dit kan onderscheppen (in hun perceptie). Daarnaast heeft ICT ook bij een fysieke activiteit zoals drugssmokkel tot een vernieuwing van werkwijze geleid, in ieder geval in een casus waarbij daders op een computernetwerk inbraken om het afhalen van een container waarin drugs verstopt was te manipuleren. Ten slotte vormen ook door ICT mogelijk gemaakte voorzieningen als cryptovaluta (en vouchers en/of prepaidkaarten) een belangrijke innovatie. Cryptovaluta kennen een zekere mate van anonimiteit en zijn het betaalmiddel op darknet markets. Samen met de TOR-netwerken waarop darknet markets functioneren maakt een munteenheid zoals bitcoin het mogelijk voor kopers en verkopers van illegale goederen en diensten om min of meer anoniem transacties aan te gaan.
De mogelijkheden die ICT biedt worden dus ook daadwerkelijk gebruikt en daardoor verandert de werkwijze van daders tot op zekere hoogte.

Aan de andere kant is, in ieder geval in ons casusmateriaal, traditionele georganiseerde criminaliteit nog steeds vrij 'traditioneel'. Zo zijn er geen aanwijzingen die duiden op een fundamentele verandering van de manier waarop offline opererende criminele netwerken zich ontwikkelen. Ook het logistieke proces van bijvoorbeeld drugssmokkel lijkt in ons casusmateriaal, ondanks de innovatieve werkwijze die we in een zaak zagen, op hoofdlijnen niet wezenlijk te zijn veranderd. Verder zagen we het gebruik van bitcoins alleen in zaken van cybercrime en online drugssmokkel (en in een witwaszaak die zich richtte op bitcoinwisselaars). Deze financiële innovatie ontbrak dus in de andere zaken. Mogelijk is het voor veel daders niet nodig om via ICT hun werkwijze drastisch te veranderen (zie ook Lavorgna en Sergi, 2014).
Interessanter is dat wanneer we naar cybercrimezaken kijken er parallellen blijken te zijn met meer traditionele georganiseerde criminaliteit. Zo zien we dat ook daders in cybercrimezaken en andere zaken met een belangrijke ICT-component een zekere lokale inbedding kennen (zie ook Leukfeldt et al.,2017b, 2017c, 2017d; Lusthaus & Varese, 2017). Een deel van de hoofddaders in cybercrimezaken lijkt dezelfde fysieke leefomgeving te delen (omdat ze elkaar bijvoorbeeld uit de buurt of het uitgaansleven kennen) en ook katvangers worden nogal eens gevonden in de naaste omgeving. De bronnen van sociaal kapitaal die worden benut voor participatie in georganiseerde criminaliteit, bestaan dus ook in deze zaken voor een belangrijk deel uit offline interacties.
Verder lijken ook darknet markets, ondanks dat online marktplaatsen in theorie niet worden gehinderd door grenzen, een belangrijke lokale (regionale), fysieke component te hebben. Bij de online marktplaats die wij bestudeerden bleek bijvoorbeeld een deel van de transacties, vooral die van grotere omvang, via fysieke ontmoetingen te worden afgehandeld. Verder bleken bij de transacties die via de marktplaats verliepen koper en verkoper nogal eens in nabijgelegen landen te wonen (zie ook Kruithof et al., 2016). Mogelijk worden door de desbetreffende daders de risico's van postzendingen als te hoog ingeschat wanneer het om, respectievelijk, grotere partijen en afstanden gaat.
Ten slotte zijn sommige daders in ICT-gerelateerde zaken in belangrijke mate afhankelijk van lokale voorzieningen, zoals postbedrijven voor online drugsverkopers en publieke plaatsen met wifi-toegang (zoals horecagelegenheden) voor bitcoinwisselaars.
Behalve de lokale dimensie is zoals gezegd de voorkeur van daders voor contant geld een andere belangrijke overeenkomst tussen traditionele en ICT-gerelateerde

georganiseerde criminaliteit. Voor traditionele vormen van georganiseerde criminaliteit is de dominantie van contant geld een bekend gegeven, maar ook daders die online opereren geven er de voorkeur aan om in ieder geval een deel van hun digitale opbrengsten, euro's of bitcoins, om te wisselen voor contant geld.

5.2 Reikwijdte van het onderzoek

Alvorens op de eventuele consequenties van onze onderzoeksbevindingen in te gaan, maken we eerst nog enkele opmerkingen over de reikwijdte van ons onderzoek.
Het empirisch materiaal van de Monitor Georganiseerde Criminaliteit bestaat uit, vaak omvangrijke, opsporingsonderzoeken op het terrein van de georganiseerde criminaliteit. Voor deze vijfde ronde van de monitor zijn dertig opsporingsonderzoeken geanalyseerd.[61] Opsporingsdossiers zijn dus de belangrijkste databron binnen de monitor. Deze opsporingsdossiers bieden een schat aan informatie en zijn van grote waarde voor wetenschappelijk onderzoek naar georganiseerde criminaliteit.
Iedereen die zich wil verdiepen in criminele fenomenen, wordt geconfronteerd met de 'muren van stilzwijgen' die criminele activiteiten omringen, vooral wanneer het gaat om georganiseerde criminaliteit (Van de Bunt, 2007, 2010). Alleen de politie heeft verregaande bevoegdheden om, via de inzet van opsporingsmethoden, door deze 'muren' heen te breken. Een onderzoeker die toegang heeft tot opsporingsdossiers profiteert mee van deze exclusieve bevoegdheden en kan zo een eveneens exclusief inzicht krijgen in de activiteiten van daders of in de wijze waarop zij zich tot elkaar en hun omgeving verhouden. Bronnen als het verslag van een undercoveroperatie, een afgeluisterd telefoongesprek of een afgeluisterde ontmoeting tussen verdachten, kunnen een onvervangbare inkijk geven in hoe daders te werk gaan (Kruisbergen, 2017, p. 184; Kleemans et al., 1998; Kruisbergen et al., 2012).
De uitgebreide zaaksverslagen die van die opsporingsonderzoeken zijn gemaakt, bieden inzicht in de *aard* van de georganiseerde criminaliteit in Nederland. Het materiaal leent zich echter niet voor het doen van kwantitatieve uitspraken. Uitspraken over de omvang van criminele activiteiten of de omvang van de schade als gevolg van die activiteiten, liggen buiten het bereik van dit onderzoek.[62]
Verder geldt voor de bestudeerde opsporingsonderzoeken dat zij vallen binnen de door ons gehanteerde begripsomschrijving van georganiseerde criminaliteit. Dit betekent onder meer dat (cyber)delicten met een terroristische, politieke, activistische of vandalistische achtergrond, maar ook delicten waarbij persoonlijk seksueel genot op de voorgrond staat, niet worden meegenomen. Mede om deze reden zijn in deze ronde bijvoorbeeld geen zaken meegenomen die zich richten op DDoS-aanvallen. Dat betekent niet dat een DDoS-aanval geen ernstig misdrijf met grote schadelijke gevolgen is. Praktijkvoorbeelden laten zien dat een DDoS-aanval, of die nu wordt uitgevoerd door bijvoorbeeld een eenling, een groep criminelen of een statelijke mogendheid, juist veel schade kan aanrichten.
Ook geldt dat alleen gevallen van georganiseerde criminaliteit zijn meegenomen die door Nederlandse autoriteiten zijn opgespoord en vervolgd. Ten slotte geldt dat de bestudeerde opsporingsonderzoeken alleen betrekking hebben op modi operandi

[61] Vijf zaken op het terrein van cybercrime/ICT-gerelateerde georganiseerde criminaliteit die in deze vijfde ronde van de monitor zijn opgenomen, maakten ook onderdeel uit van de studie van Odinot et al. (2017).

[62] Dergelijke uitspraken vallen wel binnen de doelstelling van het *Nationaal dreigingsbeeld Georganiseerde criminaliteit* (Boerman et al., 2017).

zoals die zich in het verleden hebben voorgedaan (beide laatstgenoemde beperkingen gelden voor alle Nederlandse opsporingsonderzoeken; zie ook paragraaf 1.3). Het rijke inzicht dat opsporingsdossiers biedt, kent dus ook beperkingen. Activiteiten en daders die niet in Nederlandse opsporingsdossiers terechtkomen, blijven ook buiten beeld van de onderzoeker. Deze beperking werkt voor cybercrime mogelijk sterker uit dan voor andere typen van (georganiseerde) criminaliteit. Juist bij cybercrime kan een modus operandi of een dadergroepering een sterke internationale component hebben, wat de opsporing en vervolging kan bemoeilijken. Ook een lager bewustzijn van slachtofferschap van cybercrime en een lagere aangiftebereidheid zouden het zicht op cybercrime kunnen bemoeilijken (Schuppers et al., 2016, p. 10). Bovendien zijn juist bij cybercrime lang niet alle door politie en justitie gepleegde interventies zichtbaar in individuele opsporingsdossiers. Zo is het online verzamelen van informatie of het online verstoren of voorkomen van criminaliteit, in zekere zin veel laagdrempeliger dan vergelijkbaar optreden in de offline wereld. Juist bij cybercrime zou daarom bijvoorbeeld voor verstorend optreden gekozen kunnen worden, wat vervolgens niet tot een 'zaak' in traditionele zin hoeft te leiden. Voor een goed wetenschappelijk en beleidsmatig zicht op cybercrime is het daarom van belang om behalve afgeronde, succesvolle opsporingsonderzoeken, ook andere bronnen te ontsluiten. Hierbij kan onder andere worden gedacht aan informatieverzameling rondom verstorende interventies tegen een darknet market of de inzet van een technisch, analytisch instrument als een *webcrawler*.

5.3 Mogelijke implicaties voor beleid

ICT biedt dadergroeperingen in de georganiseerde criminaliteit verschillende mogelijkheden, voor het vinden van mededaders, slachtoffers en klanten, maar ook voor het faciliteren van drugssmokkel, het afschermen van communicatie en het afschermen van geldstromen. De werkwijze van daders biedt echter ook aanknopingspunten voor preventie en bestrijding. Hieronder gaan we in op de mogelijke beleidsimplicaties van onze uitkomsten. Achtereenvolgens bespreken we een aantal overwegingen en mogelijke implicaties op het terrein van regulering (paragraaf 5.3.1), opsporing (paragraaf 5.3.2) en een situationele aanpak (paragraaf 5.3.3).

5.3.1 Regulering van cryptovaluta en aanverwante diensten?

Nieuwe criminele werkwijzen, en de opsporing daarvan, kunnen de vraag oproepen of bestaande wet- en regelgeving voldoende is toegerust voor de nieuwe situatie. Dit geldt bijvoorbeeld voor het criminele gebruik van cryptovaluta. Bitcoins en andere varianten zijn op dit moment grotendeels ongereguleerd. In dit rapport en in eerdere publicaties is beschreven hoe daders gebruikmaken van deze innovatie. Cryptomunteenheden vormen het betaalmiddel op darknet markets. Ook kunnen andere daders, die met hun activiteiten geen bitcoins maar euro's genereren, ervoor kiezen hun criminele inkomsten (deels) om te zetten in cryptovaluta, waarbij dat bij onze zaken overigens beperkt bleef tot enkele gevallen van cybercrime. Niet alleen de cryptovaluta zelf, ook aanverwante diensten vallen op dit moment grotendeels buiten financiële regulering en toezicht. Daardoor zijn bitcoinexchangers bijvoorbeeld ook niet meldplichtig in het kader van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft).[63]

[63] Dit betekent overigens niet dat financiële instellingen zoals banken geen meldingen kunnen doen bij bijvoorbeeld de politie wanneer zij ongebruikelijke transacties waarnemen die aan cryptovaluta zijn te relateren. Zo is de door ons onderzochte zaak die draait om de bitcoinwisselaars aan het licht gekomen na een melding van een bank bij

Regulering en toezicht kunnen handvatten bieden om witwassen via cryptovaluta tegen te gaan. Zo zouden bijvoorbeeld (Nederlandse) online wisselkantoren, zoals de bitcoinexchangers, onder het bereik van Nederlandse toezichthouders kunnen worden gebracht. Dit kan de witwasmogelijkheden via cryptovaluta verkleinen.[64] Aan de andere kant zou regulering vanuit het perspectief van anti-witwasbeleid ook nadelen kunnen hebben. Op dit moment lijkt de acceptatie van cryptovaluta in de reguliere economie nog laag. Regulering zou bij kunnen dragen aan 'normalisering' van cryptovaluta en een hogere graad van acceptatie van cryptovaluta als betaalmiddel, waarmee de mogelijkheden om op criminele wijze verdiende cryptovaluta in de reguliere economie om te zetten – wit te wassen – juist worden vergroot (zie ook Oerlemans et al., 2016).[65]

5.3.2 Opsporing

Inherente kwetsbaarheid technologie

De afschermingsmogelijkheden die ICT daders biedt en het internationale aspect dat sommige werkwijzen op het terrein van ICT-gerelateerde criminaliteit kenmerkt, bemoeilijken de opsporing. Daders gebruiken bijvoorbeeld met encryptie toegeruste communicatieapparatuur, online marktplaatsen waar illegale transacties plaatsvinden worden benaderd via TOR-netwerken en genoemde transacties worden met een zekere mate van anonimiteit afgerekend in cryptovaluta. Maar ook cybercriminelen en daders die ICT gebruiken om hun criminele activiteiten uit te voeren, laten sporen na en/of zijn op een andere manier kwetsbaar voor tegenmaatregelen (zie ook Odinot et al., 2017; Oerlemans et al., 2016). We lichten hieronder deze inherente kwetsbaarheid die het gebruik van technologie voor daders met zich meebrengt toe.

Ten eerste kent anonimiteit op internet ook beperkingen. Zo wordt internetverkeer vaak op de een of andere manier geregistreerd, ook al zijn die registraties niet altijd (direct) voor derden toegankelijk. De transactiegeschiedenis van bitcoins wordt bijvoorbeeld vastgelegd. Een transactie met bitcoin komt neer op het overboeken van een aantal bitcoins naar een adres dat aan de ontvanger toebehoort. Deze overboekingen worden geregistreerd in een soort logboek, waarbij wel geldt dat gebruik van een 'mixing service' het zicht kan ontnemen op de herkomst van een bitcoin. Een belemmering voor de opsporing is verder dat achter specifieke bitcoinadressen vaak pseudoniemen schuilgaan. Echter, door transactiegegevens te analyseren en te koppelen aan andere bronnen, en vanwege niet-optimaal gedrag van gebruikers, kunnen bepaalde transacties toch naar personen worden herleid (Meiklejohn et al., 2013; Ron & Shamir, 2013; Oerlemans et al., 2016). Een gebrek aan anonimiteit, kortom, zit soms tot op zekere hoogte ingebakken in de gebruikte technologie.

---

de *Electronic Crimes Task Force*, kortweg ECTF, een samenwerkingsverband tussen de politie en een aantal banken.

[64] Waarbij geldt dat de internationale aspecten die aan (dienstverlening rondom) cryptovaluta verbonden zijn de handhaving van regulering kunnen bemoeilijken.

[65] In de meest recente Criminaliteitsbeeldanalyse Witwassen wordt beredeneerd dat het ongereguleerde karakter van de bitcoin in relatie tot het criminele gebruik een (ander) maatschappelijk voordeel heeft. Aangezien transacties op het darknet via ongereguleerde cryptovaluta als Bitcoin verlopen, blijven 'foute' transacties buiten het reguliere financiële stelsel, wat de integriteit van dat stelsel ten goede komt (Soudijn, 2017, p. 37). Wel is het zo dat uit onderzoek is gebleken dat door misdaad verdiende bitcoins vaak worden omgewisseld voor bijvoorbeeld euro's, waardoor ook dit misdaadgeld toch weer in het reguliere verkeer terechtkomt (deze studie; Leukfeldt, 2014; Leukfeldt et al., 2017a, 2017b, 2017c; Oerlemans et al., 2016; Europol, 2015a).

Maar, ten tweede, ook technologie waarvan wordt verondersteld dat deze wel 'waterdicht' is, biedt daders geen garantie op afscherming van politie en justitie. Dit blijkt bijvoorbeeld uit het opsporingsonderzoek tegen *Ennetcom*. Ennetcom was een belangrijke aanbieder van versleutelde communicatie, waarvan, in ieder geval volgens het OM, veelvuldig gebruik werd gemaakt door criminelen. In 2016 kreeg het OM de beschikking over enorme hoeveelheden data van de server waarvan Ennetcom gebruikmaakte. Klanten van Ennetcom gebruikten aangepaste smartphones (*Blackberries*) die waren voorzien van encryptiesoftware (*Pretty Good Privacy*). Deze software stelt bezitters van deze smartphones in staat om onderling afgeschermd te communiceren. De telefoons waren bovendien vaak ontdaan van microfoon en camera, om afluisteren en meekijken te voorkomen. Met het opsporingsonderzoek, waarbij onder meer een kopie is gemaakt van de server, kregen politie en justitie echter de 'sleutel' in handen tot de berichten die via Ennetcom werden verstuurd. Volgens politie en justitie zijn, via de ontcijferde informatie van de server, miljoenen berichten toegankelijk gemaakt, berichten die voorheen voor de opsporing verborgen bleven. De op deze wijze verkregen informatie zou van nut zijn voor een groot aantal opsporingsonderzoeken naar zware misdrijven.[66]
Ten derde kunnen dezelfde kenmerken die een technologie aantrekkelijk maken voor daders, in sommige gevallen ook de politie handvatten bieden om die daders aan te pakken. Een sprekend voorbeeld vormt hier de darknet market *Hansa*. Deze ondergrondse marktplaats, waarop drugs werd verhandeld, is via een internationale operatie ontmanteld. Medio 2017 werden niet alleen de beheerders van deze marktplaats aangehouden, maar werden ook de servers in beslag genomen. Een kopie van de marktplaats werd vervolgens via Nederlandse servers voortgezet, onder controle van de Nederlandse politie en het OM. Op deze manier zijn grote aantallen transacties én kopers en verkopers in beeld gebracht.[67] Het beheer van een dergelijke onlinemarktplaats door de politie zou als een undercoveroperatie kunnen worden beschouwd. Ook ons eigen casusmateriaal biedt een voorbeeld van een undercoveroperatie tegen daders die op een darknet market actief waren.[68] De opkomst van internet biedt dus niet alleen daders nieuwe mogelijkheden. De (ogenschijnlijke) anonimiteit waarmee op darknet markets kan worden gehandeld en die deze marktplaatsen aantrekkelijk maakt, biedt ook opsporingsambtenaren immers een goede dekmantel (zie ook EMCDDA, 2016). Daardoor zijn ook daders die online opereren kwetsbaar voor een, oorspronkelijk voor de offline wereld ontwikkelde opsporingsmethode als een undercoveroperatie. Politieoptreden zoals ten aanzien van Hansa komt het wederzijds vertrouwen tussen kopers en verkopers op darknet markets – essentieel voor het functioneren van die marktplaatsen – niet ten goede (zie ook Kruithof et al., 2016).

Raakvlakken online-offline

ICT is een essentieel onderdeel van de huidige samenleving. Ook in veel vormen van (georganiseerde) criminaliteit speelt ICT op zijn minst enige rol, al was het maar omdat daders gebruikmaken van moderne communicatietechnologie. Kennis van ICT en daarop toegesneden opsporingsinstrumenten is daarom ook belangrijk voor de opsporing van traditionele georganiseerde criminaliteit. Het grote raakvlak tussen de online en offline wereld werkt echter twee kanten uit. In deze studie be-

[66] www.politie.nl/nieuws/2017/maart/9/11-versleutelde-berichten.html, geraadpleegd op 15 januari 2018.

[67] www.politie.nl/nieuws/2017/juli/20/ondergrondse-hansa-market-overgenomen-en-neergehaald.html, geraadpleegd op 15 januari 2018.

[68] In casus 152 legde een undercoveragent contact met een van de verdachten die betrokken waren bij een online marktplaats op het darknet. Uiteindelijk vonden online en offline meerdere contacten én pseudokopen plaats tussen undercoveragenten en verdachte(n), hetgeen mede leidde tot aanhoudingen en veroordelingen.

schreven we dat ook in cybercrimezaken en andere zaken met een duidelijke ICT-component de werkwijze van daders gekenmerkt wordt door een zekere mate van lokale inbedding. Ook vanuit het perspectief van deze daders is de wereld van 'traditionele' georganiseerde criminaliteit niet strikt gescheiden van cybercrime (zie ook Leukfeldt et al., 2017a, 2017b, 2017d; Lusthaus & Varese, 2017; Bijlenga & Kleemans, 2017). Ook bij ICT-gerelateerde criminaliteit is het immers vaak zo dat een of meerdere essentiële schakels van het criminele bedrijfsproces zich afspelen in de fysieke, offline wereld. We zagen bijvoorbeeld hoofddaders die dezelfde sociale, lokale herkomst delen, daders die katvangers rekruteren in hun lokale omgeving, bitcoinwisselaars die hun klanten bedienen op met wifi toegeruste publieke plekken en daders die drugs verhandelen via darknet markets die mede afhankelijk zijn van reguliere postbedrijven. Nieuwe verschijningsvormen van criminaliteit vereisen daarom niet alleen nieuwe bevoegdheden of specifieke, technische opsporingsinstrumenten, maar bieden ook veel aanknopingspunten voor meer klassieke methoden.

Financiële opsporing
Beleidsmatig wordt al geruime tijd ingezet op wat een financiële aanpak van georganiseerde criminaliteit kan worden genoemd. Dat omvat het financieel rechercheren, het voorkomen en bestrijden van witwassen en het afpakken van criminele verdiensten (zie ook Kruisbergen, 2017). Het ligt het voor de hand dat deze aanpak ook bij ICT-gerelateerde criminaliteit wordt gehanteerd. Ten eerste is het zo dat ook daders die online opereren vaak gemotiveerd zijn door financieel gewin.[69] Ten tweede is het zo dat bij verschillende vormen van ICT-gerelateerde criminaliteit met name het incasseren of omwisselen van de opbrengsten een fase in het criminele bedrijfsproces is waarin daders kwetsbaar zijn, omdat ze dan direct of indirect in contact komen met de reguliere omgeving. Dit geldt voor daders van bijvoorbeeld banking malware en phishing die hun digitale euro's willen omwisselen in contanten. Het geldt ook voor de drugshandelaren die hun op het darknet verdiende cryptovaluta willen omruilen voor contante euro's. Contant geld speelt nog steeds een hoofdrol in de criminele wereld, ook wanneer de criminelen zich met online activiteiten bezighouden. Dit kwam terug in ons casusmateriaal maar blijkt ook uit ander onderzoek (bijvoorbeeld Europol, 2015a).
Ten derde kan een financiële insteek bij de opsporing nieuw zicht bieden op bepaalde aspecten van criminele samenwerkingsverbanden. Zo kan het volgen van een geldstroom leiden tot nieuwe verdachten en kan informatie over de verdeling van criminele inkomsten duidelijk maken welke daders cruciale schakels zijn in criminele netwerken. Een financiële invalshoek kan belangrijke leeropbrengsten genereren, zeker gezien het feit dat er nog relatief weinig bekend is over het gebruik van specifieke ICT-gerelateerde witwasmogelijkheden en de ontwikkelingen op dit terrein elkaar snel opvolgen.

5.3.3 Situationele aanpak: drempels opwerpen

In de monitorrapportages die tot nu zijn verschenen komt steeds naar voren hoe sterk georganiseerde criminaliteit verweven is met haar sociale omgeving. In de situationele benadering – en aanpak – van georganiseerde criminaliteit wordt de nadruk niet gelegd op de hoofddaders zelf, maar wordt in plaats daarvan de aandacht gevestigd op de factoren in de omgeving die deze criminaliteit mogelijk maken. Een grondige analyse van specifieke delicttypen brengt deze factoren en andere schakels uit het criminele bedrijfsproces in kaart. Wie deze schakels kent,

[69] Daders kunnen ook handelen vanuit nieuwsgierigheid of activistische of politieke overwegingen (zie ook Weulen Kranenbarg, 2018).

kan ook barrières opwerpen tegen die delicttypen. Op het terrein van de traditionele georganiseerde criminaliteit bestaan verschillende voorbeelden van deze benadering, bijvoorbeeld ten aanzien van drugshandel en mensenhandel (Bullock et al., 2010; Cornish & Clarke, 2002; Von Lampe, 2011; Clarke, 1997; Cornish, 1994; Kleemans, 2014; Chiu et al., 2011; Tompson & Chainey, 2011).
Ook bij de verschillende ICT-gerelateerde vormen van georganiseerde criminaliteit die in dit rapport zijn besproken, maken daders gebruik van personen of voorzieningen uit hun omgeving, bijvoorbeeld van banken. Zo vinden daders van bijvoorbeeld phishing- of banking-malware-aanvallen hun slachtoffers onder rekeninghouders bij reguliere banken. Banken spelen dan ook een cruciale rol in de preventie en bestrijding van verschillende vormen van criminaliteit. Banken zijn zich daarvan bewust en werken bijvoorbeeld samen in het Electronic Crimes Task Force (ECTF), een samenwerkingsverband tussen banken, politie en het OM. De fraude gepleegd via het internetbankieren en via skimmen is de afgelopen jaren zeer sterk gedaald, hetgeen waarschijnlijk mede het gevolg is van de door banken in gang gezette maatregelen en campagnes (NVB, 2017; Oerlemans, 2016, p. 92-93; Schuppers et al., 2016, p. 64).[70] Maar ook bij de bestrijding van witwassen spelen banken een belangrijke rol. Bankrekeningen worden gebruikt voor het doorsluizen en cashen van criminele opbrengsten en voor het omwisselen van cryptovaluta in reguliere valuta. Banken kunnen meldingen doen wanneer bij bepaalde rekeningen opvallende stortingen en opnames plaatsvinden, wat kan wijzen op bijvoorbeeld het cashen van fraudegeld door money mules of omwisselacties van bijvoorbeeld bitcoinwisselaars. Deze meldingen doen zij ook – zoals ook uit ons casusmateriaal blijkt – wat de aanpak van deze vormen van criminaliteit ten goede komt. Dat het optreden van banken ertoe doet, blijkt uit het sterk afgenomen schadebedrag als gevolg van fraude met internetbankieren, maar ook uit opsporingsonderzoeken naar witwassen die opstarten na een melding door een bank. Gezien de centrale positie die banken innemen en de dynamiek in de modi operandi van daders, blijven banken een belangrijke rol spelen in de preventie en bestrijding van georganiseerde criminaliteit.
Banken, money mules (en andere manieren om geld weg te sluizen) en (fysieke) cryptowisseldiensten zijn cruciaal voor bepaalde delicttypen. De twee laatstgenoemde actoren kunnen hun rol spelen omdat ook in de wereld van gedigitaliseerde criminaliteit veel daders een voorkeur hebben voor contant geld. Op dat punt kan de aanpak meeliften met generieke maatregelen tegen contante geldstromen binnen de georganiseerde criminaliteit. Het casusmateriaal geeft aanleiding te vermoeden dat nog steeds veel, op criminele wijze verdiend geld in contante vorm zijn weg vindt in de reguliere economie. Daarbij geldt dat daders, bewust of onbewust, worden gefaciliteerd doordat zij bij sommige aanbieders kostbare goederen of diensten zonder problemen contant kunnen afrekenen (afgeschermde consumptie).[71] Vanwege de dominante rol die contant geld speelt in offline én online criminaliteit, kan het bemoeilijken van bijvoorbeeld afgeschermde consumptie een effectieve bijdrage leveren aan de bestrijding van criminele geldstromen.
Andere voorbeelden van diensten en dienstverleners die bewust of onbewust een belangrijke rol spelen in de werkwijze van daders, zijn postbedrijven (voor verzor-

[70] De daling omvat alleen de schade die bij de banken bekend is en dus niet noodzakelijkerwijs alle gevallen van door individuen geleden schade. Overigens kan cybercrime, net als andere vormen van criminaliteit, meer schade berokkenen dan alleen financiële. Zo kan emotionele schade optreden, bijvoorbeeld bij een delict als afpersing via ransomware. Ook veroorzaakt cybercrime indirecte, economische schade, bijvoorbeeld door afnemend vertrouwen in internetdiensten en stijgende beveiligingskosten (Schuppers et al., 2016).

[71] Overigens zal het gebruik van grote coupures door daders op termijn worden bemoeilijkt doordat de ECB in 2018 zal stoppen met de productie van nieuwe € 500-biljetten (zie ook Soudijn & Reuter, 2016; Europol, 2015a, p. 359-363; ECB, 2011).

ging van via internet verhandelde drugs en andere waar), 'mixing services' voor cryptovaluta, aanbieders van apparatuur of software voor afgeschermde communicatie, en online ontmoetingsplaatsen waarop technische expertise wordt gevonden die wordt ingezet bij criminele activiteiten. Het in kaart brengen van deze en andere voor daders cruciale diensten is niet alleen van belang voor de preventie van georganiseerde criminaliteit maar ook voor de opsporing. Net als bij traditionele georganiseerde criminaliteit is bij de opsporing van ICT-gerelateerde criminaliteit de hoeveelheid potentiële verdachten waar de opsporing haar instrumenten op kan richten immers groot en de capaciteit daarvoor beperkt. Er moeten dus keuzes worden gemaakt. Een gerichte opsporing van facilitators kan criminele processen (tijdelijk) verstoren. Het zendt bovendien een boodschap uit aan hen die soortgelijke diensten verlenen en die zich, zeker wanneer het gaat om relatief nieuwe soorten van dienstverlening, beroepen op onwetendheid omtrent de bedoelingen van hun klanten.

Onze analyse van opsporingsonderzoeken laat zien dat ook ICT-gerelateerde criminaliteit duidelijke raakvlakken heeft met de offline wereld en, net als traditionele georganiseerde criminaliteit, mede afhankelijk is van de reguliere omgeving. Dit toont enerzijds aan dat het onderscheid tussen cybercrime en traditionele georganiseerde criminaliteit minder scherp is dan soms wordt gedacht. Anderzijds wijst het erop dat behalve technische instrumenten ook meer traditionele opsporingsmethoden en een situationele aanpak goede mogelijkheden bieden bij de aanpak van ICT-gerelateerde criminaliteit.

Summary

Organised crime and IT

Empirical results of the fifth round of the Dutch Organised Crime Monitor

This study provides empirical insight into how organised crime uses IT and how it affects criminal operations. We do not focus on cybercrime alone. Instead, we explore the use of IT and its consequences in a broad range of types of organised crime, i.e. from 'traditional' types of organised crime such as offline drug smuggling to cybercrime.

The massive use of the internet, and more generally the effect of IT on all segments of society, entails new opportunities for organised crime. However, there is only a limited amount of empirical research into how criminals use these options and what consequences the use of IT has for how criminals operate (Leukfeldt et al., 2017a). A number of studies have recently been published. Odinot et al. analysed criminal investigations in the field of cybercrime (Odinot et al., 2017; Bulanova-Hristova et al., 2016). Leukfeldt et al. also conducted empirical research into cybercrime, focusing in particular on the processes of origin and growth and modi operandi of cyber networks (Leukfeldt et al., 2017b, 2017c, 2017d). Finally, Oerlemans et al. (2016) looked into how money is laundered in banking malware and ransomware cases.[72] In our study, we build on the work of these and other researchers by both broadening and deepening their work. The broadening consists of the fact that we do not just focus on cases of cybercrime. We investigate the use of IT and its consequences within organised crime in a broader sense. In addition, we deepen our study by analysing the use of IT and its consequences in relation to three essential aspects of criminal operations: criminal cooperation, logistics and handling money flows.

Organised crime and IT: new theoretical and empirical questions

The use of IT in relation to organised crime raises several interesting questions. This is especially true when new forms of crime such as cybercrime, or the use of new technology in traditional organised crime, are linked to existing knowledge, concepts and theories in the field of organised crime.

For example, it is worthwhile to consider what the advent of the internet means for *the way in which organised crime groups are formed and developed*. Earlier studies stress the importance of social capital; to participate and succeed in organised crime, you have to know the right people, producers, clients, facilitators, and so on (Kleemans & Van de Bunt, 1999; Morselli, 2009). Currently, the growth of the internet is opening up new horizons, at least in theory. Physical and other boundaries need no longer pose an obstacle to making contacts. One could ask whether the internet has diminished the importance of real-life social capital. Has 'knowing the right people' transformed into 'knowing your way on the deep web' (Lavorgna, 2013; Przepiorka et al., 2017; Töttel et al., 2016, pp. 28–30; Leukfeldt, 2017)?

Another interesting issue is the role of IT in the *logistics of organised crime*. Any form of organised crime can be described as a logistical process in which a number

[72] Of course, this paragraph does not provide a comprehensive overview of the literature. The most important outcomes of other studies are discussed in Section 4.

of necessary steps must be taken (Cornish & Clarke, 2002). In the case of international drug trafficking, these steps may include production/purchase of drugs, transport and storage, crossing border controls, and sales, among other things. Communication between criminals (for example, in order to coordinate activities) is also a common prerequisite for the successful completion of organised crime activities. In what way do criminals use IT to improve the logistical process and does the use of IT potentially lead to new logistical bottlenecks?
Handling money flows is a specific type of bottleneck for every successful offender. Organised crime is motivated – at least in part –by financial gain. However, criminal earnings bring certain risks, especially if your criminal operations are successful and generate a lot of money. Criminal earnings and the spending of those earnings may raise suspicion, which in turn could lead to arrest and confiscation of your assets. How and to what extent do offenders use IT-facilitated possibilities, such as bitcoin, to launder their money?

Research questions, methods and data

This research is part of the Dutch Organised Crime Monitor. A well-founded approach to organised crime is only possible when there is sound insight into the nature of organised crime. The Organised Crime Monitor provides that insight by making use of the knowledge gained during large-scale criminal investigations. This report is the result of the most recent, fifth round of the Monitor (for previous reports, see Kleemans et al., 1998, 2002; Van de Bunt & Kleemans, 2007; Kruisbergen et al., 2012). To consider specific themes in greater depth, we have chosen to develop the fifth round into three separate sub-reports. The first sub-report was published in October 2017 (Van Wingerde & Van de Bunt, 2017). This report focused on the punishing of organised crime offenders. You are reading the second sub-report, which focuses on organised crime and IT (information technology).

The following research question will be addressed:

How do organised crime groups use IT and how does this use change the ways in which they operate?

We will divide the research question into three subthemes:
- the use of IT in relation to the processes of origin and growth of organised crime groups;
- the use of IT in relation to the logistics chain of criminal processes;
- the use of IT in relation to handling criminal money flows.

Our empirical data consist of large-scale criminal investigations into organised crime. These cases are part of the Dutch Organised Crime Monitor (DOCM). The DOCM is an ongoing research project into the nature of organised crime in the Netherlands. In five data sweeps, 180 cases of organised crime are analysed. Each case includes several and sometimes dozens of individual suspects. For each of the cases, the police files are analysed. The police files contain the results of all police activities that were deployed in a case, such as wiretapping, monitoring of internet traffic, undercover policing, interrogations of suspects, confiscation of goods and financial information. For this paper, we used the thirty cases that were analysed in

the fifth and most recent data sweep.[73] These thirty cases cover various types of organised crime, such as different types of drug trafficking, illegal arms trade, human trafficking, fraud and money laundering, and cybercrime.
We distinguish four categories of cases, depending on the role that IT plays. The first category comprises 23 cases of *traditional organised crime*; in other words, cases without a strong IT component. These include cases of offline drug trafficking (cases 158, 159, 161–164, 167, 169–172, 175 and 176), human smuggling/trafficking (case 160), money laundering (cases 157, 166, 168, 177, 178 and 180), and other/combined crimes (cases 165, 174 and 179).
The second category concerns three cases of *traditional organised crime* with IT as an important innovative element in the modus operandi. One of these cases concerns an offender group that manipulates the handling of incoming containers by means of a hack in the network of a port terminal (case 151). A second case concerns people involved in a dark web market through which drugs are traded, among other things (case 152). The final case revolves around a modern variant of money laundering. It entails bitcoin exchangers who helped their customers exchange bitcoins for cash anonymously. Available information indicated that these customers earned their bitcoins via online drug trafficking (case 173).
The third category comprises two cases of *organised low-tech cybercrime*. One case concerns a variant of 'skimming' (also known as 'shimming') in which the magnetic strip of a bank card is not copied; instead, the data traffic between the so-called EMV chip on the card and the terminal in which it is used is intercepted (case 154). A second case concerns phishing operations, in which criminals seek to obtain people's online banking credentials, among other things (case 156).
Finally, the fourth category includes two cases of *organised high-tech cybercrime*. Both cases focus on banking malware, i.e. criminals manipulate payments made via internet banking through malicious software (cases 153 and 155).

Conclusions

Criminal cooperation and the use of IT

Previous reports based on the DOCM, which focused entirely on traditional, non-IT-related organised crime, provided a clear picture of criminal networks engaged in 'transit crime', international smuggling activities in which the Netherlands can be either a country of destination, a transit country, or a production country (Kleemans et al., 2002). Analyses of the traditional cases of organised crime studied in the fifth and most recent round of the DOCM do not produce different results in terms of composition and structure. Although there is no mafia-like pyramidal organisational structure, the criminal networks may be more or less structured, with key players and facilitators on whom others depend. There is also a well-known pattern in terms of involvement mechanisms in these cases. Existing social relationships, such as family and friendships, are crucial to the formation and growth of criminal networks. Where existing social relationships fail, 'outsiders' are deployed (Kleemans & Van de Bunt, 1999).
In cases of traditional organised crime as well as in cybercrime cases, we see that most networks have a more or less stable group of core members who work together over a longer period. There are also more and less important suspects and dependency relationships within most networks.

[73] We thank Geralda Odinot, Maite Verhoeven, Ronald Pool, and Christianne de Poot for sharing five cases related to cybercrime (Odinot et al., 2017).

Cybercrime cases are characterised by the importance of technical knowledge and skills. Interestingly, core members of cybercrime networks in our cases often do not have much technical knowledge themselves. However, they do know how to find technically capable facilitators. In the case of low-tech cybercrime (phishing, skimming), criminals make use of their contacts in the offline criminal environment; by contrast, in high-tech cybercrime cases (banking malware), core members acquire the necessary technical expertise through the use of internet forums. The search for technical knowledge thus takes place via offline interactions in the former case and via online interactions in the latter case.
In general, it is clear from the cases in the fifth round of the DOCM that offline social contacts play an important role in involvement mechanisms. Core members in particular know each other due to their network in the offline world and share, for example, the same local and/or social background (see also Lusthaus & Varese, 2017). Money mules are sometimes found in their home environment as well. However, there are also examples where social media platforms and online games are used to make contacts. As we have seen, especially in high-tech cybercrime networks, online forums play an important role in finding technical expertise that is lacking among the core members.

Logistics and the use of IT
Every form of organised crime consists of a logistical process in which a number of necessary steps must be taken (Cornish & Clarke, 2002). An important part of every criminal business process in organised crime is communicating with fellow criminals. This communication is necessary, among other things to coordinate the various partial steps in complex activities such as large-scale international drug trafficking. IT offers criminals important new opportunities in this respect. In various cases, for example, criminals make frequent use of phones with so-called 'PGP encryption' (which stands for: Pretty Good Privacy). Another option used by criminals to reduce the perceived risk of interception is to meet their accomplices at physical locations which they presume to be safe. These 'offender convergence settings' may include catering establishments, commercial premises, or homes.
Furthermore, we analysed the use of IT with regard to specific logistical bottlenecks. An important logistical challenge in various forms of transit crime, such as drug trafficking, is to safely pass contraband across borders. The key role played by IT in controlling and managing traffic flows at airports and seaports has increased the importance to criminals of having access to automated systems. They may obtain such access either through the cooperation of staff or, as in one case, by hacking into the relevant computer networks. One of our cases concerns a group of drug traffickers who recruited IT professionals to hack into the computer network of a container terminal at a large European port (case 151). Keyloggers and malware allowed them to manipulate the time and place of unloading containers. The criminals placed the drugs in a regular cargo container destined for a company that knew nothing about the smuggling, a widely used modus operandi. By using the hack, the criminals were able to collect the container via a dedicated PIN code before the regular company had a chance to do so.
Safely connecting supply and demand in criminal markets is another logistical bottleneck. IT has led to major innovations in this area. For example, buyers and suppliers of drugs can meet anonymously behind a computer screen. On a dark web market they can carry out transactions by using a cryptocurrency such as bitcoin, which is anonymous to a certain extent as well. Case 152 focuses on a dark web market where drugs were traded, among other things. After an online transaction is concluded, the drugs are sent by post. However, some transactions and deliveries, especially those involving larger quantities, are carried out during a physical meet-

ing with a customer. The Dutch drug traffickers who operate on this dark web market seem to focus mainly on nearby European countries (see also Kruithof et al., 2016).
Finally, digitisation has also increased the potential reach of criminals to commit payment fraud. Cases 153 and 155 (both banking malware), 154 (skimming/shimming) and 156 (phishing) belong to this type of offence. Cybercriminals, especially where it involves a phishing email or banking malware attack, can target many victims at once and wait to see who does or does not take the bait. However, cashing the proceeds –which is the last link in the logistics chain of phishing or banking malware attacks –is still a largely physical process. Often, money mules are used in these cases, who make their accounts available so the money of a phishing or malware attack victim can be transferred to them. The money is then withdrawn from the money mule account in cash (see also the section on 'Money flows and the use of IT'). This cashing process proofs to be a bottleneck. For this reason, money mules run a high risk, as banks are alert to this trick and the types of transactions associated with it.

Money flows and the use of IT
For an important part, criminal money flows often seem to remain invisible to investigators, both in cases of traditional organised crime and in cases of cybercrime. Nevertheless, the 30 cases analysed also generate important insights into this area. As regards the spending of criminal proceeds, in terms of both consumption and investment (assets found), the analyses show neither major differences compared to previous research nor major differences between traditional crime and cybercrime. Earlier research showed that organised crime offenders predominantly invest in their country of origin or in their country of residence, which investments consist of tangible, familiar assets such as residences, other real estate, and mostly small companies. In many cases, the available information indicated that the companies in which offenders invest were used for criminal activities such as transport or money laundering (Kruisbergen et al., 2015). Analyses of the 30 cases in the fifth round of the DOCM produce similar results. Investments in the legal economy often concern real estate and companies, much of which is used by offenders to facilitate their criminal operations. Offenders mainly invest in companies within well-known sectors such as wholesale and retail, hotels and restaurants, and transport. Some cybercrime cases include offenders who are involved in IT-related companies.
When it comes to concealing criminal earnings, we do see important differences between traditional organised crime on the one hand and IT-related crime on the other. The 23 cases in the area of traditional organised crime include various money laundering arrangements as described in previous publications, such as the concealment and transfer of cash. We also see more complex money laundering constructions, such as faking legal profit or salary, loan-back schemes, or the channelling of money through foreign legal entities (Kruisbergen et al., 2012). In addition to the 'traditional' ways of money laundering, use can also be made of new payment methods enabled by IT, such as cryptocurrencies and prepaid cards. In principle, a cryptocurrency such as bitcoin is not only useful for cybercriminals. For example, criminals who are active in traditional, offline drug trafficking could use the purchase of bitcoins either in a construction to protect their money flows from detection or as a speculative investment. In the 23 cases of traditional organised crime, however, we do not see the use of bitcoins or other cryptocurrencies (although in one of the cases the criminals made use of prepaid cards (case 165)).
In IT-related crime, unlike many forms of traditional organised crime, the proceeds are often digital in nature. People selling drugs on a dark web market (case 152) often receive the proceeds of their merchandise in a cryptocurrency such as bitcoin.

The perpetrators of phishing and malware attacks (cases 153, 155 and 156) gain control over the online payment transactions of their victims, which take place in digital euros. In the cyber cases that we analysed, these euros were subsequently withdrawn in cash through the use of money mules, or they were subsequently used for the purchase of bitcoins, WebMoney, prepaid cards/vouchers and/or goods, among other things. The use of new forms of money laundering in these cases also involves the use of 'new' services, facilitators and straw men, such as bitcoin 'mixing services', which conceal the link between the sending and receiving address of bitcoins, money mules, and bitcoin exchangers.
The central role of cash is a predominant shared feature of the cases that we studied, in the field of both traditional and IT-related organised crime. Criminals hide cash, make sure that cash ends up in other countries, and buy expensive goods and services with cash. It is striking that cash also plays a dominant role in cybercrime cases (see also Europol, 2015; Oerlemans et al., 2016). For example, we see offenders of phishing and banking malware attacks using money mules to cash their digital euros. Furthermore, we see criminals who earn bitcoins from online drug trafficking exchanging at least part of their cryptocurrency for cash euros, for which they rely on private bitcoin exchangers.

Synthesis
IT brings new possibilities for organised crime. Offenders use these possibilities for purposes of criminal cooperation, for logistics, and for handling money flows.
IT expands the horizon for criminals who are looking for victims, accomplices, tools or clients. The internet allows criminals involved in banking malware, for example, to cast a very wide net in their search for potential victims. Furthermore, criminals looking for specific knowledge or tools can find them through criminal meeting places on the internet. In effect, IT leads to new forms of collaboration. Drug suppliers and consumers also find marketplaces on the dark web that in principle lack physical and social boundaries. Contacts in the offline world and close social relationships therefore seem less important, as it becomes easier to find people, expertise and resources. Trust in the capacities of such a person as an online drug provider is still essential, so people make use of the possibilities offered by the internet to check the reputation of resources (Holt et al., 2015; Decary-Hétu & Dupont, 2013; Soudijn & Monsma, 2012).
Criminals also use the opportunities IT offers them to 'safely' communicate with each other. Technological developments have made encrypted communication accessible to everyone, including criminals who are active in traditional, offline forms of organised crime (see also Schuppers et al., 2016). Freely accessible hardware and software for shielded communications offer an important advantage for criminals who want to coordinate matters between themselves without the police being able to intercept them (as far as they can tell).
In addition, IT has led to new ways of working in more or less traditional activities such as drug smuggling as well, at least in a case where criminals hacked into a computer network to manipulate the collection of a container in which drugs were hidden.
Finally, IT-enabled features such as cryptocurrencies are also a major innovation. Cryptocurrencies offer a certain degree of anonymity and are the means of payment on dark web markets. Together with the TOR networks on which dark web markets operate, a currency such as bitcoin makes it possible for buyers and sellers of illegal goods and services to engage in more or less anonymous transactions.
In sum, IT is indeed used by organised crime groups, which changes their operations to some extent. However, traditional organised crime is in many ways still rather 'traditional', at least in our cases. For example, there are no indications of a

fundamental change in the way offline criminal networks develop. Nor does the logistical process of such criminal activities as drug smuggling seem to have changed significantly in our analysed cases, despite the innovative working method in one case. Furthermore, we only saw the use of cryptocurrencies in cases of cybercrime and online drug smuggling. In other words, this financial innovation was absent in the other cases. It is possible that many criminals simply do not need to drastically change or innovate their working methods.

However, what is more interesting – looking at cybercrime – is that cybercrime turns out to have a local dimension. Cybercriminals are to some extent locally embedded. This is interesting because, at least in theory, the internet allows you to defy physical borders. First, in our cybercrime cases, core members of criminal networks often knew each other in the offline world; they live in the same neighbourhood, for example, or meet each other in nightlife. Straw men such as money mules are often recruited in the vicinity of the main offenders as well. As a result, the resources of social capital used for participation in these cases of organised cybercrime consist to a large extent of offline interactions.

Second, in the dark web market that we studied, part of the transactions took place offline, particularly transactions concerning larger quantities of drugs. In addition, online transactions often concerned vendors sending packages of drugs to buyers living in nearby countries (see also Kruithof et al., 2016). Perhaps these drug traffickers considered the risks involved in sending items by post to be too high when it comes to larger shipments and distances.

Third, cybercrime offenders or offenders in cyber-related cases use local facilities. We saw bitcoin exchangers who rely on the Wi-Fi facilities of fast-food restaurants (among other places), where they physically meet up with customers who want to change euros for bitcoins.

Perhaps one of the most striking similarities between cybercrime and traditional crime is the preference of offenders for cash. Malware and phishing offenders in our cases as well as online drug traffickers change their digital currencies for cash, at least in part. This process is probably also one of the most important bottlenecks in these types of criminal operations, because changing digital currencies for cash in many cases produces some sort of trace or paper trail.

Policy implications

Regulation of cryptocurrency and related services?

The occurrence and investigation of new criminal working methods could raise the question of whether existing laws and regulations are properly equipped to deal with the new situation. This fact applies to the criminal use of cryptocurrency, for instance. Bitcoins and other variants are largely unregulated at the current time. This report, and previous publications, describe how offenders use such innovation. It is not only the cryptocurrency itself, but also related services that largely bypass financial regulation and supervision at this time. As a result, bitcoin exchangers are not subject to a reporting obligation within the framework of the Anti-Money Laundering and Anti-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme, Wwft), for example.

Regulation and supervision could provide tools to combat money laundering through cryptocurrency. For instance, Dutch online exchange offices such as the bitcoin exchangers could be brought under the scope of the Dutch supervisory bodies. This process can reduce the opportunities to launder money through cryptocurrency. Regulation, however, could also have disadvantages from an anti-money-laundering perspective. Cryptocurrency is currently not very widely accepted in the mainstream

economy. Regulation could contribute to the 'normalisation' of cryptocurrency and a higher degree of acceptance of cryptocurrency as a means of payment. This, in turn, could increase the opportunities by which cryptocurrency obtained through criminal activities might be 'laundered', or transferred to the mainstream economy (see Oerlemans et al., 2016).

Criminal investigation

Inherently vulnerable technology

The shielding possibilities offered to criminals by IT and the international aspect of cybercrime make the fight against organised crime more difficult. However, even cybercriminals and perpetrators who use IT to carry out their criminal activities leave traces and/or are vulnerable to countermeasures in another way (see also Odinot et al., 2017; Oerlemans et al., 2016).

First, anonymity on the internet has its own limitations. For example, internet traffic is often registered in one way or another, even though the registrations are not always directly accessible to third parties. Even the transaction history of bitcoins is recorded. An obstacle to detection is that the people behind specific bitcoin addresses are often using pseudonyms. By analysing transaction data and linking it to other sources, and because of the suboptimal behaviour of users, certain transactions can still be traced back to individuals (Meiklejohn et al., 2013; Ron & Shamir, 2013; Oerlemans et al., 2016). In short, a lack of anonymity is sometimes ingrained in the technology used.

Second, even technology which is presumed to be 'watertight' does not guarantee that offenders are shielded from the police. This fact is apparent from the investigation into Ennetcom, for instance. Ennetcom was a key provider of encrypted communication which, at least according to the Public Prosecution Service (Openbaar Ministerie, OM), was widely used by criminals. In 2016, the Public Prosecution Service gained access to enormous amounts of data from the server used by Ennetcom. Ennetcom customers used modified smartphones (Blackberries) which had encryption software (Pretty Good Privacy) installed. This software allowed users of these smartphones to 'safely' communicate with each other. The police, however, managed to come by the 'key' to the messages that were sent through Ennetcom. During the criminal investigation a copy was made of the server, among other things. According to the police, the decrypted information from the server gave them access to millions of messages, which up until then had been hidden from police investigations. The information obtained in this way would prove to be useful in a large number of investigations into serious crimes.

Third, the same characteristics that make a technology attractive to criminals can in some cases provide the police with tools to tackle those same criminals as well. An example is the level of anonymity offered on dark web markets, which makes these marketplaces attractive to providers of prohibited goods, but also provides a good cover for investigating officers (see also EMCDDA, 2016). As a result, criminals operating online are vulnerable to detection methods originally developed for the offline world, such as undercover operations. Our own case material provides an example of a successful undercover operation against criminals who were active on a dark web market. There are more examples, including the police intervention against Hansa Market.[74] Such undercover operations damage the mutual trust between buyers and sellers that is essential for the functioning of dark web markets (see also Kruithof et al., 2016).

[74] www.politie.nl/en/news/2017/july/20/underground-hansa-market-taken-over-and-shut-down.html

Online-offline interfaces
IT is a crucial part of contemporary society. Moreover, IT plays at least a minor role in many types of organised crime as well, even if only because offenders use modern communications technology. To this end, knowledge of IT and IT-related investigation tools are important for investigating both traditional and cybercrime. However, the interface between the online and offline worlds works both ways. As our study of cases shows, the modus operandi of cybercriminals has a significant local dimension. In the cases of cybercrime and other types of IT-related crime we studied, it turned out that one or more essential links in the criminal operations took place in the physical, offline world. For instance, we saw key players who shared the same social and local origins, offenders who recruited frontmen from their local environment, bitcoin exchangers who serviced their customers from Wi-Fi-enabled public places, and online drug dealers who relied on regular postal delivery. Because of this local dimension, new manifestations of crime not only require new powers or specific technical investigation tools, but they also provide many leads for more classical methods.

Financial investigation
Since the last decades, organised crime control policies have become supplemented with a financial approach, i.e. financial investigation, the prevention of and fight against money laundering, and the confiscation of criminal earnings (see also Kruisbergen, 2017). This approach is fruitful in the case of IT-related crime as well. First, criminals who operate online are usually motivated by financial gain as well. Second, particularly the cashing in or exchanging of proceeds in various forms of IT-related crime, is a stage in the criminal business process at which criminals are vulnerable, because they come into direct or indirect contact with the offline world. This fact applies to offenders in phishing and banking malware cases, for example, who want to exchange their digital euros for cash. It also applies to drug traffickers who want to exchange their cryptocurrency, which they earned on the dark web, for cash euros. Third, a financial approach can offer a new perspective on certain aspects of cybercrime groups. For example, investigating money flows can lead to new suspects, while information on the distribution of criminal proceeds can reveal which criminals provide crucial services in criminal networks. A financial perspective, therefore, can teach us a lot, particularly in view of the fact that relatively little is known about money flows in cybercrime cases.

The situational approach: putting up barriers
The monitor reports that have been published to date all demonstrate how closely organised crime is interwoven with its social environment. The situational approach to organized crime, instead of focusing on offenders, focuses on the environmental factors that make the occurrence of crime possible. In the various IT-related forms of organised crime that are discussed in this report, offenders also use people or facilities in their surroundings, such as banks. For instance, the perpetrators of phishing or banking malware attacks find their victims among the account holders at ordinary banks. For this reason, banks play a vital role in preventing and combating various types of crime. Banks are aware of this role and participate in the Electronic Crimes Task Force (ECTF), which is a collaboration between banks, the police and the Public Prosecution Service. Figures published for fraud committed through Internet banking and skimming have fallen significantly in recent years, probably due in part to banks initiating measures and campaigns to detect and prevent these crimes. The banks also play an important role in combating money laundering. Bank accounts are used to transfer and cash in criminal earnings or to convert cryptocurrency into regular currency. Banks can report transactions from specific accounts

which could indicate banking fraud or money laundering. As can be seen from our case study material, these reports are beneficial to tackling these criminal activities. The importance of the action taken by the banks is evidenced by the significant reduction in the amount lost through Internet banking fraud and by the investigations into money laundering initiated after a report of a bank. Given the central position of the banks and the dynamics in the modi operandi of the offenders, banks continue to play an important role in preventing and combating organised crime.
Banks, money mules (and other ways of channelling money), and cryptocurrency exchange services are crucial to certain forms of crime. The latter two services may exist because many offenders prefer cash even in the world of digital crime. In this regard, the approach to IT-related crime can profit from general measures against cash money flows within organised crime. The case study material gives rise to assume that a significant proportion of the money earned by illegal means is still finding its way into regular economy in the form of cash. Offenders spending their money are facilitated, intentionally or unintentionally, by providers allowing expensive goods or services to be paid for in cash ('concealed consumption'). Because of the dominant role played by cash in offline and online crime, making this concealed consumption more difficult could be an effective contribution to combating criminal money flows.
Other examples of services and service providers that play an intentional or unintentional role in the offenders 'working methods are postal companies', 'mixing services' for cryptocurrency, providers of equipment and software for shielded communications, and online meeting places where technical expertise need for specific crimes can be found. Identifying these and other services vital to the offenders is not only important for the prevention of organised crime. It is also important for the investigation of organised crime. Usually, the number of potential suspects in investigations into IT-related crime is larger than available capacity allows for (just as with traditional organised crime). As a result, choices have to be made. Targeted investigation of facilitators can temporarily or permanently disrupt criminal processes. Moreover, it sends a message to those who provide similar services and who profess ignorance of their clients 'intentions, certainly when it involves relatively new types of services.

Our analyses of criminal investigations show that even IT-related crime has important interfaces with the offline world and is partly reliant on the mainstream environment just as traditional organised crime. On the one hand, this conclusion implies that the distinction between cybercrime and traditional organised crime is not as clear-cut as some might assume. On the other hand, it indicates that more traditional investigation methods and a situational approach provide useful opportunities in the approach to IT-related crime in addition to technical tools.

References

Boerman, F., Grapendaal, M., Nieuwenhuis, F., & Stoffers, E. (2017). *Nationaal dreigingsbeeld 2017: Georganiseerde criminaliteit*. Zoetermeer: Nationale Politie, Landelijke Eenheid, Dienst Landelijke Informatieorganisatie.

Bulanova-Hristova, G., Kasper, K., Odinot, G., Verhoeven, M., Pool, R., Poot, C. de, Werner, W., & Korsell, L. (red.) (2016). *Cyber-OC – Scope and manifestations in selected EU member states.* Wiesbaden : Bundeskriminalamt.

Bunt, H.G. van de (2007). Muren van stilzwijgen. In H.G. van de Bunt, P. Spierenburg & R. van Swaaningen (red.), *Drie perspectieven op sociale controle* (pp. 133-136). Den Haag: Boom Juridische Uitgevers.

Bunt, H.G. van de (2010). Walls of secrecy and silence: The Madoff case and cartels in the construction industry. *Criminology and Public Policy*, *9*(3), 435-453.
Bunt, H.G. van de, & Kleemans, E.R., m.m.v. Poot, C.J. de, Bokhorst, R.J., Huikeshoven, M., Kouwenberg, R.F., Nassou, M. van, & Staring, R. (2007). *Georganiseerde criminaliteit in Nederland: Derde rapportage op basis van de Monitor Georganiseerde Criminaliteit*. Den Haag: Boom Juridische uitgevers. Onderzoek en beleid 252.
Cornish, D.B., & Clarke, R.V. (2002). Analyzing Organized Crimes. In A.R. Piquero & S.G. Tibbetts (eds.), *Rational Choice and Criminal Behavior: Recent Research and Future Challenges* (pp. 41-64). New York: Garland.
Décary-Hétu, D., & Dupont, B. (2013) Reputation in a dark network of online criminals. *Global Crime*, *14*(2-3) 175-196.
EMCDDA (European Monitoring Centre for Drugs and Drug Addiction) (2016). *The internet and drug markets*. Luxemburg: Publications Office of the European Union.
Europol (European Police Office) (2015). Why is cash still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering. *Trends in Organized Crime*, *18,* 355-379.
Holt, T.J., Smirnova, O., Chua, Y.T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime 16*(2), 81-103.
Kleemans, E.R., Berg, E.A.I.M. van den, & Bunt, H.G. van de, m.m.v. Brouwers, M., Kouwenberg, R.F., & Paulides, G. (1998). *Georganiseerde criminaliteit in Nederland: Rapportage op basis van de WODC-monitor*. Den Haag: WODC. Onderzoek en beleid 173.
Kleemans, E.R., Brienen, M.E.I., & Bunt, H.G. van de, m.m.v. Kouwenberg, R.F., Paulides, G., & Barensen, J. (2002). *Georganiseerde criminaliteit in Nederland: Tweede rapportage op basis van de WODC-monitor*. Den Haag: Boom Juridische uitgevers. Onderzoek en beleid 198.
Kleemans, E.R., & Bunt, H.G. van de (1999). The social embeddedness of organized crime. *Transnational Organized Crime*, *5*(1), 19-36.
Kruisbergen, E.W. (2017). *Combating organized crime: A study on undercover policing and the follow-the-money strategy*. Amsterdam: Vrije Universiteit.
Kruisbergen, E.W., Bunt, H.G. van de, & Kleemans, E.R. (2012). *Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit*. Den Haag: Boom Lemma. Onderzoek en beleid 306.
Kruisbergen E.W., Kleemans E.R., & Kouwenberg R.F. (2015). Profitability, power, or proximity? Organized crime offenders investing their money in legal economy. *European Journal on Criminal Policy and Research*, *21*(2), 237-256.
Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). *Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands*. Santa Monica, CA/Cambridge, VK: Rand Corporation**.**
Lavorgna, A. (2013). *Transit crimes in the Internet age: How new online criminal opportunities affect the organization of offline transit crimes*. University of Trento. Doctoral School of International Studies.
Leukfeldt, E.R. (red.) (2017). *Research agenda the human factor in cybercrime and cybersecurity*. Den Haag: Eleven International Publishing.
Leukfeldt, E.R., A. Lavorgna, & E.R. Kleemans (2017a). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research*, *23*(3), 287-300.
Leukfeldt, E.R., Kleemans, E.R., & Stol, W.P. (2017b). A typology of cybercriminal networks: From low tech locals to high tech specialists. *Crime, Law and Social Change*. DOI: 10.1007/s10611-016-9646-2.

Leukfeldt, E.R., Kleemans, E.R., & Stol, W.P. (2017c). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology*. DOI:10.1093/bjc/azw009.
Leukfeldt, E.R., Kleemans, E.R., & Stol, W.P. (2017d). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change*. DOI: 10.1007/s10611-016-9647-1.
Lusthaus, J., & Varese, F. (2017). Offline and local; The hidden face of cybercrime. *Policing: A Journal of Policy and Practice*. Doi.org/10.1093/police/pax042
Meiklejohn, S., Pomarole, M., Jordan, G. Levchenko, K., McCoy, D., Voelker, G.M., & Savage, S. (2013). *A fistful of bitcoins: Characterizing payments among men With no names*. San Diego: University of California. Geraadpleegd april 2018: http://dx.doi.org/10.1145/2504730.2504747.
Morselli, C. (2009). *Inside criminal networks*. New York: Springer.
Odinot, G., Verhoeven, M.A., Pool, R.L.D., & De Poot, C.J. (2017). *Organised cybercrime in the Netherlands: Empirical findings and implications for law enforcement*. Den Haag: WODC. Cahier 2017-1.
Oerlemans, J.J., Custers, B.H.M., Pool, R.L.D., & Cornelisse, R. (2016). *Cybercrime en witwassen: Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware*. Den Haag: Boom criminlogie. Onderzoek en beleid 319.
Przepiorka, W., Norbutas, L., & Corten, R. (2017). Order without law: Reputation promotes cooperation in a cryptomarket for illegal drugs. *European Sociological Review*, DOI 10.1 093/esr/jcx072.
Ron, D., & Shamir, A. (2013). Quantitative analysis of the full bitcoin transaction graph. *Financial cryptography and data security*, *7859*, 6-24.
Schuppers, K. Rombouts, N., Zinn, P., & Praamstra, H. (2016). *Cybercrime en gedigitaliseerde criminaliteit: Nationaal dreigingsbeeld 2017*. Driebergen: Nationale Politie.
Soudijn, M.R.J., & Monsma, E. (2012). Virtuele ontmoetingsuimtes voor cybercriminelen. *Tijdschrift voor Criminologie 54*(4), 349-360.
Töttel, U., Bulanova-Hristova, G., & Flach, G. (eds.) (2016). *Research conferences on organised crime at the Bundeskriminalamt in Germany, Volume III, Transnational Organised Crime, 2013–2015*. Wiesbaden: Bundeskriminalamt. Available at: www.polizei.de/SharedDocs/Downloads/EN/Publications/Other/ResearchConferencesOnOrganisedCrime2013-2015.html).
Wingerde, C.G. van, & Bunt, H.G. van de (2017). *Geëiste en opgelegde straffen bij de strafrechtelijke afhandeling van georganiseerde criminaliteit: Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit*. Apeldoorn: Politie & Wetenschap.

Literatuur

Ablon, L., Libicki, M.C., & Golay, A.A. (2014). *Markets for cybercrime tools and stolen data: Hackers' bazaar.* RAND: www.rand.org.

Aldridge, J., & Décary-Hétu, D. (2014). *Not an 'eBay for drugs': The cryptomarket 'Silk Road' as a paradigm shifting criminal innovation*. http://ssrn.com/abstract=2436643, geraadpleegd april 2018.

Algemene Rekenkamer (2014). *Bestrijden witwassen: Stand van zaken 2013*. Den Haag: Algemene Rekenkamer.

Bernaards, F, Monsma, E., & Zinn, P. (2012). *High tech crime criminaliteitsbeeldanalyse 2012*. Woerden: Korps landelijke politiediensten, Dienst Nationale Recherche.

Bernasco, W. (red.) (2010). *Offenders on offending: Learning about crime from criminals*. Cullompton, Devon: Willan Publishing.

Bijlenga, N., & Kleemans, E.R. (2017). Criminals seeking ICT-expertise: an exploratory study of Dutch cases. *European Journal of Criminal Policy and Research*. https://doi.org/10.1007/s10610-017-9356-z

Boerman, F., Grapendaal, M., Nieuwenhuis, F., & Stoffers, E. (2017). *Nationaal dreigingsbeeld 2017: Georganiseerde criminaliteit*. Zoetermeer: Nationale Politie, Landelijke Eenheid, Dienst Landelijke Informatieorganisatie.

Brå (Brottsförebyggande rådet) [The Swedish National Council for Crime Prevention] (2008). *Criminal assets recovery in Sweden.* English summary of Brå report no. 2008:10. Stockholm: Brå.

Bruinsma, G.J.N. (1996). Georganiseerde misdaad en legale economische sectoren. In F. Bovenkerk (red.), *De georganiseerde criminaliteit in Nederland:* Het criminologisch onderzoek voor de parlementaire enquêtecommissie opsporingsmethoden in discussie (pp. 125-132). Deventer: Gouda Quint.

Bruinsma, G.J.N., & Bovenkerk, F. (1996). Inleiding. In G.J.N. Bruinsma & F. Bovenkerk (red.), *De georganiseerde criminaliteit in Nederland: Branches* (pp. 2-8). Den Haag: SDU.

Buehn, A., & Schneider, F. (2013). A preliminary attempt to estimate the financial flows of transnational crime using the MIMIC method. In B. Unger & D. van der Linde (red.), *Research Handbook on Money Laundering* (pp. 172-189). Cheltenham, UK/Northampton, MA: Edward Elgar.

Bulanova-Hristova, G., & Kasper, K., (2016). Cyber-OC in Germany. In G. Bulanova-Hristova, K. Kasper, G. Odinot, M. Verhoeven, R. Pool, C. de Poot, W. Werner, & L. Korsell (red.), *Cyber-OC – Scope and manifestations in selected EU member states* (pp. 165-220). Wiesbaden: Bundeskriminalamt.

Bulanova-Hristova, G., Kasper, K., Odinot, G., Verhoeven, M., Pool, R., Poot, C. de, Werner, W., & Korsell, L. (red.) (2016). *Cyber-OC – Scope and manifestations in selected EU member states.* Wiesbaden : Bundeskriminalamt.

Bullock, K., Clarke, R.V., & Tilly, N. (2010) (red.). Situational prevention of organised crimes. Cullompton: Willan.

Bullock, K., Mann, D., Street, R., & Coxon, C. (2009). *Examining attrition in confiscating the proceeds of crime*. Londen: Home Office.

Bunt, H.G. van de (2007). Muren van stilzwijgen. In H.G. van de Bunt, P. Spierenburg & R. van Swaaningen (red.), *Drie perspectieven op sociale controle* (pp. 133-136). Den Haag: Boom Juridische Uitgevers.

Bunt, H.G. van de (2010). Walls of secrecy and silence: The Madoff case and cartels in the construction industry. *Criminology and Public Policy*, *9*(3), 435-453.

Bunt, H.G. van de, & Kleemans, E.R. (2000). De WODC-monitor georganiseerde criminaliteit. In H. Moerland & B. Rovers (red.), *Criminaliteitsanalyse in Nederland* (pp. 263-276). Den Haag: Elsevier Bedrijfsinformatie.
Bunt, H.G. van de, & Kleemans, E.R., m.m.v. Poot, C.J. de, Bokhorst, R.J., Huikeshoven, M., Kouwenberg, R.F., Nassou, M. van, & Staring, R. (2007). *Georganiseerde criminaliteit in Nederland: Derde rapportage op basis van de Monitor Georganiseerde Criminaliteit*. Den Haag: Boom Juridische uitgevers. Onderzoek en beleid 252.
Bunt, H.G. van de, & Siegel, D. (red.) (2009). *Ondergronds bankieren in Nederland*. Den Haag: Boom.
Cabana, P.F. (2014). Improving the recovery of assets resulting from organised crime. *European Journal of Crime, Criminal Law and Criminal Justice*, *22*(1), 13-32.
Chiu, Y. N., Leclerc, B., & Townsley, M. (2011). Crime script analysis of drug manufacturing in clandestine laboratories: Implications for prevention. *The British Journal of Criminology*, *51*(2), 355-374. DOI: 10.1093/bjc/azr005.
Christin, N. (2012). *Traveling the Silk Road: A measuretnent analysis of a large anonymous online marketpiace*. Pittsburgh, PA: Carnegie Mellon University.
Chu, B., Holt, T.J., & Ahn, G.J. (2010). *Examining the creation, distribution, and function of malware on-line.* Z.pl.: Z.uitg. Technical Report for National Institute of Justice. NIJ Grant No. 2007-IJ-CX-0018.Geraadpleegd april 2018: www.ncjrs.gov/pdffiles1/nij/grants/230112.pdf
Clarke, R.V. (1997). Introduction. In: R.V. Clarke (red.), *Situational Crime Prevention: Successful Case Studies* (pp. 1-43). Guilderland, NY: Harrow and Heston.
Cornish, D.B. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies*, *3*, 151-196.
Cornish, D.B., & Clarke, R.V. (2002). Analyzing Organized Crimes. In A.R. Piquero & S.G. Tibbetts (eds.), *Rational Choice and Criminal Behavior: Recent Research and Future Challenges* (pp. 41-64). New York: Garland.
Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. *Global Crime 13*(3), 160-175.
Décary-Hétu, D., & Dupont, B. (2013) Reputation in a dark network of online criminals. *Global Crime*, *14*(2-3) 175-196.
Décary-Hétu, D., Morselli, C., & Leman-Langlois, S. (2012). Welcome to the scene: A study of social organization and recognition among Warez hackers. *Journal of Research in Crime and Delinquency, 49*(3), 359-382.
Dhanjani, N., & Rios, B. (2008). *Bad sushi: Beating phishers at their own game*. Paper presented at the Annual Blackhat Meetings. Las Vegas, Nevada.
DNB (De Nederlandsche Bank) & Betaalvereniging (2017). *Betalen aan de kassa 2016: Uitkomsten DNB/Betaalvereniging Nederland onderzoek naar het gebruik van contant geld en de pinpas in Nederland in 2016*. Geraadpleegd april 2018: www.dnb.nl/binaries/Factsheet_Betalen_aan_de_kassa_WEB_tcm46-356702.PDF?2017112910
Dupont, B., Côté, A.M., Savine, C., & Décary Hétu, D. (2016). The ecology of trust among hackers. *Global Crime 17*(2), 129-151.
Duyne, P.C. van, & Levi, M. (2005). *Drugs and money: Managing the drug trade and crimemoney in Europe*. Abingdon: Routledge.
ECB (2011). *The use of euro banknotes: Results of two surveys among households and firms*. ECB, Monthly Bulletin, April 2011. Geraadpleegd april 2018: www.ecb.europa.eu/pub/pdf/other/art2_mb201104en_pp79-90en.pdf
EMCDDA (European Monitoring Centre for Drugs and Drug Addiction) (2016). *The internet and drug markets*. Luxemburg: Publications Office of the European Union.

EMCDDA (European Monitoring Centre for Drugs and Drug Addiction) & Europol (2017). *Drugs and the darknet: Perspectives for enforcement, research and policy*. Luxemburg: Publications Office of the European Union.
Europol (European Police Office) (2015a). Why is cash still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering. *Trends in Organized Crime*, *18,* 355-379.
Europol (European Police Office) (2015b). *Why Is cash Still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering*. Den Haag: European Police Office.
Europol (European Police Office) (2016). *Internet Organised Crime Threat Assessment (IOCTA) 2016*. Den Haag: European Police Office.
Faber, W. (2013). Ondermijning als activiteit en als gevolg: Een poging tot duiding van een lastig te definiëren fenomeen. *Finecscience*, 4 februari 2013, 16-22.
Felson, M. (2003). The process of co-offending. In M. J. Smith & D.B. Cornish (red.), *Theory for practice in situational crime prevention (*volume 16*,* pp. 149-168*).* Devon: Willan Publishing.
Felson, M. (2006). *The ecosystem for organized crime*. Helsinki: HEUNI. HEUNI paper nr 26.
Fernández Steinko, A. (2012). Financial channels of money laundering in Spain. *British Journal of Criminology*, *52*(5), 908–931.
FIU-Nederland (2017). *Jaaroverzicht 2016*. Den Haag: FIU-Nederland.
Franklin, J., Paxson, V., Perrig, A., & Savage, S. (2007). *An inquiry into the nature and cause of the wealth of internet miscreants*. Bijdrage gepresenteerd op *CCS07*, 29 oktober - 2 november 2, 2007 in Alexandria, VA.
Grabosky, P. (2007). The Internet, technology, and organized crime. *Asian Journal of Criminology*, *2*(2), 145-161.
Herley, C., & Florencio, F. (2009). *Nobody sells gold for the pPrice of silver: Dishonesty, uncertainty and the underground economy*. Redmond, WA: Microsoft. Microsoft TechReport nr. MSR-TR-2009-34.
Holt, T.J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior 28*(2), 171-198.
Holt, T.J. (2013). Exploring the social organisation and structure of stolen data markets. *Global Crime, 14*(2-3), 155-174.
Holz, T., Engelberth, M., & Freiling, F. (2009). Learning more about the underground economy: A case-study of keyloggers and dropzones. In M. Backes & P. Ning (eds.), *Computer Security-ESCORICS* (pp. 1-18). Berlin/Heidelberg: Springer.
Holt, T.J., & Kilger, M. (2008). Techcrafters and makecrafters: A comparison of two populations of hackers. *2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing, 67-78.*
Holt, J.T., & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies, 23*(1), 33-50.
Holt, T.J., & Smirnova, O. (2014). *Examining the structure, organization, and processes of the international market for stolen data*. Washington: U.S. Department of Justice.
Holt, T.J., Smirnova, O., Chua, Y.T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime 16*(2), 81-103.
Holt, T.J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the Social Networks of Malware Writers and Hackers. *International Journal of Cyber Criminology* (IJCC) *6*(1), 891–903.
Huisman, W. (2017). De aanpak van ondermijnende criminaliteit: oude wijn in nieuwe zakken? *Delikt en Delinkwent*, *5*, 31-38.

Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change*, (1), 1–20.
Hutchings, A., & Holt, T.J. (2015). A Crime Script Analysis of the Online Stolen Data Market. *British Journal of Criminology* 55(3): 596–614.
Kazemier, B., & Rensman, M. (2015). De illegale economie en nationaal inkomen. *Justitiële verkenningn*, *41*(1): 40-53.
Kleemans, E.R. (2014). Theoretical perspectives on organized crime. In L. Paoli (red.), *Oxford handbook of organized crime* (pp. 32-52). Oxford: Oxford University Press.
Kleemans, E.R., Berg, E.A.I.M. van den, & Bunt, H.G. van de, m.m.v. Brouwers, M., Kouwenberg, R.F., & Paulides, G. (1998). *Georganiseerde criminaliteit in Nederland: Rapportage op basis van de WODC-monitor*. Den Haag: WODC. Onderzoek en beleid 173.
Kleemans, E.R., Brienen, M.E.I., & Bunt, H.G. van de, m.m.v. Kouwenberg, R.F., Paulides, G., & Barensen, J. (2002). *Georganiseerde criminaliteit in Nederland: Tweede rapportage op basis van de WODC-monitor*. Den Haag: Boom Juridische uitgevers. Onderzoek en beleid 198.
Kleemans, E.R., & Bunt, H.G. van de (1999). The social embeddedness of organized crime. *Transnational Organized Crime*, *5*(1), 19-36.
Kleemans, E.R., & Poot, C.J. de (2007). *Criminele carrières in de georganiseerde misdaad*. Den Haag: WODC.Cahier 2007-13.
Klerks, P.P.H.M. (2000). *Groot in de hasj: Theorie en praktijk van de georganiseerde criminaliteit*. Antwerpen: Kluwer Rechtswetenschappen.
Koppen, M.V. van (2013). *Pathways into organized crime: Criminal opportunities and adult onset offending*. Amsterdam: Vrije Universiteit.
Korte, L.R. (2017). 'Hitman, at your service': een crime-scriptanalyse van liquidaties in Nederland. *Justitiële verkenningen*, *43*(5), 29-44.
Kruisbergen, E.W. (2017). *Combating organized crime: A study on undercover policing and the follow-the-money strategy*. Amsterdam: Vrije Universiteit.
Kruisbergen, E.W., Bunt, H.G. van de, & Kleemans, E.R. (2012). *Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit*. Den Haag: Boom Lemma. Onderzoek en beleid 306.
Kruisbergen E.W., Kleemans E.R., & Kouwenberg R.F. (2015a). Profitability, power, or proximity? Organized crime offenders investing their money in legal economy. *European Journal on Criminal Policy and Research*, *21*(2), 237-256.
Kruisbergen, E.W., Kleemans, E.R., & Kouwenberg, R.F. (2015b). Wat doen daders met hun geld? Uitkomsten van de Monitor Georganiseerde Criminaliteit. *Justitiële verkenningen*, *41*(1), 84-102.
Kruisbergen, E.W., & Soudijn, M.R.J. (2015). Wat is witwassen eigenlijk? Introductie tot theorie en praktijk. *Justitiële verkenningen*, *41*(1), 10-23.
Kruisbergen, E.W., Kleemans, E.R., & Kouwenberg R.F. (2016). Explaining attrition: Investigating and confiscating the profits of organized crime. *European Journal of Criminology*, *13*(6), 677-695
Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). *Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands*. Santa Monica, CA/Cambridge, VK: Rand Corporation**.**
Lavorgna, A. (2013). *Transit crimes in the Internet age: How new online criminal opportunities affect the organization of offline transit crimes*. University of Trento. Doctoral School of International Studies.
Lavorgna, A. (2014a). Internet-mediated drug trafficking; towards a better understanding of new criminal dynamics. *Trends in Organized Crime*, *17*(4), 250-270.

Lavorgna, A. (2014b). Wildlife trafficking in the Internet age: the changing structure of criminal opportunities. *Crime Science*, *3*(5), 1-12.
Lavorgna, A. (2015a). Organised crime goes online: realities and challenges. *Journal of Money Laundering Control*, *18*(2), 153-168.
Lavorgna, A. (2015b). The online trade in counterfeit pharmaceuticals: New criminal opportunities, trends and challenges. *European Journal of Criminology*, *12*(2), 226-241.
Lavorgna, A., & Sergi, A. (2014). Types of organized crime in Italy: The multi-faceted spectrum of Italian criminal associations and their different attitudes in the financial crisis and in the use of internet technologies. *International Journal of Law, Crime and Justice*, *42*(1), 16-32.
Leukfeldt, E.R. (2014). Cybercrime and social ties: Phishing in Amsterdam. *Trends in Organized Crime 17*(4), 231-249.
Leukfeldt, E.R. (2016). *Cybercriminal networks: Origin, growth and criminal capabilities*. Den Haag: Eleven International Publishers.
Leukfeldt, E.R. (red.) (2017). *Research agenda the human factor in cybercrime and cybersecurity*. Den Haag: Eleven International Publishing.
Leukfeldt, E.R., A. Lavorgna, & E.R. Kleemans (2017a). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research*, *23*(3), 287-300.
Leukfeldt, E.R., Kleemans, E.R., & Stol, W.P. (2017b). A typology of cybercriminal networks: From low tech locals to high tech specialists. *Crime, Law and Social Change*. DOI: 10.1007/s10611-016-9646-2.
Leukfeldt, E.R., Kleemans, E.R., & Stol, W.P. (2017c). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology*. DOI:10.1093/bjc/azw009.
Leukfeldt, E.R., Kleemans, E.R., & Stol, W.P. (2017d). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change*. DOI: 10.1007/s10611-016-9647-1.
Leukfeldt, E.R., Kleemans, E.R., & Stol, W.P. (2017e). The use of online crime markets by cybercriminal networks: a view from within. *American Behavioral Scientist*. DOI 10.1177/0002764217734267.
Leukfeldt, E.R., Poot, C. de, Verhoeven, M., Kleemans, E.R., & Lavorgna, A. (2017f). Cybercriminal networks. In: E.R. Leukfeldt (red.), *Research agenda: The human factor in cybercrime and cybersecurity*. Den Haag: Eleven International Publishers.
Levi, M. (2012). The organization of serious crimes for gain. In M. Maguire, R. Morgan & R. Steiner (red.), *The Oxford handbook of criminology* (5e ed., pp. 595–622). Oxford: Oxford University Press.
Lu, Y., Luo, X., Polgar, M., & Cao, Y. (2010). Social network analysis of a criminal hacker community. *Journal of Computer Information Systems, 51*(2), 31-41.
Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime 13*(2), 71-94.
Lusthaus, J., & Varese, F. (2017). Offline and local; The hidden face of cybercrime. *Policing: A Journal of Policy and Practice*. Doi.org/10.1093/police/pax042
Madarie, R., & Kruisbergen, E.W. (nog te verschijnen). *Traffickers in transit: Analysing the logistics and involvement mechanisms of organised crime at logistical nodes in the Netherlands*. *Empirical results of the Dutch Organised Crime Monitor*.
Malm, A., & Bichler, G. (2013). Using friends for money: The positional importance of money-launderers in organized crime. *Trends in Organized Crime*, *16*(4), 365–381.

Martin, J. (2014a). Lost on the Silk Road: online drug distribution and the 'cryptomarket'. *Criminology & Criminal Justice, 14*(3), 351-367.
Martin, J. (2014b). *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. Basingstoke, VK: Palgrave Macmillan.
Maurtiz, H. (2014). *De aard en omvang van Money Muling: Fraude met internetbankieren en witwassen*. Scriptie, uitgevoerd voor de Nationale Politie.
McAfee Center for Strategic and International Studies (2014). *Net losses: Estimating the Global Cost of Cybercrime. Economic impact of cybercrime II*. Santa Clara, CA: McAfee. www.mcafee.com/nl/resources/reports/rp-economic-impact-cybercrime2.pdf
Meiklejohn, S., Pomarole, M., Jordan, G. Levchenko, K., McCoy, D., Voelker, G.M., & Savage, S. (2013). *A fistful of bitcoins: Characterizing payments among men With no names*. San Diego: University of California. Geraadpleegd april 2018: http://dx.doi.org/10.1145/2504730.2504747.
Meloen, J.D., Landman, R., Miranda, H. de, Eekelen, J. van, & Soest, S. van, m.m.v. Duyne, P.C. van, & Tilburg, W. van (2003). *Buit en besteding: Een empirisch onderzoek nkruitaar de omvang, de kenmerken en de besteding van misdaadgeld*. Zoetermeer: Nationale Recherche Informatie.
Moore T., & Christin N. (2013). Beware the middleman: Empirical analysis of bitcoin-exchange risk. In A.R. Sadeghi (red.), *Financial cryptography and data security, FC 2013, lecture notes in computer science, volume 7859*. Berlin/Heidelberg: Springer.
Morselli, C. (2009). *Inside criminal networks*. New York: Springer.
Naylor, R.T. (1999). Wash-out: A critique of follow-the-money methods in crime control policy. *Crime, Law and Social Change*, *32*(1), 1-58.
NVB (Nederlandse Vereniging van Banken) (2017). *Factsheet Veiligheid en fraude*. Z. pl.:NVB. www.nvb.nl.
Odinot, G., Verhoeven, M.A., Pool, R.L.D., & De Poot, C.J. (2017). *Organised cybercrime in the Netherlands: Empirical findings and implications for law enforcement*. Den Haag: WODC. Cahier 2017-1.
Oerlemans, J.J., Custers, B.H.M., Pool, R.L.D., & Cornelisse, R. (2016). *Cybercrime en witwassen: Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware*. Den Haag: Boom criminlogie. Onderzoek en beleid 319.
OM (Openbaar Ministerie) (2014). *Jaarbericht 2013*. Den Haag: Openbaar Ministerie.
OM (Openbaar Ministerie) (2015). *Jaarbericht 2014*. Den Haag: Openbaar Ministerie.
OM (Openbaar Ministerie) (2016). *Jaarbericht 2015*. Den Haag: Openbaar Ministerie.
OM (Openbaar Ministerie) & Politie (2015). *Verantwoording aanpak georganiseerde criminaliteit 2014*. Den Haag: Openbaar Ministerie.
PEO (Parlementaire Enquêtecommissie Opsporingsmethoden) (1996). *Inzake opsporing: Enquête opsporingsmethoden*. Den Haag: Sdu Uitgevers.
Peretti, K.K. (2008). Data breaches: What the underground world of 'carding' reveals. *Santa Clara Computer and High-technology Law Journal, 25*(2), 345-414.
Przepiorka, W., Norbutas, L., & Corten, R. (2017). Order without law: Reputation promotes cooperation in a cryptomarket for illegal drugs. *European Sociological Review*, DOI 10.1 093/esr/jcx072.
Ron, D., & Shamir, A. (2013). Quantitative analysis of the full bitcoin transaction graph. *Financial cryptography and data security*, *7859*, 6-24.
Schell, B.H., & Melnychuk, J. (2011). Female and male hacker conferences attendees: Their autism-spectrum quotient (AQ) scores and self-reported adulthood experiences. In T.J. Holt & B.H. Schell (red.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 144-168). New York: Information Science Reference.

Schuppers, K. Rombouts, N., Zinn, P., & Praamstra, H. (2016). *Cybercrime en gedigitaliseerde criminaliteit: Nationaal dreigingsbeeld 2017*. Driebergen: Nationale Politie.
Schneider, F., & Windischbauer, U. (2008). Money laundering: Some facts. *European Journal of Law and Economics*, *26*, 387-404.
Sieber, U., & Bögel, M. (1993). *Logistik der Organisierten Kriminalität*. Wiesbaden: Bundeskriminalamt.
Soudijn, M.R.J. (2014). Using strangers for money: A discussion on money-launderers in organized crime. *Trends in Organized Crime*, *17*(3), 199-217.
Soudijn, M.R.J. (2015). Hawala and money laundering: Potential use of red flags for persons offering hawala services. *European Journal on Criminal Policy and Research*, *21*(2), 257–274.
Soudijn, M.R.J. (2017). *Witwassen: Criminaliteitsbeeldanalyse 2016*. Zoetermeer: Politie, Landelijke Eenheid, Dienst Landelijke Informatieorganisatie.
Soudijn, M.R.J. & Akse, Th. (2012). *Witwassen. Criminaliteitsbeeldanalyse 2012*. Driebergen: KLPD, Dienst Nationale Recherche.
Soudijn, M.R.J., & Monsma, E. (2012). Virtuele ontmoetingsuimtes voor cybercriminelen. *Tijdschrift voor Criminologie 54*(4), 349-360.
Soudijn, M.R.J., & Reuter, P. (2016). Cash and carry: The high cost of currency smuggling in the drug trade. *Crime, Law and Social Change,* 66(3), 271–290. DOI 10.1007/s10611-016-9626-6.
Soudijn, M.R.J., & Zegers, B.C.H.T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime 15*(2-3), 111-129.
Tompson, L., & Chainey, S. (2011). Profiling illegal waste activity: Using crime scripts as a data collection and analytical strategy. *European Journal on Criminal Policy and Research*, *17*(3), 179-201. DOI: 10.1007/s10610-011-9146-y.
Töttel, U., Bulanova-Hristova, G., & Flach, G. (eds.) (2016). *Research conferences on organised crime at the Bundeskriminalamt in Germany, Volume III, Transnational Organised Crime, 2013–2015*. Wiesbaden: Bundeskriminalamt. Beschikbaar als pdf op: www.polizei.de/SharedDocs/Downloads/EN/Publications/Other/ResearchConferencesOnOrganisedCrime2013-2015.html).
Verhage, A. (2009). Between the hammer and the anvil? The anti-money laundering-complex and its interactions with the compliance industry. *Crime, Law and Social Change*, *52*(1), 9-32.
Vettori, B. (2006). *Tough on criminal wealth: Exploring the practice of proceeds from crime confiscation in the EU*. Dordrecht: Springer.
Von Lampe, K. (2011). The application of the framework of situational crime prevention to 'organized crime'. *Criminology & Criminal Justice*, *11*(2), 145-163.
Wall, D.S. (2005). The Internet as a conduit for criminals. In A. Pattavina (red.), *Information technology and the criminal justice System* (pp. 77-98). Thousand Oaks, CA: Sage.
Wehinger, F. (2011). The dark net: Self-regulation dynamics of illegal online markets for identities and related services. *Intelligence and Security Informatics Conference*. 10.1109/EISIC.2011.54.
Werner, Y. & Korsell, L. (2016). Cyber-OC in Sweden. In G. Bulanova-Hristova, K. Kasper, G. Odinot, M. Verhoeven, R. Pool, C. de Poot, W. Werner & L. Korsell (red.), *Cyber-OC: Scope and manifestations in selected EU member states* (pp. 101-164). Wiesbaden: Bundeskriminalamt.
Weulen Kranenbarg, M. (2018). *Cyber-offenders versus traditional offenders: An empirical comparison*. Amsterdam: Vrije Universiteit.
Wingerde, C.G. van, & Bunt, H.G. van de (2017). *Geëiste en opgelegde straffen bij de strafrechtelijke afhandeling van georganiseerde criminaliteit: Rapportage in*

het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit. Apeldoorn: Politie & Wetenschap.
Yip, M., Shadbolt, N., & Webber, C. (2012). Structural Analysis of Online Criminal Social Networks. In *IEEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 60-65). Arlington, VA: IEEE.
Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing & Society, 23*(4), 516-539.

Wet- en regelgeving, kamerstukken en ministeriële stukken

Ministerie van Justitie/Ministerie van Binnenlandse Zaken (1996). *Plan van aanpak ter implementatie besluitvorming enquête opsporingsmethoden*. Den Haag: Ministerie van Justitie/Ministerie van Binnenlandse Zaken.
Minister van veiligheid en Justitie (2013). *Bestrijding georganiseerde criminaliteit*. Tweede Kamer, vergaderjaar 2012–2013, 29 911, nr. 79.

Geraadpleegde websites

https://coinmarketcap.com/historical/, geraadpleegd op 9 juni 2017.
http://datanews.knack.be/ict/nieuws/7-miljoen-dollar-aan-ethereum-gestolen-in-online-overval/article-normal-879833.html, geraadpleegd op 31 augustus 2017.
https://fd.nl/beurs/1200322/bitcoin-bereikt-nieuw-hoogtepunt-op-goed-nieuws-uit-japan-en-vs, geraadpleegd op 15 juni 2017.
https://www.politie.nl/nieuws/2017/juli/20/ondergrondse-hansa-market-overgenomen-en-neergehaald.html, geraadpleegd op 15 januari 2018.
https://www.politie.nl/nieuws/2017/maart/9/11-versleutelde-berichten.html, geraadpleegd op 15 januari 2018.
https://www.wmtransfer.com, laatst geraadpleegd op 16 november 2017.
http://www.xe.com/currencycharts/?from=XBT&to=USD&view=10Y, geraadpleegd op 12 juni 2017.
https://youtu.be/TNwhIHqM60g, geraadpleegd april 2018.

Bijlage 1 Samenstelling begeleidingscommissie

Voorzitter	
Mr. F.K.G. Westerbeke	Hoofdofficier Landelijk Parket, Openbaar Ministerie
Leden	
Drs. J.W. van Borselen	Directoraat-Generaal Politie, Ministerie van Justitie en Veiligheid
Mr. drs. J. Dobbelaar	Directoraat-Generaal Rechtspleging en Rechtshandhaving, Ministerie van Justitie en Veiligheid
Dr. A.J.J. Meershoek	Universiteit Twente
W. van der Schaaf MBA	Afdelingshoofd Analyse en Onderzoek, Landelijke Eenheid, Nationale Politie

Bijlage 2 Aandachtspuntenlijst

De gegevens voor de aandachtspuntenlijst worden verkregen door middel van interviews en, vooral, dossieronderzoek. In eerste instantie dienen de betrokken OvJ/ parketsecretaris en/of de teamleider van het onderzoek te worden benaderd. Het gesprek met deze actor(en) dient voor een globaal overzicht van de zaak en dient tevens als inleiding tot het te bestuderen opsporingsdossier.
Hoewel een zaak meerdere deelonderzoeken kan omvatten, wordt per zaak in principe één aandachtspuntenlijst ingevuld. De 'structuur' van de zaak en van de deelonderzoeken kan dan worden aangegeven onder de aandachtspunten 1 en 2. Ook kan daar worden aangegeven dat bepaalde deelonderzoeken om bepaalde redenen beknopter of niet nader zijn geanalyseerd.

De antwoorden dienen kort te worden toegelicht. In zoverre andere bronnen zijn geraadpleegd dient dit apart te worden vermeld. Beweringen die afkomstig zijn uit interviews, dienen zo veel mogelijk op hun betrouwbaarheid te worden getoetst.
Bepaalde informatie kan relevant zijn voor meer dan één aandachtspunt. In dat geval wordt informatie onder ieder relevant aandachtspunt herhaald.
De met een bolletje asterisk (*) aangegeven vermeldingen dienen te worden opgevat als aandachtspunten. Het zijn geen in te vullen categorieën.
Nummer de verdachten en gebruik deze nummering zo veel mogelijk in de tekst (in principe staan er alleen persoons- en bedrijfsgegevens bij de aandachtspunten 3.2 tot en met 3.4).

Probeer zo min mogelijk kwalificerende opmerkingen te maken; laat de feiten zelf spreken. Maak gebruik van typerende citaten uit verhoren of tapgesprekken

Overzicht aandachtspunten

1 Zaakgegevens

- Korte omschrijving (bijv.: Nederlands-Surinaamse groep die zich bezighield met cocaïne-invoer via de haven in Rotterdam of Nederlandse/Duitse/Russische daders die aan ransomware deden):
- Codenaam van de zaak:
- Procesverbaal-nummer:
- Relaties met andere onderzoeken:
- Onderzoekende instantie(s):
- Naam teamleider(s) en officier van justitie:
- Datum start onderzoek:
- Datum opening en sluiting SFO (Financieel gerechtelijk onderzoek) (indien van toepassing):
- Naam onderzoeker(s):

- Data interviews en dossieronderzoek:
- Gegevens van de respondenten (namen, functies, telefoonnummers):
- Andere geraadpleegde bronnen:
- Nog aan te vullen gegevens:
  - Verdachtengegevens (o.a. antecedenten uit JD).
  - Vonnissen (in eerste aanleg en in hoger beroep).
  - *SFO:

2 Overzicht opsporingsonderzoek

Het gaat hierbij om gegevens die relevant zijn voor het interpreteren van de informatie die in het kader van het opsporingsonderzoek is verzameld.

- Wat was de aanleiding tot het onderzoek?
- Hoe is de zaak aan het licht gekomen (CIE-informatie, sporen, aangifte etc.)?
- De strafbare feiten en de verdachten waarop het onderzoek zich heeft gericht.
- Eventuele belangrijke problemen en wijzigingen die zich in het verloop van het onderzoek hebben voorgedaan.
- Noem alle ingezette opsporingsmethoden.
- Noteer van ieder ingezet middel de opbrengsten. Welke methoden heeft veel of juist weinig betrouwbare informatie opgeleverd?
- Is er speciale software gebruikt om grote data bestanden te doorzoeken, categoriseren of analyseren? Zo ja, welke software was dit? En wat was het resultaat van de inzet van de programmatuur?
- Welke relevante personen zijn er wel en niet aangehouden en verhoord, wie zijn er gehoord, et cetera.
- Wat is de reden dat bepaalde personen niet zijn aangehouden of verhoord? (Verblijf in buitenland, verdachte is niet geïdentificeerd?)
- Hebben verdachten verklaringen afgelegd? In hoeverre bekennen ze. Noteer ook of verdachten toegang hebben verleend tot automatische werken door het afgeven van wachtwoorden en dergelijke (geven ze bijv. het wachtwoord voor hun mailbox, werken ze mee aan het ontsleutelen van bestanden etc.).
- Met betrekking tot welke aspecten van de zaak (zoals bijvoorbeeld witwassen, export, import, ontwikkelen van malware) is er veel respectievelijk betrouwbare informatie verzameld?
- Is er in de opsporing sprake geweest van internationale samenwerking? Zo ja, waarom, wanneer en met wie?
- Zijn er rechtshulpverzoeken ingediend? Zo ja, wat was het doel van de aanvraag, wat is het resultaat en wat is de tijdspanne? Noteer ook of aan andere landen verzoeken zijn gedaan tot inzage in e-mails of andere communicatie die is verlopen via een bedrijf/persoon/apparaat dat onder dat land valt (bijvoorbeeld verzoek aan VS tot inzage in mailbox van een hotmailaccount van een verdachte).

3 Het samenwerkingsverband

3.1 Omvang en samenstelling van het criminele samenwerkingsverband

- Totale aantal verdachten.
- Structuur en samenstelling van de groep / het netwerk: hoe zijn de verdachten gerelateerd en wat is hun rol of functie in het samenwerkingsverband.
- (Verschillende gerelateerde (sub)groepen, kernfuncties, belangrijke ondersteunende functies, periferie).

- Met name bij grotere groepen / samenwerkingsverbanden is het belangrijker om de structuur en de samenstelling aan te geven, dan om alle persoonsgegevens van 'perifere' verdachten te noteren (dit is overigens ter beoordeling van degene die de zaak analyseert).

3.2 Hoofdverdachten

Vermeld per verdachte de volgende gegevens (verdachten nummeren):
- Verdachtenummer:
- Naam: (* Voornamen ACHTERNAAM (bijnamen / roepnamen…….))
- Parketnummer(s):
- Geboortedatum:
- Geboorteplaats (geboorteland):
- Geslacht:
- Nationaliteit:
- Woonplaats:
- Beroep:
- Criminele antecedenten:
- ICT-skills:
- Bijzonderheden: (* arbeidsverleden, specialisatie, taal, andere kwalificaties (bijv. ICT)
- Rol in de criminele groep (* inclusief verwantschapsrelaties binnen de groep):

3.3 Andere verdachten

Vermeld de volgende gegevens over de andere verdachte(n) (nummering 3.2 voortzetten):
- Verdachtenummer:
- Naam: (* Voornamen ACHTERNAAM (Bijnamen / roepnamen: ...))
- Geboortedatum:
- Geboorteplaats (geboorteland):
- Geslacht:
- Nationaliteit:
- Woonplaats:
- Beroep:
- Criminele antecedenten:
- ICT-skills:
- Bijzonderheden: (* arbeidsverleden, specialisatie, taal, andere kwalificaties (bijv. ICT)
- Bijzonderheden:
- Rol:

3.4 Overige betrokken personen en bedrijven

Het gaat hierbij om overige betrokken personen en bedrijven, die niet formeel als verdachte zijn aangemerkt, maar die wel betrokken zijn bij het samenwerkingsverband en/of daarvoor een faciliterende functie vervullen, bijvoorbeeld een ICT-bedrijf dat apparatuur verschaft of kennis.
N.B.: Licht de betrokkenheid van deze personen verder toe onder 5.

Nummer de betrokkenen (P1, P2, etc. voor natuurlijke personen en B1, B2, etc. voor bedrijven / rechtspersonen) en vermeld de onderstaande gegevens:

Personen
- Nummer:
- Naam: (* Voornamen ACHTERNAAM (Bijnamen / roepnamen: ...))
- Geboortedatum:
- Geboorteplaats (geboorteland):
- Geslacht:
- Nationaliteit:
- Woonplaats:
- Beroep:
- Rol bij criminele activiteiten:

Bedrijven
- Persoonsnummernummer:
- Naam bedrijf:
- Plaats (land) van vestiging:
- Soort bedrijf:
- Eigenaren / directeuren:
- Rol bij criminele activiteiten:

3.5 Herkomst van de (hoofd)verdachten

Geef kort aan uit welke landen de (hoofd)verdachten afkomstig zijn (en eventueel: uit welke regio/streek/dorp) en uit welke etnische groep (bijvoorbeeld: Turkije, Koerden).
- 'Etnische' bindingen binnen (delen van) het criminele netwerk.
- De mate van 'etnische' geslotenheid respectievelijk openheid van (delen van) het criminele netwerk.

3.6 Ontstaansgeschiedenis en bestendigheid van en verhoudingen, rollen en taken binnen het samenwerkingsverband

Geef een beschrijving van het ontstaan van het samenwerkingsverband, de specifieke rol en kwaliteiten van de (hoofd)verdachten, de taakverdeling binnen de groep, het onderlinge vertrouwen, de duur van de criminele activiteiten en de ontwikkeling van het samenwerkingsverband.
- Banden gebaseerd op familierelaties (specifiek beschrijven!), vriendschapsrelaties, herkomst, beroep, etc.
- Hoe en wanneer is het samenwerkingsverband ontstaan?
- Hebben de leden over het algemeen een criminele achtergrond (en zo ja welke) of juist niet?
- Vertrouwen of achterdocht in de onderlinge relaties? (in offline as well as online relations; if on line, it should be elaborated upon at item 3.8)?
- De structuur van de groep / het netwerk (zelfstandige eenheid of wisselende samenstelling gebaseerd op een specifiek doel, cruciale functies / contacten).
- Hiërarchische verhoudingen en / of wederzijdse afhankelijkheid.
- Plaats/Rol en kwaliteiten van de leider(s) / hoofdpersonen.
- Facilitators / illegale dienstverleners: witwassers, geldwisselaars, ondergrondse bankiers, documentenvervalsers, transporteurs, B.V.-makelaars, etc.
- Plaats en taak van de andere leden binnen het samenwerkingsverband.
- Duur van de activiteiten van het samenwerkingsverband.
- Wisselingen in het samenwerkingsverband.

- Aanwezigheid van geweld, onderlinge conflicten.
- Ontwikkeling van het samenwerkingsverband: 'sneeuwbaleffect' en / of 'rekrutering'.

3.7 Bindingsmechanismen

Wat hield de leden van het samenwerkingsverband bij elkaar en op welke wijze vonden geheimhouding, controle en disciplinering plaats binnen het samenwerkingsverband?

- Sociale relaties: familierelaties (specifiek beschrijven!), vriendschapsrelaties, herkomst, beroep, etc.
- Economisch voordeel en / of immateriële beloningen.
- Gehoorzaamheid uit angst vanwege dreiging met sancties en / of feitelijke geweldpleging. (online/offline)
- Andere bindingsmechanismen.

3.8 De rol van ICT

- Welke rol speelt ICT binnen het samenwerkingsverband (los van de modus operandi)?
- In welke mate vinden de contacten tussen de leden online plaats? Zijn er ook puur online contacten (zonder fysieke contacten)?
- Wat voor soort contacten waren er online? (chat, beslissingen nemen, conflicten, etc?)
- Welke rol heeft ICT gespeeld bij het ontstaan van het samenwerkingsverband?
- Hoe wordt elkaars vertrouwen gewonnen bij online contacten en bij het aangaan van online relaties?
- In welke mate hebben de verschillende leden een ICT-achtergrond en/of ICT-kennis/-kwalificaties?
- Verhouding tussen traditionele criminaliteit en het gebruik van ICT en/of cybercrime: gaat het voor zover om daders die al actief waren in traditionele georganiseerde criminaliteit en later ICT gingen toepassen of niet?
- Zijn de activiteiten mbt het gebruik van ICT belegd bij specialisten of is het meer 'doe het zelf'?
- Zijn er speciaal personen gerekruteerd vanwege zijn/haar ICT skills?
- Andere gevolgen van het gebruik van ICT voor de samenwerking/onderlinge verhoudingen etc?

3.9 De rol van vrouwen

Welke rol speelden vrouwen bij de illegale activiteiten?:

- Vrouwen met een zelfstandige rol (en waaruit blijkt die zelfstandige rol)?
- Logistieke functies (toelichten).
- Afscherming van illegale activiteiten.
- Contacten met de dienstverlenende omgeving en met aanbieders of afnemers van illegale goederen en diensten.

4 Activiteiten en werkwijze

4.1 Primaire activiteiten, modus operandi en werkterrein van de groep / het netwerk

Samenvatting

Geef een toelichting op de voornaamste criminele activiteiten van de groep en op de werkwijze (modus operandi).

- Geleverde goederen (drugs, wapens, voertuigen etc.).
- Bij drugs: o.a. wel of geen specialisatie in bepaalde soorten drugs, de delen van het logistieke proces die men zelf verzorgt en / of uitbesteedt: productie, invoer, doorvoer, uitvoer, distributie.
- Geleverde diensten (prostitutie, witwassen, afscherming, Levering of maken van Botnets, etc.).
- Parasitaire activiteiten (malware, phising, identiteitsfraude, afpersing, mensenhandel, ontvoering, oplichting etc.).
- Logistiek; beschrijf de logistieke processen die ondernomen worden voor de productie, import, doorvoer, distributie.
- Herkomst, bestemming, gebruikte routes.
- Logistieke kenmerken, gebruik logistieke knooppunten (havens, vliegvelden, servers, providers, etc.), hoe worden logistieke knelpunten opgelost?
- Smokkelmethoden, ontduiken controles etc.
- Welke internationale aspecten hebben de illegale activiteiten? (bijvoorbeeld: drugs die vanuit Zuid-Amerika worden geïmporteerd in Nederland en vervolgens worden vervoerd naar Duitsland, of Russische daders die malware ontwikkelen en daarmee slachtoffers in West-Europa aanvallen).
- Relevante marktregelingen: (BTW, accijnzen, afvalverwerking etc.).

De rol van ICT

- Aard/doel gebruik.
- Als ICT in meer traditionele criminaliteit (drugs, mensenhandel etc.) is gebruikt, hoe en waarom? Welk voordeel werd er mee behaald, welk probleem werd er mee opgelost? Leverde het nieuwe problemen op?
- ICT in 'echte' cyberzaken / ICT als doelwit (ransomware, carding, hacken): omschrijving MO.
- Gebruik bij communicatie: TOR-netwerken, middelen als mail, skype, chatfuncties, afgeschermde netwerken.
- Werving mededaders.
- Gebruik bij inkoop.
- Gebruik bij verkoopkanalen.
- Leggen van contacten.
- Witwassen (cryptovaluta, prepaid stored value cards, overig).

4.2 Secundaire activiteiten

Zijn er nog bijzondere, strafbare of niet strafbare nevenactiviteiten te vermelden?

4.3 Indicatie van de materiële en immateriële schade

Geef een indicatie van de aard en de omvang van de materiële en immateriële schade (bij voorkeur op basis van het dossier en / of de interviews, in andere gevallen nadrukkelijk de bron vermelden).

- Schade voor personen (letsel, materiële schade).

- Schade voor landen/overheden, schade aan opsporingsinstanties e.d. (integriteitsverlies, imagoschade, verlies van vertrouwen, niet afgedragen heffingen etc.).
- Schade aan markten, branches (concurrentievervalsing), milieu, schade voor ICT-systemen (directe schade, betrouwbaarheid).
- Indien mogelijk; Een schatting van de omvang van de schade voor Nederland en andere landen (indien mogelijk: per jaar en voor de totale periode waarin men actief was).

5 Contacten met de omgeving

5.1 Contacten met de omgeving (samenvatting)

Geef hier een korte samenvatting (op basis van aandachtspunt 5.2 tot en met 5.9) van de mogelijkheden die de omgeving (buurt, bedrijf, beroep, etc.) biedt aan het criminele samenwerkingsverband en de risico's en geef aan hoe het criminele samenwerkingsverband omgaat met deze mogelijkheden en risico's.

5.2 Contacten met andere criminele groeperingen of daders

Zijn er contacten met andere criminele groeperingen of daders? Beschrijf de aard van de vastgestelde contacten en geef hierbij aan of het contact wordt gekenmerkt door samenwerking of door concurrentie en/of geweld. Hoe komen contacten tot stand; hoe tasten beide partijen elkaar af?
N.B. Geef een indicatie van de betrouwbaarheid van de informatie.
- Facilitators / illegale dienstverleners: witwassers, geldwisselaars, ondergrondse bankiers, documentenvervalsers, transporteurs, B.V.-makelaars, etc.
- Zakelijke relaties.
- Gemeenschappelijke projecten.
- Uitwisseling kennis / menskracht.
- Onderlinge dienstverlening.
- Ruilhandel.
- Territoriale afspraken.
- Geweld (bedreiging, intimidatie, geweldpleging, liquidatie, afpersing, chantage of ontvoering).
- Ontneming goederen (ripdeals).
- Verdeelsleutel van winsten; prijsbepaling.

5.3 Contacten met terroristische en / of separatistische bewegingen

Vermeld de naam van de groeperingen. Beschrijf de aard van de contacten.
N.B. Geef een indicatie van de betrouwbaarheid van de informatie.

5.4 Betrokkenheid van wettige ondernemingen en rechtspersonen

In hoeverre zijn er relaties met wettige bedrijven, welke rol spelen deze wettige bedrijven bij de criminele activiteiten en op welke manier zijn deze bedrijven bewust of onbewust betrokken bij de illegale activiteiten?
- Directe facilitering van illegale activiteiten (o.a. Dekmantel-firma's).
- Geef tevens aan of deze bedrijven bewust voor dit doel zijn opgericht of reeds bestonden voor de aanvang van de illegale activiteiten.
- Actieve samenwerking.

- Meeprofiteren door afname van (te) goedkope goederen, meeprofiteren van creditcardfraude/carding.
- Onbewust een belangrijke rol vervullen voor het criminele samenwerkingsverband.
- ICT-bedrijven.
- Spy-shops.
- Witwassen van misdaadgelden.
- Ontmoetingsplekken en huisvesting.
- Vervoer van goederen en personen.

N.B.: Geef bij meeprofiterende bedrijven aan wat de verhouding was tot het criminele samenwerkingsverband, in welke mate men op de hoogte was of had kunnen zijn van de illegale activiteiten en wat de reden was om mee te werken.

5.5 Corrupte contacten met overheidsfunctionarissen

Beschrijf de individuele contacten met personen werkzaam bij de overheid, politie, justitie, douane etc., die door hun functie bepaalde diensten konden verlenen aan het criminele samenwerkingsverband:
- Het leveren van benodigde middelen zoals vergunningen, paspoorten, visa, vervalste documenten, etc.
- Het omzeilen van controles (bijvoorbeeld: grenscontroles, bordeelcontroles, administratieve controles, etc.).
- Het verstrekken van opsporingsinformatie (bijvoorbeeld: informatie over lopend opsporingsonderzoek of op handen zijnde politieacties).

Beschrijf de aard van de geleverde diensten en beschrijf de mogelijke redenen waarom deze diensten werden geleverd:
- Sociale relaties.
- Economisch voordeel en/of immateriële beloningen.
- Dreiging met sancties en/of feitelijke geweldpleging.
- Andere motieven.

5.6 Contacten met externe deskundigen / specialisten

De mogelijkheid bestaat dat de verdachten regelmatig gebruikmaken van diensten uit de bovenwereld, zonder dat er sprake is van corruptie, pressie of intimidatie. Te denken valt hierbij in de eerste plaats aan personen uit de bankwereld en de vrije beroepsgroepen zoals bijvoorbeeld notarissen, advocaten, belastingadviseurs, beleggers, accountants en makelaars. Daarnaast kan gedacht worden aan andere deskundigen en specialisten, die een schijn van betrouwbaarheid wekken en daarmee een bijdrage leveren aan de afscherming van de illegale activiteiten.

Beschrijf de aard van de geleverde diensten en de mate waarin de externe deskundige zich van zijn bijdrage aan de criminele organisatie bewust was of had moeten zijn.
N.B.: Indien deze deskundige (hoofd)verdachte is, dit ook onder dit aandachtspunt vermelden.

5.7 Overige contacten met de omgeving

Zijn er nog andere contacten met personen uit de omgeving, die van belang zijn voor de uitvoering van de illegale activiteiten?

Beschrijf de aard van de geleverde diensten en de mogelijke redenen waarom deze werden geleverd.
- Sociale relaties.
- Economisch voordeel en/of immateriële beloningen.
- Dreiging met sancties en/of feitelijke geweldpleging.
- Andere motieven.

5.8 Specifieke afschermingsmethoden

Wordt er gebruikgemaakt van één of meer van de onderstaande specifieke afschermingsmethoden? Zo ja, waar blijkt dit dan uit en wat houden deze afschermingsactiviteiten concreet in?
- Verspreiden van valse informatie (nepfacturen, ed.).
- Inbraken.
- Geweld (bedreiging, intimidatie, geweldpleging, afpersing, chantage of ontvoering).
- Liquidaties (n.b.: geef aan hoe hard eventuele vermoedens zijn en wat de mogelijke aanleiding voor de liquidatie(s) is geweest).
- Screenen medewerkers.
- Vernietiging / vervalsing administratie.
- Communicatie – gedrag: beperking informatie-uitwisseling (o.a. Codetaal).
- Communicatie – middelen: ict, overig.
- Contra-tap.
- Contra-observatie.
- Desinformatiecampagnes.
- Andere dan de gebruikelijk communicatiekanalen.
- Verblijf in het buitenland.

5.9 Reacties op de overheid

- In hoeverre reageren de betrokken daders op maatregelen van de overheid of op politieacties?
- Op welke manier reageren de betrokken daders in deze gevallen (bijvoorbeeld: contra-activiteiten, aanpassen strategie, vermijdingsgedrag, etc.)?

6 Omvang, verdeling en besteding van het wederrechtelijk verkregen voordeel (wvv)

6.1 Omvang van het wvv

Geef een schatting van de omvang van het totale wederrechtelijk verkregen voordeel (wvv) en geef indien mogelijk een toelichting m.b.v.:
- Een indicatie van de lucrativiteit van de criminele activiteiten / de 'winstmarge' (op basis van verkregen baten en gemaakte kosten (indien mogelijk: per eenheid)).
- De geschatte omvang van de illegale activiteiten (indien mogelijk: per jaar respectievelijk voor de geschatte totale duur van de criminele activiteiten).

6.2 Verdeling van het wvv binnen het samenwerkingsverband

Beschrijf kort de wijze waarop het wvv binnen het samenwerkingsverband wordt verdeeld.

- Staan de medewerkers op de loonlijst, worden zij betaald met een deel van het wvv en/of bestaat er een bepaalde relatie tussen beloningen en prestaties?.
- Welke verdachten verdienen er relatief het meest aan de criminele activiteiten?

6.3 Besteding wvv door de betrokken personen

Waar (in Nederland of elders) en waaraan wordt het wvv besteed? In hoeverre is er sprake van puur consumptieve privé-bestedingen (dure levensstijl), van investeringen in andere illegale activiteiten of van investeringen in legale ondernemingen/ activiteiten?

- Consumptieve privé-bestedingen (dure levensstijl).
- Investeringen in andere illegale activiteiten.
- Aankoop roerende goederen.
- Aankoop onroerende goederen.
- Vestiging wettige onderneming(en) – alle bedrijven van alle verdachten.
- Investering in bestaande wettige ondernemingen.
- Communicatie.
- Beleggingen (o.a. Aandelen, obligaties, projectontwikkeling).
- Sponsoring (sport, cultuur, politie, evenementen).

6.4 Geldtransacties en witwassen

Ga beknopt in op de geldtransacties binnen de criminele groep en op het verschijnsel witwassen (het omzetten van de verborgen, niet te verantwoorden herkomst van gelden in een wel te verantwoorden herkomst).
Besteed hierbij aandacht aan de betrokkenheid bij illegale geldtransacties van Nederlandse banken, wisselkantoren, buitenlandse banken, wettige bedrijven, trusts, ambassades en consulaten.

Betalingsverkeer

- Ruilhandel (inclusief bitcoins en andere cryptocurrencies, prepaid stored value cards, etc.).
- Kredietverstrekking / voorschotten.
- Ondergronds bankieren.
- Financiële transacties (zie hieronder).

Wegsluizen van gelden zonder witwassen (witwassen niet altijd noodzakelijk)

- Wisseltransacties.
- Fysieke verplaatsingen (door personen of per post).
- Girale verplaatsingen, money transfers.
- Ondergronds bankieren.

Witwassen

- Het voorwenden van vermogensstijging (o.a. ABCD-transacties, vastgoedhandel, kunsthandel en effectenhandel).
- Het overdragen van vermogen (o.a. schenken van vermogen aan jezelf, gefingeerde gokwinsten en lenen aan jezelf ('loan back methode')).
- Het creëren van inkomsten.

6.5 Vermogensbestanddelen / bezittingen

Ga kort in op de vermogensbestanddelen/bezittingen die in het kader van het strafrechtelijk onderzoek zijn getraceerd. Geef hierbij tevens aan welke vermogensbestanddelen/bezittingen in beslag zijn genomen.

- Horecagelegenheden.
- Detailhandel.
- Andere bedrijven – geef hier een zo volledig mogelijk overzicht van alle legale ondernemingen waarbij de daders betrokken zijn, ook als die ondernemingen niet voor criminele activiteiten worden gebruikt.
- Woningen/gebouwen/complexen.
- Auto's.
- Vaar- en vliegtuigen.
- Contant geld, sieraden, etc.

7 Strafrechtelijke afdoening

7.1 Rechtszaak in eerste aanleg en vonnissen

- Is er een strafzaak geweest en heeft dit geleid tot een vonnis?
- Wat is het aantal en de aard van de strafeisen en de vonnissen?
- Ten laste legging en veroordeling. Op basis van welke artikelen van het Wetboek van Strafrecht (of andere relevante wetten) zijn de verdachten veroordeeld?
- Is er hoger beroep aangetekend?

7.2 Sfo/ontnemingsvordering

- Heeft er een strafrechtelijk financieel onderzoek plaatsgevonden? Zo ja, wat zijn daarvan de belangrijkste uitkomsten?
- Ontnemingsvorderingen en de resultaten daarvan.

8 Evaluatie

8.1 Leerervaringen en nieuwe inzichten

Wat zijn de belangrijkste leerervaringen van dit onderzoek geweest?

- Welke nieuwe inzichten heeft deze zaak opgeleverd over het verschijnsel georganiseerde criminaliteit?
- In hoeverre wijkt de zaak af van gangbare beelden van georganiseerde criminaliteit en in hoeverre bevestigt deze zaak deze beelden?
- Is er een bestuurlijke rapportage, wat is de inhoud?

8.2 Mogelijkheden voor preventie

Wat maakte het uitvoeren van de criminele activiteiten zo gemakkelijk / moeilijk en op welke manier zouden barrières opgeworpen kunnen worden (preventie)?

- Maatschappelijke probleemgebieden en mogelijke ontwikkelingen daarin.
- Criminogene factoren overheidsbeleid (o.a. regelgeving, prikkels, toezicht, controle, opsporing).
- Potentiële barrières / preventiemogelijkheden.

8.3 Mogelijke nieuwe ontwikkelingen

Welke mogelijke nieuwe ontwikkelingen signaleert u op het gebied van de georganiseerde criminaliteit?

8.4 Effectiviteit van toegepaste recherchestrategie(ën)

- Wat zijn de maatschappelijke effecten van dit opsporingsonderzoek geweest?
- Wat valt er te zeggen over de effectiviteit van de toegepaste recherche-strategie(ën)?

8.5 Te interviewen personen en op te vragen rapporten

Noteer hier de gegevens van te interviewen personen of op te vragen rapporten, die relevant kunnen zijn voor het eindrapport.

Bijlage 3 Beknopte casusbeschrijvingen

Hieronder volgen beknopte beschrijvingen van de 180 zaken die in vijf rondes van de Monitor Georganiseerde Criminaliteit zijn geanalyseerd.

Casus 1
Mensensmokkel vanuit India. De route liep via Rusland en Polen naar Duitsland en/of Nederland en van daaruit veelal naar Engeland, Canada of de VS. Transporten vonden plaats met auto's, schepen en vliegtuigen.

Casus 2
Productie van en handel in heroïne en cocaïne; witwasactiviteiten. In openbare gelegenheden werden contacten gelegd met klanten. Opbrengsten werden via verschillende postkantoren omgewisseld en doorgesluisd naar Marokko. Via een Brusselse bank werd geld ook witgewassen.

Casus 3
Productie van en handel in amfetamine. Legale en illegale grondstoffen kocht men bij legale bedrijven en bij een drietal leveranciers. De deelprocessen van productie werden door verschillende koppels en groepjes uitgevoerd op diverse locaties in binnen- en buitenland.

Casus 4
Mensenhandel. Vrouwen werden in Oost- en Centraal-Europa geworven en meestal per bus (onder valse voorwendselen) naar Nederland gebracht. Zij belandden in de prostitutie. Met hulp van een ambtenaar kregen vrouwen een aanmeldingsstempel in hun paspoort. Ook antedateerde hij stempels, zodat vrouwen langer in Nederland konden blijven.

Casus 5
Productie van en handel in xtc en amfetamine; invoer van hasj; export van xtc, amfetamine, hasj , nederwiet en cocaïne. xtc en amfetamine werden in een laboratorium geproduceerd en per boot naar Engeland en Spanje vervoerd. Hasj werd vanuit Marokko per rubberboot naar Spanje gesmokkeld. De smokkel vanuit Spanje via Nederland naar Engeland vond plaats met vrachtwagens. Vanuit Colombia werd een cocaïnetransport naar Nederland georganiseerd.

Casus 6
Handel in cocaïne, heroïne, hasj, xtc en amfetamine. De cocaïne werd vanuit Venezuela per container naar Nederland vervoerd. Heroïne werd in een tankauto naar Engeland gesmokkeld. Wat de hasj betreft ging het om het bezit van ruim 1.000 kilo en aanwijzingen van vervoer van Marokko naar Spanje en van Spanje naar Engeland. In Nederland geproduceerde xtc en amfetamine werden door de organisatie vervoerd naar Engeland.

Casus 7
Invoer van cocaïne. In een zeiljacht werd de cocaïne vanuit het Caribisch gebied naar een haven in Nederland gebracht. Een van de hoofdverdachten van de Colombiaanse groep werd naar Nederland gestuurd om de operatie hier voor de Colombianen te begeleiden en de voor hen bestemde cocaïne in ontvangst te nemen.

Casus 8
Invoer van cocaïne en marihuana die per container vanuit Colombia via Nederland West-Europa werden binnengebracht om daar te worden overgedragen aan een Colombiaanse groep, die de partijen weer doorleverde. Ook werd cocaïne op het lichaam van een koerier per vliegtuig en via postpakketten vervoerd.

Casus 9
Mensensmokkel en vervalsing van paspoorten. Gemiddeld ging het om 240-300 personen per jaar op de route Iran – Nederland – Canada. Personen reisden deels op een eigen paspoort en een authentiek visum en deels op vervalste documenten. Ook werd gebruikgemaakt van nepuitnodigingen van bedrijven en van pasjeshouders op een luchthaven, waardoor personen vrijwel probleemloos het land konden binnenkomen.

Casus 10a
Mensenhandel; exploitatie van meer- en minderjarige vrouwen. De over het algemeen jonge vrouwen werden door vaste ronselaars in Oost- en Centraal-Europa onder valse voorwendselen naar Nederland gehaald. In Slovenië werden de vrouwen overgedragen aan andere vervoerders en voorzien van valse reisdocumenten. In Nederland moesten de vrouwen onder dwang werken als prostituee.

Casus 10b
Mensenhandel; exploitatie van meer- en minderjarige vrouwen. In Oost- en Centraal-Europa werden vrouwen geronseld. Er werd gebruikgemaakt van diverse routes met als centrale ontmoetingsplaats Hongarije, waar de vrouwen werden voorzien van valse reisdocumenten en werden overgedragen aan chauffeurs, die de reis naar Nederland verder verzorgden. In Nederland werden zij gedwongen in de prostitutie te werken.

Casus 11
Smokkel over de weg van hasj uit Pakistan, heroïne uit Turkije en van cocaïne uit Colombia door middel van zeeschepen, die aankwamen in Ierland, Engeland, België, Nederland, Frankrijk en Malta. Door middel van koeriers werden de verdovende middelen indien nodig verder naar Nederland gebracht. Koeriers fungeerden ook als geldloper.

Casus 12
Mensenhandel. In Oost- en Midden-Europa werden meer- en minderjarige vrouwen onder valse voorwendselen geronseld. Zij werden van valse reisdocumenten voorzien en per auto naar Nederland gebracht. De vrouwen werden door de hoofdverdachte in seksclubs geplaatst en tot prostitutie gedwongen. Ook kwam het voor dat zij werden doorverkocht.

Casus 13
Mensenhandel. Vooral in Tsjechië en Polen werden vrouwen door middel van misleiding geronseld. Met valse papieren reisden de vrouwen per vliegtuig of bus naar Nederland of Duitsland. In seksclubs werden de vrouwen tot prostitutie gedwongen of doorverkocht.

Casus 14
Mensenhandel. De hoofdverdachte ronselde of kocht meer- en minderjarige vrouwen in met name Tsjechië, of in Nederland van doorgaans buitenlandse ronselaars, vervoerders en souteneurs. In Nederland werden de vrouwen doorverkocht aan exploi-

tanten en aan souteneurs, of zij kwamen te werken in seksclubs, in een privéclub of in de raamprostitutie.

Casus 15
Mensenhandel. Vrouwen werden in Tsjechië geronseld en reisden via Duitsland per auto met de hoofdverdachte af naar Nederland. Daar werden zij overgedragen aan de hoofdverdachte van de hierboven beschreven Casus 14.

Casus 16
Cocaïnehandel. Vanuit Curaçao werd cocaïne in pakketten levensmiddelen verzonden naar België of Duitsland. De pakketten werden op een Nederlandse luchthaven 'opgevangen'. Vanuit Curaçao werd het airwaybill-nummer doorgespeeld aan luchthavenpersoneel in Nederland. Dit onderschepte de lading en bracht de handel buiten het vliegveld.

Casus 17
Beheer van vijftien wietkwekerijen, cocaïnehandel, fraude en geweld. De kwekerijen waren ondergebracht in schuren, kelders, slaapkamers en zolders. De wiet werd verkocht aan coffeeshops. De cocaïne was bestemd voor de tussenhandel ten behoeve van het lokale circuit. De fraude betrof het opkopen en leeghalen van noodlijdende BV's. Het geweld ging om bedreigingen in verband met overnames in de horeca en om bedreiging van een koppelbazenbedrijf en van schuldenaars.

Casus 18
Handel in cocaïne en heroïne. Een organisatie in Turkije leverde op bestelling heroïne en cocaïne. Die werden door middel van vrachtauto's naar Polen getransporteerd, waar ze door Nederlandse Turken werden afgehaald. Via tussenpersonen werden de drugs op lokale markten in Nederland afgezet en doorverkocht aan afnemers in Duitsland.

Casus 19
Afpersing, ripdeals, flessentrekkerij, illegale loterij, drugshandel en koppelbazerij. Onder andere door bedreiging, mishandeling, werd getracht een aantal personen geld afhandig te maken. Slachtoffers en daders kwamen uit hetzelfde (criminele) milieu. De ripdeals betroffen het niet betalen en niet leveren van hasj en het beroven van houders van coffeeshops. Bij de flessentrekkerij werden gedane bestellingen niet of ten dele betaald. Een illegale lotto werd overgenomen en voortgezet. Daarnaast zag men hasjhandel in kleine partijen. Door de verdachten werden een koppelbazenbedrijf en een Engelse limited opgericht. Dit laatste om Engelse werknemers in Duitsland te laten werken.

Casus 20
Handel in hasj, productie van en handel in xtc en amfetamine. Bij de productie van xtc ging het vooral om de voorbereiding. Wat de amfetamine betreft ging het meer om 'pogingen' tot produceren. Of dit voor beide producten daadwerkelijk gelukt is, wordt niet duidelijk. Bij de handel in xtc leken de pillen op bestelling door de hoofdverdachte in Nederland te worden aangekocht en doorgeleverd. Een poging om xtc aan een groep in Spanje te leveren mislukte. Bewezen is dat de hoofdverdachte betrokken was bij de uitvoer van 2 kilo hasj.

Casus 21
Primair ging het om 'contra-activiteiten': het onderscheppen van berichtenverkeer van politie en justitie. Voor het onderscheppen van semafoon- en radioverkeer

gebruikte men een speciaal ontwikkeld semafoonprogramma en speciaal ontworpen scanners. Ook hield de groep zich bezig met het kraken van cryptogegevens van een observatieteam. Hiervoor werden computers, software en scanners aangekocht, die door 'deskundige verdachten' werden aangepast. Gegevens werden doorgespeeld aan derden. Daarnaast zag men creditcardfraude, fraude met overboekingen, diefstal c.q. heling van computers en handel in PMK.

Casus 22
Handel in cocaïne, die per schip vanuit Brazilië door koeriers in weekendtassen vervoerd werd naar België, om per auto verder vervoerd te worden naar Nederland. Daar werd de cocaïne overgedragen aan een groepslid en onder bewaking gesteld van weer een ander. De woningen van medeverdachten werden gebruikt voor opslag, testen en in plakken persen.

Casus 23
Handel in versnijdingsmiddelen en heroïne. De heroïne werd rechtstreeks uit Turkije geïmporteerd en in Nederland afgezet. Ook was er sprake van uitvoer van heroïne en versnijdingsmiddelen naar Frankrijk. Laatstgenoemde middelen werden bij een wettige leverancier besteld.

Casus 24
Hasjhandel. Boten werden aangekocht die op een bepaalde plaats werden beladen met Pakistaanse en Marokkaanse hasj. Soms werd de waar overgeladen op een andere boot, soms werd rechtstreeks naar een bepaalde haven gevaren om te lossen. De hasj werd opgeslagen om daarna te worden overgedragen aan afnemers in Nederland, Engeland en Canada. Buitenlands geld werd via koeriers naar Nederland vervoerd.

Casus 25
Hasjhandel. Partijen hasj werden met schepen afgehaald (Pakistan en Marokko) en naar een ontmoetingspunt gevaren, waar de handel door een kleinere boot werd afgehaald die dan naar de plaats van bestemming voer (Nederland, Australië, Engeland). Ladingen werden soms overboord gezet om later weer opgevist te worden.

Casus 26
Handel in hasj, xtc, precursoren, amfetamine en valse merkkleding. De drugshandel geschiedde op twee wijzen. Ten eerste door het gebruikmaken van reguliere ladingen en het daarin verbergen van de verdovende middelen; ten tweede door het zelf vervoeren met een chauffeur, waarbij de organisatie gebruikmaakte van een geprepareerde vrachtauto. De handel in valse merkkleding geschiedde via de lijn Turkije - Nederland - Spanje.

Casus 27
Invoer van hasj, marihuana en cocaïne. De groep hanteerde twee methoden: containers met een reguliere lading, bestemd voor bonafide bedrijven, werden gebruikt om sporttassen of koffers met cocaïne naar Nederland te brengen. Bij de tweede methode werden containers, met op papier een reguliere lading, gebruikt om partijen marihuana en hasj Nederland binnen te brengen. Hierbij gebruikte men niet bestaande bedrijven in voormalige Oostbloklanden.

Casus 28
Invoer hasj; handel in xtc en amfetamine. Marokkaanse hasj werd gesmokkeld met een camper en een touringcar. Via twee bedrijven werden grondstoffen besteld die vervolgens werden doorgeleverd aan producenten van amfetamine/'. Ook via Tsjechië en Frankrijk werden grondstoffen in Nederland ingevoerd. Amfetamine werd naar Engeland gebracht in een geprepareerde auto.

Casus 29
Fraude: ontduiking van EU-heffingen. Melkpoeder uit het Oostblok had als zogenaamde bestemming onder andere Spanje en Nigeria, maar werd in Nederland afgezet. De T1 documenten werden niet bij de douane aangeboden of de schijn werd gewekt dat aanzuivering had plaatsgevonden. Het 'groene strookje' werd van een (valse) stempel voorzien en weer teruggestuurd naar de douane-expediteur. In feite werd nooit betaald. Valse aankoopfacturen verhulden waar de melkpoeder vandaan kwam.

Casus 30
Invoer van cocaïne vanuit Zuid-Amerika naar Nederland en witwassen. Invoer geschiedde in containers per schip. In een garnalenverwerkingsbedrijf in Zuid-Amerika werd de waar verpakt in dozen garnalen met een dubbele bodem. Ten behoeve van het witwassen had de organisatie de beschikking over ruim 45 bedrijven in Nederland, Zwitserland en de Nederlandse Antillen.

Casus 31
Geld wisselen en vermoedelijk ondergronds bankieren. Drugs- en textielhandelaren die geld wilden wisselen konden hierover telefonisch afspraken maken, of naar de woning of winkel van de hoofdverdachten gaan en daar hun geld afleveren. De wisselaars bekeken eerst of zij te wisselen geld direct aan anderen kwijt konden. De rest werd in België gewisseld.

Casus 32
Heroïnehandel; vermoedelijke productie/handel in xtc, precursoren en amfetamine. De heroïne werd vanuit zuid Oost-Azië in pakketten kleding naar woonadressen of bedrijven gestuurd op naam van een onbekende adressant. Ook werd van daaruit de heroïne in kisten met porselein naar een Duits restaurant gezonden. Doorvoer naar Frankrijk geschiedde met koeriers per auto of trein.

Casus 33
Mensenhandel. Op eigen initiatief of op bestelling werden de vrouwen in Nigeria geronseld. Voor paspoorten werd gebruikgemaakt van een documentenvervalser. Per vliegtuig reisde men af naar Nederland of Duitsland. De vrouwen werden in Nederland, Duitsland en België tewerkgesteld in een bordeel of in de raamprostitutie.

Casus 34
Mensenmokkel (kinderen). Vanuit India werden jongens, veelal van 8 tot 15 jaar, met 'nepouders' naar Europa gebracht, waarvoor de echte ouders ruim € 11.000 per kind moesten betalen. De nepouders brachten de kinderen naar Europa op hun paspoort waarop hun eigen kinderen stonden bijgeschreven. De reis liep via Duitsland, Frankrijk of Zwitserland en dan naar Nederland. Een volgend paar nepouders bracht de kinderen vervolgens naar de VS.

Casus 35
Mensensmokkel (Turken). Het traject Turkije - Nederland geschiedde veelal op Russische en Poolse schepen, of in containers op vrachtwagens via België, Frankrijk en Duitsland, of rechtstreeks via luchtverkeer. Door veelvuldige controles in Engeland is de organisatie, na een andere methode, overgestapt op het als verstekeling aan boord zetten in Nederlandse en Belgische havens. Dit gebeurde met de hulp van bemanningsleden, al dan niet met medeweten van de kapitein.

Casus 36
Handel in heroïne en '; belastingfraude. Pakistaanse heroïne werd vanuit Turkije met in Nederland geprepareerde auto's naar Nederland gebracht. De xtc werd afgenomen van een onbekend gebleven leverancier. De belastingfraude had betrekking op door de hoofdverdachte georganiseerde colportageactiviteiten en bestond uit verkeerde opgave van aantallen gesloten contracten.

Casus 37
Productie van precursoren en '. De groep maakte gebruik van drie laboratoria voor de productie van '. Door bepaalde verdachten werden grondstoffen geleverd. Een andere regelde betalingen, personenvervoer van en naar de laboratoria en contacten met opdrachtgevers. Men was ook doende om zelf grondstoffen te maken en om zelf direct uit een bepaalde chemische stof xtc te maken.

Casus 38
Handel in hasj, die vooral in Pakistan werd aangekocht en daarna in containers met dekladingen per schip werd vervoerd naar België, in transit naar Polen of Frankrijk. De aankoop vond plaats via ontmoetingen in onder andere Turkije. Soms werd gebruikgemaakt van een schip waarin de hasj voor langere tijd werd opgeslagen. Met kleine schepen werden vervolgens partijen vanaf het opslagschip gehaald. De waar werd doorverkocht naar de VS of Canada.

Casus 39
Oliefraude: verwerving van olieproducten door middel van verduistering, heling en valsheid in geschriften. De olieproducten werden door een aantal schippers achtergehouden en afgeleverd bij een bedrijf, dat de producten op zijn beurt weer zwart doorverkocht aan een volgend bedrijf. Uiteindelijk kwam alles bij een onderneming terecht die ervoor zorgde dat de producten weer 'witgewassen' in het officiële circuit verhandeld werden. Dit witwassen geschiedde met valse facturen die door verschillende verdachten werden aangeleverd.

Casus 40
Samenstelling, verveelvoudiging en distributie van illegale cd's en cd-roms; flessentrekkerij. Met behulp van 'plof-BV's' liet de groep cd's en cd-roms masteren en persen, om deze vervolgens in het grijze en zwarte circuit te verhandelen. Het masteren en persen gebeurde ook in het buitenland. Via de plof-BV's werden ook grote hoeveelheden goederen besteld bij bedrijven die echter nooit betaald werden.

Casus 41
Heroïnehandel vanuit Turkije. Door Poolse echtparen werd de heroïne in geprepareerde personenauto's vanuit Turkije via Bulgarije naar Polen vervoerd. Daar werd de handel overgenomen door een ander (Pools) echtpaar en vervolgens naar Nederland vervoerd.

Casus 42
Handel in heroïne, cocaïne, xtc en methadon. Cocaïne werd vanuit Zuid-Amerika per vliegtuig door koeriers gesmokkeld in pakketjes, maar ook door het slikken van bolletjes. Heroïne werd in vrachtwagens vanuit Turkije vervoerd via Griekenland, Roemenië en Italië. De handel werd in Nederland afgezet en uitgevoerd naar Engeland, Duitsland, Spanje en België. Aan Turkije werden xtc en methadonpillen geleverd.

Casus 43
Handel in cocaïne, heroïne en marihuana. De invoer liep via Schiphol, door middel van koeriers of verborgen in apparatuur, in containers, of in vrachtwagens. Meestal geschiedde de uitvoer door middel van koeriers in auto's richting Duitsland, Frankrijk en Spanje.

Casus 44
Productie van en handel in synthetische drugs. De benodigde chemicaliën werden bij bedrijven in Duitsland, Italië, Zwitserland en Nederland ingekocht. De grondstoffen werden vervolgens doorgeleverd of verwerkt tot synthetische drugs. De pillen werden geslagen in een bedrijf van de hoofdverdachte. Afnemers zaten door heel Nederland.

Casus 45
Productie van en handel in synthetische drugs en nepdrugs. De grondstoffen kwamen bij andere Nederlandse criminele groeperingen vandaan en via contacten met chemische bedrijven. De productie vond plaats in laboratoria in Nederland. De afzetmarkt lag zowel in Nederland als in het buitenland.

Casus 46
Mensensmokkel vanuit China en vervalsen van paspoorten. De route was veelal dezelfde en liep, grotendeels per vliegtuig, vanuit China via Moskou of de Oekraïne naar Praag. Hier vandaan, maar ook via Oostenrijk, werden de gesmokkelden naar het land van bestemming gebracht, zoals Nederland en Duitsland.

Casus 47
Productie van en handel in xtc en amfetamine. De drugs kwamen uiteindelijk terecht bij Nederlandse afnemers, maar er waren ook lijnen naar het buitenland.

Casus 48
Wapensmokkel vanuit Oost-Europa. De vuurwapens werden rechtstreeks aangekocht bij een fabriek. Via Hongarije, Oostenrijk en Duitsland werden de wapens over de weg naar Nederland vervoerd en verkocht via contacten in onder meer coffeeshops.

Casus 49
Creditcardfraude. In Chinese restaurants werden door obers creditcards gekopieerd door de gegevens van de magneetstrip op te slaan. Deze gegevens werden elders op blanco creditcards gedrukt. Met die vervalste creditcards werden allerlei aankopen gedaan in België, Duitsland, Frankrijk, Denemarken en Japan.

Casus 50
Hasjhandel vanuit Marokko. De organisatie verzorgde transporten per vrachtwagen op het traject Spanje – Nederland (deels bestemd voor de Nederlandse markt) en vanuit Nederland naar Denemarken, Noorwegen, Schotland, Engeland en Ierland.

Casus 51
De groep hield zich bezig met het organiseren van schijnhuwelijken, met name van schijnrelaties. Via de hoofdverdachte en zijn dochter werden mensen aan elkaar gekoppeld, met als doel een verblijfsvergunning te krijgen voor degene die zich illegaal in het land bevond. Daarnaast werden er via een stichting valse naturalisaties geregeld.

Casus 52
Geld wisselen. Het ging hierbij om het wisselen van grote hoeveelheden buitenlands geld in Nederlandse guldens, afkomstig van organisaties die softdrugs exporteerden.

Casus 53
Mensensmokkel vanuit Irak. De organisatie had contact met een groep die in Irak voor de uitreis zorgde. Een deel van de mensen werd uit Jemen gehaald. Daarnaast was deze criminele groep een onderdeel van een netwerk van smokkelorganisaties, die de route over land via Turkije, Griekenland, Albanië en Italië gebruikten. Eindbestemmingen waren Noord- en West-Europa.

Casus 54
Mensensmokkel en vervalsing paspoorten. De smokkelactiviteiten van deze groep betroffen vooral de doorvoer van Irakese mannen van Nederland naar Zweden. De route liep van Schiphol via Parijs naar Noorwegen of Zweden voor telkens een of twee personen. De groep regelde de reis en de benodigde valse papieren.

Casus 55
Mensensmokkel en handel in vervalste paspoorten. De ene groep kocht gestolen paspoorten, bewerkte die en hield zich bezig met mensensmokkel uit Iran/Irak naar Nederland en Engeland. De tweede groep gebruikte routes vanuit Italië naar België, Duitsland en Nederland, en vanuit Nederland naar Scandinavië. De derde groep was afnemer van valse paspoorten en exploiteerde illegale raamprostituees uit het Oostblok.

Casus 56
Cocaïnehandel vanuit Zuid-Amerika. De groep maakte gebruik van machines, die In Israël werden opgekocht en geprepareerd. Deze machines werden vervolgens via Europa naar Zuid-Amerika getransporteerd, waar de cocaïne werd ingebracht, waarna zij weer terug naar Europa werden vervoerd, onder meer via Nederland, België en Duitsland.

Casus 57
Heroïnehandel vanuit Turkije. De smokkel werd uitgevoerd met vrachtauto's en gedeeltelijk door middel van een busdienst die eigendom was van familie van de hoofdverdachte. De route liep vanuit Irak/Iran naar Istanbul (in Turkije werd de ruwe opium in een laboratorium verwerkt tot heroïne), via Bulgarije/Roemenië naar Nederland.

Casus 58
Cocaïnehandel vanuit Colombia. Door middel van koeriers werden de verdovende middelen per vliegtuig vanaf de Antillen/Suriname overgebracht naar Nederland.

Casus 59
Mensensmokkel, heling en vervalsing van paspoorten. De groep smokkelde Irakese personen van Nederland naar Engeland. De klanten werden via België door Frankrijk

naar Calais vervoerd en van daaruit per veerboot naar Dover. Valse paspoorten werden aangekocht.

Casus 60
Vervaardigen, verveelvoudigen en verspreiden van illegale cd's en cd-rom's. De organisatie maakte gebruik van diverse reguliere buitenlandse bedrijven, onder meer voor het persen. Verspreid werd de handel onder meer in cafés, verenigingen en buurthuizen.

Casus 61
Wapenhandel vanuit de Balkan. De vuurwapens waren afkomstig uit Slovenië/Kroatië en werden over de weg door middel van koeriers naar Nederland gebracht. Het ging om kopieën van bestaande merken die van bedenkelijke kwaliteit waren. Zij kwamen uiteindelijk bij Joegoslavische afnemers terecht.

Casus 62
Mensenhandel vanuit het Oostblok. Vrouwen werden in een discotheek geronseld en onder valse voorwendselen met valse paspoorten naar Nederland gehaald en vervolgens gedwongen om in de prostitutie te werken.

Casus 63
Handel in cocaïne en synthetische drugs. De hoofdverdachte van deze groep kon wel aan synthetische drugs komen (‘), maar niet aan cocaïne. Om dit op te lossen ruilde hij met een andere criminele organisatie xtc tegen cocaïne.

Casus 64
Productie van en handel in synthetische drugs en invoer van cocaïne. De cocaïne werd per schip vanuit Zuid-Amerika in machines Nederland binnengesmokkeld. Met auto's en vrachtwagens werden xtc en amfetamine vervoerd naar onder meer Hongarije en Engeland.

Casus 65
Geld wisselen voor drugshandelaren en ondergronds bankieren. Het wisselen werd uitgevoerd bij banken en wisselkantoren in België. Daarnaast was er sprake van informele moneytransfers door een aantal ondergrondse bankiers. Deze zorgden ervoor dat illegale verdiensten konden worden weggesluisd naar het buitenland.

Casus 66
Hasjhandel vanuit Marokko. Een Marokkaanse medeverdachte regelde de aanvoer naar Spanje. De organisatie zorgde voor verder transport naar Nederland met vrachtauto's. De hasj was bestemd voor de Nederlandse, de Scandinavische en de Engelse markt.

Casus 67
Oliefraude. Vanuit België en Duitsland werden minerale oliën in Nederland in het vrije verkeer gebracht zonder dat afdracht van btw/accijnzen had plaatsgevonden. Het geleidedocument werd telkens valselijk voorzien van een Nederlands douanestempel. De goederen werden in het vrije verkeer gebracht door een aantal papieren firma's en werden dan 'gewit' door tussenkomst van legale ondernemingen.

Casus 68
Handel in merkvervalste kleding vanuit Turkije. Een persoon in Turkije regelde inkoop en transport vanuit Turkije en vanuit Thailand via Turkije en Duitsland naar

Nederland, via vrachtvervoer over de weg. Na opslag in loodsen werd de kleding doorverhandeld.

Casus 69
Sigarettensmokkel. De sigaretten werden legaal ingekocht, buiten de EU gebracht en vervolgens de EU weer binnengesmokkeld. Daarmee deed men voorkomen dat de handel niet voor de EU bestemd was, zodat geen accijns betaald hoefde te worden. Een andere methode was het valselijk afstempelen van de bij de zendingen behorende documenten. De sigaretten kwamen uiteindelijk terecht in Ierland, Engeland, Spanje en Portugal.

Casus 70
Handel in cocaïne, xtc en marihuana. De cocaïne werd uit Colombia betrokken en kwam per schip naar Nederland, soms via tussenhavens in Duitsland, België of Spanje. De xtc werd gekocht van een andere organisatie. De exacte herkomst van de marihuana is niet bekend.

Casus 71
Autodiefstal. Diefstal geschiedde door het openbreken van auto's, door het benaderen van eigenaren om behulpzaam te zijn bij de diefstal (afgeven van kentekens en autosleutels) en door het huren van luxe wagens bij autoverhuurbedrijven en garages m.b.v. valse rijbewijzen. De auto's werden vervolgens als gestolen opgegeven. Over de weg en via havensteden in Engeland en Italië kwamen de wagens uiteindelijk bij de afnemer terecht.

Casus 72
Valutatermijnhandel. Doel van de organisatie was klanten te bewegen geld te investeren in de valuta(termijn)handel, om zich deze gelden vervolgens wederrechtelijk toe te eigenen. Na ondertekening door de klanten van een contract maakten zij geld over naar een rekening bij een Zwitserse bank. Over dit geld konden zij vervolgens niet meer beschikken, mede doordat de hele handel voornamelijk op papier bestond.

Casus 73
Geld wisselen. De groep hield zich bezig met het wisselen van geld dat door (drugs)organisaties werd aangeleverd. Bij een vast kantoor in België werd het geld gewisseld.

Casus 74
Geld wisselen. De groep wisselde in België geld met een criminele herkomst. Als dekmantel voor het wisselen werden een antiekzaak en een kledingwinkel gebruikt.

Casus 75
Mensenhandel. De groep hield zich bezig met het ronselen van vrouwen, vooral in Nigeria, om hen in Europa te verhandelen aan seksexploitanten. De reis naar Nederland maakten de slachtoffers zelfstandig, per vliegtuig naar Schiphol, onder een valse naam en met een vals paspoort. De eindbestemming was vaak Nederland, maar velen werden verhandeld aan exploitanten in Duitsland, België en Italië.

Casus 76
Diefstal van auto's en motoren, gewapende overvallen en inbraken en handel in cocaïne. Het ging hier om een netwerk van samenwerkende groepen die elk hun eigen specialiteit hadden. De voertuigen werden geleverd aan reguliere motor- en

autobedrijven. Verder pleegden zij overvallen en inbraken op onder meer postkantoren en juweliers door het gehele land. Eén van de verdachten bezat een winkel, van waaruit verdovende middelen werden verhandeld. Cocaïne werd ingevoerd vanuit Aruba en uitgevoerd naar onder meer Italië.

Casus 77
Handel in vuurwapens en explosieven. Vanuit Joegoslavië werd de handel met touringcarbussen en vrachtwagens via Duitsland naar Nederland vervoerd. Eén van de verdachten zocht naar kopers; meestal vonden de afleveringen van wapens plaats in wegrestaurants. Bij huiszoekingen werden nog twee hennepkwekerijen aangetroffen.

Casus 78
Handel in vuurwapens. De groep bracht op grote schaal wapens in het zwarte circuit. De aanlevering werd verricht door twee Belgische wapenhandelaren door wapens op papier te exporteren en deze wapens, die gewoon in België bleven, daarna zwart te verhandelen. Een Nederlandse wapenhandel zorgde voor exportvergunningen naar een postbusfirma in Gibraltar.

Casus 79
Geld wisselen, drugshandel en wapenhandel. Door deze groep werd geld gewisseld (verdiend met drugsleveringen aan coffeeshops) en gehandeld in wiet, hasj, xtc, amfetamine en vuurwapens. De wapens werden verkregen van twee Zwitsers in ruil voor drugs. Wiet werd deels ingekocht bij thuiskwekers; hasj werd gekocht van verschillende leveranciers.

Casus 80
Handel in vuurwapens. De precieze werkwijze van deze groep is niet duidelijk in beeld gekomen. Vermoedelijk betrok de groep de wapens vanuit het voormalige Oostblok, vooral uit Rusland.

Casus 81
Handel in xtc, MDMA, BMK, PMK, amfetamine, hasj, marihuana en nederwiet. De verdovende middelen werden naar verschillende landen uitgevoerd en verkocht aan afnemers in onder meer Engeland, Zweden en Nederland zelf. Het vervoer van de verdovende middelen werd uitgevoerd per (huur)auto, bestelbus, vrachtauto, via een transportbedrijf, per trein, per boot, per zeecontainer en per touringcar.

Casus 82
Mensensmokkel. Vanuit China werden groepen mensen naar West-Europa gesmokkeld en via Nederland en België naar het Verenigd Koninkrijk vervoerd. Daar werden de gesmokkelden opgevangen en werden zij geholpen bij het aanvragen van asiel.

Casus 83
Mensensmokkel. Crimineel samenwerkingsverband dat zich bezig hield met de smokkel van mensen vanuit China naar West-Europa. Via Nederland en België werden de gesmokkelden verder vervoerd naar het Verenigd Koninkrijk.

Casus 84
Handel in cocaïne, amfetamine, xtc, MDMA-pillen, hasj, hennep en sigaretten door verschillende samenwerkingsverbanden. De verdovende middelen werden per boot en per vrachtwagen in- of uitgevoerd.

Casus 85
Productie van en handel in xtc, amfetamine, MDMA, PMK, cocaïne, hasj en hennep, deels bestemd voor de Engelse markt. Vervoer geschiedde per vracht-, bestel- en personenauto.

Casus 86
Smokkel van heroïne vanuit Turkije via Nederland naar Spanje, deels ook bestemd voor de Nederlandse markt. Als deklading werden machineonderdelen, groente en fruit gebruikt.

Casus 87
Invoer van heroïne vanuit Turkije in Nederland en de distributie ervan en geldsmokkel m.b.v. koeriers naar Dubai en Turkije.

Casus 88
Inkoop bij legale bedrijven van apparatuur en materialen die, al dan niet na bewerking ervan, werden doorverkocht aan afnemers voor de vervaardiging van synthetische drugs.

Casus 89
Uitvoer van xtc naar de VS, Engeland en Panama, via koeriers met koffers en reguliere vervoersbedrijven. Bij dit laatste werd speelgoed als deklading gebruikt.

Casus 90
Bezit en uitvoer van xtc; invoer van cocaïne in Nederland. xtc werd ook gebruikt als betaal- c.q. ruilmiddel voor cocaïne. xtc werd naar de Cariben vervoerd; cocaïne vanuit Zuid-Amerika via de Cariben naar Nederland.

Casus 91
Bezit en uitvoer van xtc naar vooral New York en verder naar Spanje en Duitsland. Daarbij werd onder meer gebruikgemaakt van koeriers en pakketdiensten.

Casus 92
Inkoop van xtc en de uitvoer ervan naar de VS, Australië en Engeland door een organisatie die opereerde vanuit Amsterdam. De pillen werden afgenomen van Nederlanders die zich bezighielden met de productie van de xtc en de verkoop ervan aan groothandelaren.

Casus 93
Mensensmokkel en -handel. Het samenwerkingsverband hield zich zowel bezig met vrouwenhandel vanuit de Baltische staten, met als doel deze vrouwen in Nederland in de prostitutie voor zich te laten werken, als met mensensmokkel. Deze mensen werd beloofd dat zij, in ruil voor grote bedragen, hier werk en een huis zouden krijgen.

Casus 94
Primaire activiteit was de grootschalige invoer van cocaïne vanuit Colombia. Daarnaast vond invoer plaats van hasj en uitvoer van `. Behalve de handel in verdovende middelen hield men zich ook bezig met illegale gokspelen.

Casus 95
Uitvoeren van illegale geldtransacties. Deze bestonden uit het omwisselen dan wel verplaatsen van geld naar het buitenland. Het ging om geld dat afkomstig was van verdovende middelenhandel.

Casus 96
Cocaïnesmokkel van Curaçao naar Nederland, waarbij de cocaïne hetzij door koeriers werd gesmokkeld dan wel door middel van postpakketten werd verzonden. De opbrengsten werden via money transfers naar Curaçao overgemaakt.

Casus 97
Cocaïnesmokkel. Door de groep werd met behulp van een geprepareerd voertuig cocaïne vanuit Nederland naar Italië gesmokkeld, waar zich Joegoslavische afnemers bevonden. De cocaïne werd geleverd door een persoon uit Rotterdam.

Casus 98
Smokkel van xtc vanuit Nederland naar de VS en een enkele keer naar Canada. Hierbij werd gebruikgemaakt van stewards als koeriers. De pillen werden in de handbagage meegenomen van de stewards waarbij gebruik werd gemaakt van de personeelsingang.

Casus 99
Cocaïnesmokkel vanuit Curaçao, de Dominicaanse Republiek naar Nederland door middel van het slikken van bolletjes. Opbrengsten werden via money transfers vanuit Nederland naar Curaçao en de Dominicaanse Republiek verzonden.

Casus 100
Smokkel van cocaïne die per schip naar West-Europa werd vervoerd. Dit gebeurde in containers met verschillende soorten dekladingen, vooral fruit. De andere lijn betrof xtc die voornamelijk in postpakketten naar de VS werd verstuurd. Tijdens het onderzoek werd ook een '-laboratorium aangetroffen.

Casus 101
Er was in deze zaak sprake van twee groeperingen die een samenwerkingsverband hadden teneinde verdovende middelentransporten tot stand te laten komen. De Colombiaanse organisatie zorgde voor de aanvoer van de cocaïne en verzorgde de dekladingen in Latijns-Amerika. De Nederlandse c.q. Surinaamse tak verzorgde de invoer.

Casus 102
De groepering bestond hoofdzakelijk uit medewerkers van een bagage afhandelingsbedrijf op een luchthaven. Uit koffers werden rugtassen met cocaïne gehaald, die vervolgens door de medewerkers van 'airside' naar 'landside' werden gebracht. Op 'landside' werd de rugtas overgedragen aan een andere medewerker van de groepering.

Casus 103
Smokkel en fabricage van sigaretten. De smokkel werd per schip uitgevoerd vanuit twee Baltische staten. Via een aantal Noord-Duitse havens werden de containers over de weg met vrachtwagens de EU binnengebracht. Vanuit Duitsland werden de sigaretten naar België vervoerd. Ook beschikte de organisatie in België over een productielijn voor sigaretten.

Casus 104
Fraude. Vennootschappen kochten voor omvangrijke bedragen bepaalde rechten, onder meer in olie, kolen en goud. Geld dat in de vennootschappen aanwezig was werd niet gebruik om de verworven rechten te exploiteren, maar werd verdeeld onder leden van de organisatie. Om het spoor naar deze begunstigden te verhullen werd bij de verdeling gebruikgemaakt van diverse buitenlandse bankrekeningen, trustkantoren en Limiteds.

Casus 105
Verschillende criminele activiteiten, vooral productie van en handel in `. De organisatie maakte gebruik van verschillende `-laboratoria. Daarnaast was sprake van heling, handel in hasj en in verschillende geneesmiddelen, waaronder Viagra.

Casus 106
Fraude. Aankopen van BV's om vervolgens de belastingheffing te frustreren. Om het geheel voor de fiscus zo ondoorzichtig mogelijk te maken werden onder meer de namen van gekochte rechtspersonen veranderd; bedrijven verkocht (en toch de oorspronkelijke zeggenschap gehandhaafd); documenten vervalst; eigendom en exploitatie verdeeld over verschillende rechtspersonen; en deed men het voorkomen alsof administratie gestolen of incompleet was.

Casus 107
Mensensmokkel. Illegalen uit diverse landen werden vanuit Turkije via Nederland naar het Verenigd Koninkrijk gesmokkeld. Landen van herkomst waren onder meer Albanië, Slovenië, Georgië, Afghanistan en Turkije.

Casus 108
Mensensmokkel. Illegalen werden vanuit Noord-Afrikaanse en Arabische landen via Nederland naar het Verenigd Koninkrijk gesmokkeld. Landen van herkomst waren onder meer Somalië, Ethiopië, Soedan, Saoedi-Arabië, Jemen en Koeweit.

Casus 109
Mensenhandel. De vrouwen waren afkomstig uit Estland met als bestemmingsland Nederland. Gereisd werd via Zweden, Denemarken en Duitsland. De vrouwen werden in de prostitutie tewerkgesteld.

Casus 110
Mensenhandel. Vrouwen werden naar Nederland gesmokkeld en belandden in de prostitutie. Zij waren afkomstig uit de Oekraïne, Moldavië, Polen, Slowakije, Tsjechië, Wit-Rusland, en Rusland.

Casus 111
Mensensmokkel vanuit China naar Nederland. Chinezen werden naar Moskou gevlogen en vervolgens met de trein naar Tsjechië, Slowakije of Polen gebracht om daarna per auto via Duitsland naar Nederland vervoerd te worden. Chinezen konden ook verder reizen naar Engeland.

Casus 112
Wisselen van geld en innen en uitbetalen van internationale overboekingen. Bij het wisselen van geld opereerde de hoofdverdachte zelfstandig. Bij internationale overboekingen werd samengewerkt met personen in Dubaï en Pakistan. Geld was voornamelijk afkomstig van verdovende middelenhandel.

Casus 113
Hoofdactiviteit van de verdachten was de productie van en handel in amfetamine. Ook werd eenmaal hasj uitgevoerd en verkocht in Duitsland. In een aangetroffen amfetaminelaboratorium werden, behalve amfetamine, chemicaliën en BMK aangetroffen.

Casus 114
Inkoop van xtc en uitvoer ervan naar onder meer Australië, Nieuw-Zeeland en Azië. De pillen werden gekocht in Nederland. Wat het smokkelen betreft was er geen vaste modus operandi. Naast xtc was er ook sprake van een cocaïnetransport vanuit Zuid-Amerika dat in Nederland werd geregeld.

Casus 115
De organisatie hield zich bezig met mensenhandel, met de verstrekking en het gebruik van valse paspoorten, met handel in verdovende middelen (vooral het uitvoeren van cocaïne vanuit Nederland naar Italië) en met het witwassen van geld.

Casus 116
Mensenhandel. In Roemenië werden vrouwen benaderd, die tewerkgesteld werden in clubs, bars of op een tippelzone. De vrouwen werd voorgehouden te gaan dansen in een club of te gaan bedienen in de horeca. Het transport werd uitgevoerd met een autobus van een regulier personenvervoerbedrijf en met minibusjes.

Casus 117
Mensenhandel. In Bulgarije werden vrouwen benaderd die vervolgens in Nederland in de prostitutie terechtkwamen. Vervoer geschiedde per vliegtuig, auto of minibusje.

Casus 118
Ondergronds bankieren en mensensmokkel. Het merendeel van de transacties betrof de inleg in Nederland van kleine geldbedragen door personen van voornamelijk Irakese afkomst, bestemd voor familie in Irak. De hoofdverdachte is als organisator en coördinator betrokken geweest bij enkele mensensmokkeltransporten en ook fungeerde hij als borgsteller voor de financiële afhandeling van mensensmokkeltransporten.

Casus 119
Witwassen van crimineel vermogen en handel in drugs. Voor het witwassen werd gebruikgemaakt van diverse rechtspersonen in Nederland en Luxemburg. De verdovende middelen betroffen voornamelijk cocaïne, die per vliegtuig en boot vanuit Zuid-Amerika naar Nederland werd vervoerd, en om xtc die naar Zuid-Amerika werd gebracht. In een woning werd een hennepkwekerij aangetroffen.

Casus 120
Afpersing, waarbij de hoofdverdachte de rol van afperser had. De afpersing vond plaats rondom vastgoedtransacties.

Casus 121
Afpersing van een aantal personen uit de vastgoedwereld en witwassen van de afgeperste gelden. De hoofdverdachte had daarbij de rol van afperser. De modus operandi kwam er (onder meer) op neer dat de slachtoffers een verzonnen probleem werd gepresenteerd en vervolgens werd tegen betaling een oplossing voor dat probleem aangeboden.

Casus 122
Hasjhandel, productie van hennep en witwassen. De hasj werd vanuit Marokko naar West-Europa vervoerd. Door de organisatie werden verder diverse hennepkwekerijen geëxploiteerd waartoe, al dan niet onder valse naam, verschillende locaties werden gehuurd. De hoofdverdachte was ook betrokken bij verschillende growshops.

Casus 123
Mensenhandel. Het netwerk was actief in de prostitutie en hield zich bezig met het uitbuiten van verschillende vrouwen. Deze werden tewerk gesteld in Amsterdam, Utrecht, Alkmaar, Den Haag en Antwerpen. De vrouwen waren voornamelijk afkomstig uit Duitsland en Nederland, een kleiner deel kwam uit (voormalig) Oost-Europese landen.

Casus 124
Smokkel van cocaïne van Zuid-Amerika naar West-Afrika (voorbereidingshandelingen, er is nooit een concreet transport onderschept) en witwassen. Een lege boot werd de zee opgestuurd vanuit Zuid-Amerika en vervolgens bevoorraad met cocaïne via kleinere scheepjes. Het lossen van de lading bij West-Afrika ging ook met kleinere bootjes. Zo werd de gehele problematiek rond het in- en uitschepen van boten in havens voorkomen.

Casus 125
Mensenhandel. Het ronselen van vrouwen gebeurde in Hongarije, waarbij het slachtoffer iemand leerde kennen die dan vertelde dat er veel werk was in Nederland. De vrouwen werd voorgehouden dat zij in een bar of elders in de horeca konden werken. Eenmaal in Nederland bleek dat zij in de rosse buurt moesten werken. Sommige vrouwen wisten overigens dat zij in de prostitutie terecht zouden komen.

Casus 126
Invoer van cocaïne door medewerkers van de bagagekelder Schiphol en witwassen. Koffers met cocaïne worden de medewerkers onderschept en buiten het luchthaventerrein gebracht.

Casus 127
Productie en (internationale) handel in synthetische drugs, invoer en handel in precursoren en witwassen. De organisatie liet verdovende middelen door anderen produceren. Daarom moesten 'laboratoriumeigenaren' zo veel mogelijk zelf zorgen voor de apparatuur en een locatie. Er werd 113 kg. amfetamine in beslag genomen. Andere trajecten (invoer PMK en de productie van LSD) mislukten.

Casus 128
Invoer cocaïne vanuit Midden- of Zuid-Amerika naar Nederland en witwassen. De cocaïne werd voor de kust van Zuid-Amerikaans land door kleine boten naar grote zeeschepen gebracht. Voor de kust van Nederland werden de partijen cocaïne middels kleine boten weer van de zeeschepen afgehaald. Ook vond transport plaats via luchthavens, waarbij koeriers werden ingezet die de cocaïne via een koffer met dubbele bodem probeerden Nederland in te smokkelen.

Casus 129
Mensenhandel, mensensmokkel en het vervalsen van reisdocumenten. Minderjarige meisjes werden in Nigeria geronseld om onder valse voorwendsels in landen als Italië en Spanje in de prostitutie te gaan werken. Nederland was daarbij transitland.

De meisjes dienden zich in Nederland als asielzoeker aan te melden. Daar de slachtoffers minderjarig waren, werden zij in open opvangcentra geplaatst. Dit maakte het voor de criminele organisatie in Nederland relatief eenvoudig om de slachtoffers uit de centra te halen, waarna zij verdwenen. Ruim vijftig meisjes werden door de organisatie verhandeld, waarvan er uiteindelijk maar tien werden teruggevonden.

Casus 130
Productie van en (internationale) handel in xtc en witwassen. Zo zien we de uitvoer van xtc naar de VS, handel in PMK, de invoer van aceton vanuit België naar Nederland, uitvoer van xtc naar Australië, uitvoer van xtc naar België. Vervoer werd op verschillende wijzen gedaan, zoals in jerrycans, kroonluchters, in een metalen kluis, een pizzaoven, PVC-pijpen en bloempotten.

Casus 131
Poging tot invoer in Nederland van 485 kg cocaïne (subsidiair de voorbereidingshandelingen daartoe) en witwassen. De cocaïne kwam uit Colombia, vervolgens werd het in Brazilië, Uruguay of Argentinië verpakt, en in Nederland ontvangen en in kleinere porties verdeeld om door te zenden naar andere Europese landen.

Casus 132
Productie en verkoop van xtc, die echter geen (of nauwelijks) MDMA bevatte maar mCPP. Dit middel staat niet op de lijst van de Opiumwet maar valt onder de Wet op de geneesmiddelen. MCPP is een poeder dat, na toevoeging van bijvoorbeeld een antibraakmiddel, meteen tot pillen geslagen kan worden. Je hebt daar alleen een recept voor nodig en een tabletteermachine.

Casus 133
Handel in versnijdingsmiddelen. Verdachten kochten paracetamol en cafeïne in bij de reguliere handel. Zij verkochten het door aan personen die de stoffen gebruikten als middel om onder meer heroïne mee te versnijden.

Casus 134
Leveren van verwarmingsmantels, rondbodemkolven en andere laboratoriumbenodigdheden door een glasblazer aan personen die deze apparatuur gebruikten voor de productie van synthetische drugs.

Casus 135
Een glasblazer houdt zich bezig met het vervaardigen van materiaal (vooral de aanpassing van kolven) voor de productie van synthetische drugs. Dit materiaal wordt afgenomen door producenten van synthetische drugs.

Casus 136
Witwassen, valsheid in geschriften, oplichting en belastingfraude. Het witwassen had onder meer betrekking op miljoenen euro's aan afgeperst geld.

Casus 137
Heroïnehandel. De heroïne werd ingekocht in Turkije en per auto naar Nederland vervoerd. De groep versneed de heroïne en verkocht het aan lokale afnemers en aan afnemers in Frankrijk, Duitsland, België en Ierland. Nederland fungeerde als transitland. Vrouwen fungeerden als tolk.

Casus 138
Hennephandel en witwassen. De groep hield zich bezig met inkoop, bewerking en verkoop van hennep. De natte hennep werd ingekocht via tussenpersonen. De eindafnemers kwamen uit België, Duitsland en Polen, maar er werd bemiddeld door tussenpersonen die in Nederland woonden.

Casus 139
Cocaïnehandel en witwassen. De hoofdverdachten importeerden de drugs vanuit Peru en Brazilië, soms via Suriname, naar Nederland. De drugs werden binnengesmokkeld via Schiphol of per boot afkomstig uit Brazilië via de haven van Vlissingen. Voor het vervoer van de drugs worden koeriers ingeschakeld die de drugs meenemen in een koffer (smokkel per vliegtuig) of tas (boot). Daarnaast werken de broers ook met bolletjesslikkers.

Casus 140
Cocaïnesmokkel door een groepering die voor een belangrijk deel bestaat uit familieleden en wordt aangevoerd door een vrouw. De familie importeert de drugs vanuit Venezuela via Colombia naar Curaçao en van daaruit wordt het per vliegtuig meegesmokkeld naar Nederland. Het wordt (onder meer) via bolletjesslikkers het land binnen gevoerd.

Casus 141
Het ging om een officiële bank die echter zonder vergunning vanuit Nederland opereerde en in een aantal gevallen naliet om een MOT-melding te doen.

Casus 142
Beleggingsfraude. De verdachten zetten een onderneming op waarvan zij het deden voorkomen dat deze investeerde in vakantieressorts. Via mooi ogend promotiemateriaal en professioneel uitziende prospectussen wisten zij beleggers te trekken om te investeren. Het ingelegde geld werd echter grotendeels niet geïnvesteerd maar verdween in de zakken van de daders.

Casus 143
Vastgoedfraude. Het crimineel samenwerkingsverband verhoogde de kosten van een bouwproject dat in opdracht van een vastgoedfonds werd uitgevoerd. Als gevolg hiervan had dat fonds teveel betaald aan verdachten G en H. Deze sluisden het teveel betaalde bedrag vervolgens door naar verdachten K, O en R. Het project is overigens nooit gerealiseerd.

Casus 144
Vastgoedfraude. Het project X was een project van een vastgoedfonds voor eindbelegger Z. Vermoedelijk had hoofdverdachte A van het vastgoedfonds verdachte J van de eindbelegger omgekocht, waardoor J akkoord was gegaan met een te hoge verkoopprijs. Er werd veel gewerkt met onderaanneming en bouwclaims, waardoor het geheel erg onoverzichtelijk is gemaakt. Hierdoor kon de ruimte gecreëerd worden voor de fraude, ook door middel van kosten-batenanalyses. Vervolgens is het geld op basis van valse facturen doorgesluisd naar verschillende bedrijven. Uiteindelijk is het grootste deel van het geld terechtgekomen bij de hoofdverdachten.

Casus 145
Vastgoedfraude. Het betrof veronderstelde fraude met vastgoedtransacties. Verdachten werden echter vrijgesproken.

Casus 146
Witwassen door middel van ondergronds bankieren. De hoofdverdachten opereerden vanuit een telecomwinkel. Hun bedrijf was een legale onderneming en vormde tegelijkertijd een belangrijk knooppunt voor een netwerk van ondergronds bankieren.

Casus 147
Witwassen van criminele gelden, valsheid in geschrifte, faillissementsfraude. Als woningbemiddelaar zocht de hoofdverdachte naar woningen voor zijn klanten uit het criminele milieu. Hij maakte voor zijn klanten onder meer valse documenten op, schakelde katvangers in, nam contant geld aan en betaalde 'salaris' uit. Hierdoor werd de (ware) identiteit van de klant voor de autoriteiten, voor makelaars en voor verhuurders verhuld. Vaak ging het gepaard met hypotheekfraude, doordat valse inkomensgegevens werden verstrekt.

Casus 148
Witwassen van criminele gelden. De hoofdverdachten waren een autoverhuurbedrijf begonnen om klanten, veelal afkomstig uit het criminele milieu, de mogelijkheid te geven ook contant en 'anoniem' te kunnen betalen. Auto's werden op naam gezet van het bedrijf of van een katvanger. Het bedrijf voldeed de verzekering en belastingen en betaalde zelfs verkeersboetes en dit werd verrekend in de prijs.

Casus 149
Witwassen van geld door middel van ondergronds bankieren. Hoofdverdachte A opereerde vanuit een woning, waar klanten geld kwamen halen en brengen. A kreeg van hoofdverdachte B uit Pakistan door wie er geld kwamen brengen en vervolgens werd het geld, na instructies van B, uitbetaald aan andere klanten. A fungeerde in die zin als een verdeelcentrum. Daarnaast kwamen er ook klanten geld wisselen van kleine naar grote coupures.

Casus 150
Witwassen van gelddoor middel van ondergronds bankieren. Het crimineel samenwerkingsverband opereerde vanuit een wasserette, waarvan de hoofdverdachten eigenaar waren. Daar kwamen klanten langs die geld wilden overboeken. De overboekingen gingen voornamelijk van Engeland naar Nederland. Ook vonden er vermoedelijk overboekingen plaats naar Thailand, Turkije, Pakistan en Dubai.

Casus 151
Cybercrime / drugssmokkel. Het CSV hackte met behulp van personen met computerkennis de computersystemen van twee bedrijven (terminal/rederij) en gebruikte die hack om containers met drugs vanuit de Antwerpse haven binnen te halen. De containers werden afgehaald voordat de reguliere bedrijven dit konden doen.

Casus 152
Cybercrime / drugs- en wapenhandel. Via online markplaats(en) werd gehandeld in cocaïne, hasj, heroïne, xtc , amfetamine en wapens. De goederen werden verstuurd binnen Nederland en naar afnemers in Zweden, België, Frankrijk, Duitsland, het VK.

Casus 153
Cybercrime. Computers en mobiele telefoons werden besmet met malware, met als doel frauduleuze banktransacties uit te voeren. Na inloggen op 'internetbankieren', werden slachtoffers doorgeleid naar een door de verdachten gemanipuleerde internetpagina.

Casus 154
Cybercrime. Een variant van skimmen (ook wel shimmen genoemd) waarbij niet de magneetstrip van een bankpas werd gekopieerd, maar waarbij het dataverkeer werd afgevangen tussen de pas en de terminal waar deze pas werd ingestoken. De aldus verkregen informatie werd op passen geladen waarmee vervolgens op verschillende plekken in de wereld geld werd opgenomen.

Casus 155
Cybercrime. Via banking malware werd geld van rekeningen gehaald. Slachtoffers ontvangen een mail die afkomstig lijkt van een energiebedrijf. In de mail wordt het slachtoffer verzocht een openstaand bedrag te voldoen, waarbij via een link meer informatie kan worden verkregen over de factuur. Wanneer op de link wordt geklikt, wordt de malware geladen. Via deze malware wordt geld vanaf bankrekeningen weggesluisd naar bankrekeningen die waren geopend door speciaal daarvoor geworven money mules. Daarna verdween het geld door middel van cashopnamen en overboekingen naar andere rekeningen.

Casus 156
Cybercrime. Phishing. Slachtoffers ontvingen e-mails die afkomstig leken te zijn van hun bank en waarin om bepaalde informatie werd gevraagd. Vervolgens belde een nep-bankmedewerkster met een verhaal over de beveiliging van de site van de bank, waarna de slachtoffers een code moesten geven (TAN-code). Vanaf dat moment werd ook meteen geld van de rekeningen gehaald.

Casus 157
Witwassen van waarschijnlijk uit drugshandel afkomstig geld. De hoofdverdachte ontvangt contant geld, vermoedelijk afkomstig van cocaïnehandel, en geeft dat door aan andere mensen. Een andere hoofdverdachte geeft hem het geld. De geldtransporten hebben vermoedelijk Zuid-Amerika als eindbestemming.

Casus 158
Hennepteelt. Het CSV wilde in Spanje hennep verbouwen in het kader van een zogenoemde Cannabis Social Club. Dit wordt daar juridisch beschouwd als een soort 'rokersclub', waarvan men lid kan worden en waarbij het onder strikte voorwaarden mogelijk is om in verenigingsverband legaal hennep te kweken en te gebruiken. Uiteindelijk worden grote hoeveelheden hennep en marihuana in beslag genomen en ook hasj en cocaïne.

Casus 159
Cocaïnesmokkel vanuit Suriname. Een CSV had een eigen schoonmaakbedrijf op de luchthaven Schiphol. Via het schoonmaakbedrijf kregen daders toegang tot vliegtuigen waarna zij de verborgen cocaïne uit de vliegtuigen konden halen.

Casus 160
Mensensmokkel/-handel. Filipijnse werknemers werden in dienst genomen voor de Nederlandse binnenscheepvaart. Door het CSV werden voor de Filipijnse werknemers een verblijfsvergunning en een tewerkstellingsvergunning aangevraagd, waarbij een valselijk opgemaakte arbeidsovereenkomst werd overlegd.

Casus 161
Productie van en handel in synthetische drugs en softdrugs, export van harddrugs naar Groot-Brittannië, witwassen en ondergronds bankieren. Drugs werden door de afnemer afgehaald in Nederland, of werden met vrachtwagens vervoerd in tassen.

De productie van synthetische drugs had het CSV in eigen hand en de geldstromen liepen o.a. via ondergronds bankieren.

Casus 162
Drugssmokkel. Verschillende soorten drugs (amfetamine, hasj en cannabis) werden in vrachtwagens naar onder andere Engeland, Spanje en Frankrijk vervoerd. Hiervoor werd deels gebruikgemaakt van reguliere transportbedrijven.

Casus 163
Cocaïnesmokkel. Een CSV waarvan verschillende drugshandelaren deel uitmaakten, importeerde cocaïne vanuit Zuid-Amerika via de Rotterdamse haven. Daarbij werd gebruikgemaakt van een douanier, die ervoor kon zorgen dat containers met drugs niet door werden gecontroleerd.

Casus 164
Drugshandel. Het CSV handelde in heroïne vanuit Turkije en in cocaïne vanuit Zuid-Amerika. Om bijeen te komen en tot afspraken te komen met derden werd gebruikgemaakt van een café. Tijdens de onderzoeksperiode werd ook een tweetal hennepkwekerijen ontmanteld.

Casus 165
Criminele organisatie die het plegen van liquidaties tot oogmerk had. Er werd een grote partij (automatische) wapens en munitie aangetroffen.

Casus 166
Witwassen van waarschijnlijk uit drugshandel afkomstig geld. Het CSV nam van opdrachtgevers geld in ontvangst, verstopte het in bergplaatsen in koffers of rugtassen en zorgde ervoor dat deze door geldkoeriers naar Zuid-Amerika werden gebracht.

Casus 167
Cocaïnehandel en witwassen. Het CSV hield zich bezig met drugshandel, het financieren ervan en witwassen. Er werd gebruikgemaakt van eigen vervoermiddelen alsook van reguliere rederijen en luchtvaartmaatschappijen om de aangekochte cocaïne te vervoeren vanuit Zuid-Amerika naar Nederland.

Casus 168
Witwassen. De hoofdverdachte had wederrechtelijk verkregen vermogen opgebouwd uit de logistieke facilitering van handel in drugs. Bij de drugstransporten werd gebruikgemaakt van rechtspersonen in diverse landen die als dekmantel fungeerden. Onder hun naam werden met drugs gevulde machinerieën vervoerd.

Casus 169
Hennepteelt. Door de verdachten werden in verschillende panden hennepkwekerijen opgezet. Ook werd een hennepknipperij opgezet.

Casus 170
Internationale handel in verschillende soorten drugs (onder meer cocaïne, hennep en amfetamine). De illegale handelsstroom omvatte verschillende werelddelen. Er werd onder meer gebruikgemaakt van de zogenoemde freezones van Singapore en Dubai. De smokkel vond plaats in machines, waarbij in holle ruimten drugs werden verborgen.

Casus 171
Drugshandel. Een vooral in Brabant opererend CSV was betrokken bij de productie van en handel in onder meer xtc. Het CSV was tevens betrokken bij de handel in cocaïne, de teelt en handel in hennep en het witwassen van het geld dat hiermee werd verdiend.

Casus 172
Witwassen. De hoofdverdachte opereerde vrij zelfstandig in het ondergronds bankieren, zonder aansturing van *brokers*. Hij had een vast netwerk van tussenpersonen en geldkoeriers. De tussenpersonen introduceerden verschillende klanten bij de hoofdverdachte of lieten geldtransacties plaatsvinden via hem. Tevens werden bij de tussenpersonen, in opdracht van de hoofdverdachte, geldbedragen ingebracht en opgehaald.

Casus 173
Cybercrime. Witwassen van bitcoins. Verdachten kochten bitcoins in van personen die ze vermoedelijk via drugshandel op darknet markets hadden verdiend en gaven daar euro's voor terug. Deze bitcoinwisselaars ontmoeten hun klanten vooral in openbare gelegenheden.

Casus 174
Het CSV bestond grotendeels uit leden van een bekende motorclub. Zij werden verdacht van wapenhandel, drugshandel (hennep en harddrugs) en afpersing.

Casus 175
Drugshandel. Een loods werd door het CSV gebruikt als 'marktplaats', als trefpunt voor een groot aantal kopers en verkopers van drugs en benodigde middelen voor de productie van drugs.

Casus 176
Cocaïnehandel. Een CSV hield zich in Amsterdam en Rotterdam bezig met handel in cocaïne die vanuit Zuid-Amerika werd geïmporteerd. Daarbij werd gebruikgemaakt van boten, vliegtuigen en bolletjesslikkers. Het CSV had zowel contacten in Colombia als in Nederland en België. Drugs en geld werden opgeslagen in stashhuizen van waaruit partijen werden doorverkocht aan afnemers.

Casus 177
Witwassen door middel van ondergronds bankieren. Een ondergrondse bankier voerde in samenwerking met *brokers* illegale geldtransacties uit tussen Engeland en Nederland. Britse ponden werden in Engeland bij een ondergrondse bankier ingebracht en in Nederland uitbetaald. De hoofdverdachte maakte daarbij gebruik van meerdere geldkoeriers. De herkomst van het geld betrof vermoedelijk drugshandel.

Casus 178
Witwassen door middel van ondergronds bankieren. Het ging om ondergrondse bankiers die grote contante geldbedragen uitbetaalden en in ontvangst namen in Nederland, veelal in opdracht van *brokers* in het buitenland. Gezien de werkwijze en grootte van de bedragen bestond het vermoeden dat het geld afkomstig was uit de opbrengst van enig misdrijf.

Casus 179
Fraude en witwassen/overige delicten. Met behulp van vals opgemaakte e-docu-

menten werden hypotheken aangevraagd en werden bouwdepots leeggetrokken. Ook werd een aantal kilo hasj en een vuurwapen aangetroffen.

Casus 180
Witwassen. Er vinden op bankrekeningen van rechtspersonen contante stortingen plaats van in totaal miljoenen euro's. Vervolgens wordt geld doorgeboekt naar rekeningen in het buitenland, onder meer China en Hong Kong. Het vermoeden bestond dat op deze manier geld werd witgewassen dat door anderen met drugshandel was verdiend.