VU VRIJE UNIVERSITEIT AMSTERDAM
CIROC Centre for Information and Research on Organised Crime
Universiteit Utrecht
Erasmus Universiteit Rotterdam
Maastricht University
Wetenschappelijk Onderzoek- en Documentatiecentrum Ministerie van Veiligheid en Justitie

UWSBRIEF NIEUWSBRIEF NIEUWSBRIEF NIEUWSBRIEF **NIEUWSBRIEF 35** 17e jaargang · nr 1 · oktober 2017 N

Inleiding

Op 1 september 2017 heeft prof. dr. Henk van de Bunt, een van de drijvende krachten en oprichters van het Centre for Information and Research on Organised Crime, na een wetenschappelijke carrière van ruim veertig jaar afscheid genomen als hoogleraar criminologie aan de Erasmus Universiteit Rotterdam. Tijdens zijn drukbezochte afscheidscollege getiteld 'Achter de muren van stilzwijgen en geheimhouding: de burgemeester, de soigneur en de fraudeur' maakte hij met de introductie van het concept 'mega crime' duidelijk dat zijn emeritaat niet het einde van zijn wetenschappelijke carrière betekent. Ook zal hij actief blijven binnen CIROC. Het liber amicorum voor Henk van de Bunt '*Over de muren van stilzwijgen*' bevat verschillende interessante bijdrages over georganiseerde misdaad. Ter ere van zijn emeritaat werd Henk van de Bunt tijdens een plechtige afscheidsbijeenkomst tot officier in de Orde van Oranje-Nassau benoemd. De bestuursleden van CIROC feliciteren hem met deze koninklijke onderscheiding en wensen hem al het goede toe met deze nieuwe fase in zijn leven.

Deze CIROC-nieuwsbrief verschijnt aan de vooravond van een studiemiddag getiteld 'Liquidaties in Nederland: verschijningsvormen en aanpak'. Tijdens deze studiemiddag zal aandacht worden besteed aan enkele nieuwe ontwikkelingen op het gebied van liquidaties en de consequenties en dilemma's die deze ontwikkelingen met zich meebrengen voor de aanpak van liquidaties. Barbra van Gestel, een van de sprekers tijdens deze studiemiddag, beschrijft in deze nieuwsbrief enkele centrale bevindingen uit een voorstudie over liquidaties, waarbij een trend van professionalisering van observatiemethoden en contrastrategieën samen lijkt samen te gaan met een verdere verruwing en onervarenheid bij de uitvoering van liquidaties.

Verder bevat deze CIROC-nieuwsbrief een bijdrage over de stand van zaken van de bestuurlijke aanpak van georganiseerde misdaad over 2016 op basis van gesprekken met deelnemers in de RIEC-samenwerking en digitale bevraging van coördinatoren en gemeentelijke hoofden openbare orde en veiligheid. Het derde artikel handelt over mobiel banditisme en de vraag hoe en door wie of wat mobiele bendes in Nederland worden gefaciliteerd. Er blijkt in de legale beroepsgroep een opmerkelijke faciliterende rol voor de marktkraamsector te zijn weggelegd en ook Facebook speelt een belangrijke rol als virtuele ontmoetingsplaats voor bendeleden die zich in verschillende Europese landen bevinden.

De drie hier op volgende artikelen gaan over verschillende vormen van georganiseerde cybercrime en de complexiteit van de opsporing hiervan, over cybercrime in relatie tot witwassen en de cruciale rol van bitcoins hierbij en tot slot over het Internet of Things. Dit Internet of Things gaat over een netwerk van 'slimme apparaten, sensoren en objecten die met elkaar en met het internet verbonden zijn.' De auteurs concluderen onder andere dat producenten onvoldoende veilige toepassingen op de markt zetten die mogelijkheden bieden voor cybercriminelen die zich op afstand toegang kunnen verschaffen tot systemen.

In de laatste bijdrage staan twee studies naar orgaanhandel en mensenhandel met het oogmerk van orgaanverwijdering centraal. Empirisch onderzoek naar orgaanhandel is veelal medisch van aard en kennis over de achterliggende criminele netwerken en actoren is dan ook schaars. Dat maakt beide onderzoeken die zich baseren op onder andere interviews met patiënten die reisden voor betaalde niertransplantaties en transplantatiespecialisten (Ambagtsheer) en de analyse van verschillende buitenlandse strafzaken (De Jong) bijzonder.

Prof.dr. Richard Staring (Criminologie, EUR)

INHOUDSOPGAVE

Analyse

Liquidaties in Nederland
Dr. Barbra van Gestel (WODC)

Sinds de dubbele liquidatie op 29 december 2012 in de Staatsliedenbuurt in Amsterdam - waarbij kogels door de straten vlogen die ook willekeurige auto's en woningen raakten - is Nederland opgeschrikt door tientallen moordzaken waarbij sprake was van excessief vuurwapengebruik op de openbare weg. Hoewel liquidaties geen nieuw fenomeen zijn in Nederland (het aantal schommelde in de afgelopen decennia tussen de 20 en 30 per jaar), zijn er wel geluiden dat de aard van het delict verandert. Bij de het ministerie van Veiligheid en Justitie bestond de behoefte aan een overzicht van bestaande kennis hieromtrent en het WODC is daarom gevraagd een verkennende studie te verrichten naar deze thematiek. Voor die studie is geïnventariseerd welke kennis over dit onderwerp aanwezig is op de 'werkvloer' van de opsporing. Daarvoor hebben we gesprekken gevoerd met twaalf sleutelinformanten; met politie- en justitiefunctionarissen die met de opsporing en vervolging van liquidaties zijn belast en vanuit die hoedanigheid kennis hebben over het fenomeen. Aanvullend hebben we drie interne politiedocumenten bestudeerd die goeddeels gebaseerd waren op operationele opsporingsinformatie. Voorts is informatie uit verschillende openbare journalistieke bronnen geraadpleegd. De informatie is vergaard in de periode april 2016-november 2016. In deze bijdrage staan de belangrijkste bevindingen.

Conflicten
Liquidaties zijn volgens geïnterviewde sleutelinformanten meestal het gevolg van conflicten die gerelateerd zijn aan de handel in drugs. Het gaat bijna altijd om geld en om de verdeling van de drugsmarkt. De achterliggende motieven voor liquidaties zijn volgens sleutelinformanten door de tijd heen niet of nauwelijks veranderd. Wel is het aantal spelers op de drugsmarkt volgens hen toegenomen; er zijn steeds meer mensen in Nederland die in de drugshandel werkzaam zijn. Tegelijkertijd is een deel van de grote spelers uit de zogenoemde 'Hollandse netwerken' weggevallen doordat ze zijn geliquideerd of opgepakt, en hebben nieuwe spelers hun plek ingenomen. Geïnterviewde sleutelinformanten hebben de indruk dat deze ontwikkelingen leiden tot onrust en verschuivingen in machtsposities en daarmee gepaard gaande conflicten. Dat leidt niet zozeer tot een toename van liquidaties maar mogelijk wel tot een andere samenstelling

van betrokken groepen en tot een andere stijl van werken. Veranderingen in het fenomeen liquidaties die door sleutelinformanten worden gesignaleerd, vinden vooral plaats in de voorbereidende en uitvoerende fase van een liquidatie.

Verruwing
De drempel om een liquidaties te plegen lijkt vandaag de dag lager te zijn dan vroeger, dat stellen althans veel geïnterviewden. De indruk bestaat dat het aantal mensen in Nederland dat bereid is tegen betaling een moordopdracht te plegen, groter is geworden. Schutters zijn steeds vaker '*home grown*', of zoals een politiefunctionaris zegt: 'Lang was het moeilijk om in Nederland mensen te vinden voor het plegen van een liquidatie. Nu vind je ze bij bosjes'. Tegelijkertijd signaleren sleutelinformanten een grotere beschikbaarheid van zware vuurwapens zoals Kalasjnikovs of Scorpions. Het gebruik van deze wapens is niet nieuw maar het lijkt gewoner en meer 'standaard' bij de uitvoering van liquidaties. Voor het hanteren van deze zware volautomatische wapens zijn schietvaardigheden nodig en die vaardigheden blijken veel relatief 'nieuwe' schutters niet te hebben. Ze zijn niet gewend met volautomatische wapens om te gaan en hebben doorgaans veel schoten nodig om een slachtoffer doeltreffend te raken. Mede vanuit die onervarenheid, gaan uitvoerders vaker slordig te werk en lijken ze '*collateral damage*' op de koop toe te nemen. Dat uit zich ook in het schieten op de verkeerde personen, die het doelwit van de liquidatie niet blijken te zijn. Die slordigheid en 'overkill aan geweld' is volgens geïnterviewden vooral te zien bij liquidaties die door een nieuwe generatie cocaïnehandelaren worden uitgevoerd. Maar ook bij woonwagenbewoners en motorclubs wordt de laatste jaren excessiever en grover geweld gesignaleerd bij de uitvoering van liquidaties.

Specialisatie
Tegenover verruwing en onervarenheid bij de uitvoering van liquidaties, bespeuren sleutelinformanten een sterke mate van specialisatie en professionalisering tijdens de voorbereidende werkzaamheden. Afgelopen jaren zijn bij de opsporing gespecialiseerde groepen in beeld gekomen, die in groepsverband voorbereidende handelingen voor hun rekening nemen. De indruk bestaat bij geïnterviewde sleutelinformanten dat het voorbereiden van liquidaties een 'business' op zich is geworden, een bedrijfstak waar personen en groepen zich in hebben gespecialiseerd en waar snel geld mee verdiend kan worden. Voor het volgen en in kaart brengen van potentiele slachtoffers wordt gebruikgemaakt van professionele ICT-apparatuur. Zogenoemde 'voorverkenners' nemen hedendaagse volg- en observatiestrategieën van de politie over en leveranciers van benodigde spionageapparatuur (veelal spyshops) hebben een belangrijke rol gekregen bij de voorbereiding van liquidaties. Bij het wissen van mogelijke dadersporen, wordt ook rekening gehouden met (nieuwe) observatietechnieken van de politie. Criminele groepen die liquidaties voorbereiden, anticiperen op het gebruik van spionage apparatuur door het 'sweepen' (schoonvegen) van auto's en woningen. Er zijn faciliterende bedrijven die deze sweepdiensten aanbieden. Een andere veelgebruikte manier om digitale sporen te wissen is het gebruik van speciaal geprepareerde PGP-telefoons en het vervalsen van kentekenplaten voor gestolen auto's.

Tot slot
Samenvattend kan gesteld worden dat de beschikbaarheid van nieuwe groepen schutters en nieuwe middelen leiden tot een aantal stijlaanpassingen aan de *modus operandi* die bij liquidaties wordt toegepast. Enerzijds zien we een proces van professionalisering van observatiemethoden en contra-strategieën, waarbij gebruik wordt gemaakt van nieuwe technologische middelen. Daarbij wordt sterk geanticipeerd op technieken die de politie hanteert. Digitalisering van middelen en sporen spelen daarbij een voorname rol. Anderzijds wordt een ruwere werkwijze gesignaleerd bij de daadwerkelijke uitvoering van liquidaties. Die verruwing zou kunnen worden toegeschreven aan een ruime beschikbaarheid van zware vuurwapens in Nederland en aan een ruime beschikbaarheid van nieuwe onervaren *home grown* schutters, die bereid zijn tegen betaling een moord te plegen. De combinatie van grofheid, knulligheid en professionaliteit leidt er in de praktijk toe dat dadergroepen, ondanks hun investeringen in professionele digitale afschermingsmethoden, uiteindelijk toch vaak (fysieke) sporen achterlaten. Liquidaties blijven fysieke geweldsdelicten waarbij fysieke handelingen nodig zijn. De grove en slordige werkwijzen zorgen voor veiligheidsrisico's, maar bieden niettemin tegelijkertijd kansen voor de opsporing.

Gestel, B. van, m.m.v. M. A. Verhoeven (2017). *Verkennende voorstudie liquidaties*. Den Haag: WODC. Zie voor het hele rapport https://www.wodc.nl/onderzoeksdatabase/2624-verkennende-voorstudie-liquidaties.aspx

Bestuurlijk boeven vangen: een stand van zaken in de bestuurlijke aanpak van georganiseerde criminaliteit
Dr. John Smits (Arena), mr. Niko Struiksma (Pro Facto) en drs. Bert Schudde (Pro Facto)

De aanpak van georganiseerde criminaliteit is geen exclusieve taak van justitie en politie. Gemeenten vervullen een belangrijke rol bij het opwerpen van barrières tegen het voet aan de grond krijgen van georganiseerde criminaliteit. Ze beschikken over een breed palet aan instrumenten. Bijvoorbeeld door het weigeren van vergunningen aan malafide ondernemers of door het sluiten van drugspanden. Het bevorderen van de bestuurlijke aanpak van georganiseerde criminaliteit (hierna: de bestuurlijke aanpak) is in 2007 verankerd in het programma 'Bestuurlijke aanpak van georganiseerde misdaad', een onderdeel van het kabinetsprogramma 'Veiligheid begint bij voorkomen'. De aanname in het programma is dat de effectiviteit van de aanpak wordt bepaald door voldoende bewustzijn en rolneming van gemeenten, een voldoende bestuurlijke en organisatorische verankering, brede samenwerking én het feitelijk inzetten van instrumenten.

Om gemeenten te helpen bij (de opbouw van) de aanpak, zijn in 2009 Regionale Informatie en Expertise Centra (RIEC's) opgericht, samenwerkingsverbanden, gefinancierd door de gemeenten en het Rijk. In navolging van onderzoeken over 2009 en 2012 is de stand van zaken en ontwikkeling in de bestuurlijke aanpak in 2016 door ons onderzocht. Dit is gebeurd aan de hand van een digitale bevraging van de gemeentelijke hoofden/coördinatoren openbare orde en veiligheid (respons 69%) en gesprekken en werkbijeenkomsten met deelnemers in de RIEC-samenwerking. De bevindingen zijn als volgt.

Algemeen bewustzijn, sense of urgency
Vrijwel alle gemeenten lijken zich bewust van de mogelijke aanwezigheid van georganiseerde criminaliteit. Het feitelijke zicht daarop via bijvoorbeeld ondermijningsbeelden wisselt sterk. Er lijkt een duidelijke relatie tussen het feitelijk inzicht en de 'sense of urgency' rond de bestuurlijke aanpak. Het actueel houden van ondermijningsbeelden is dus essentieel.

Brede onderkenning en vastlegging gemeentelijk rol binnen integrale aanpak
Vrijwel alle gemeenten erkennen hun rol bij de aanpak van georganiseerde criminaliteit en hebben uitgangspunten vastgelegd. Gemeenten (en andere partners) spreken liever niet meer van 'bestuurlijke aanpak' maar van 'integrale aanpak' met daarbinnen een bestuurlijke rol. De regie moet volgens de gemeenten bij de lokale (of regionale) driehoek – justitie, politie, burgemeester – liggen en niet exclusief bij de gemeente, een andere partner of het RIEC. In de reflectie is aangeven dat daar in eerste aanleg ook moet worden bepaald of een zaak wordt opgepakt en welke partner ('wie staat het sterkst') het voortouw neemt.

Lokale organisatie steviger dan 2012 maar blijft fragiel
De lokale organisatie staat steviger dan in 2012 door een duidelijker omlijnde werkstructuur en meer capaciteit. Maar het blijft fragiel, zeker bij kleine(re) gemeenten. De vaak beperkte capaciteit is verdeeld over verschillende taken en verantwoordelijkheden. Tijd voor het bijhouden van kennis en het netwerk is vaak beperkt. Als taken en verantwoordelijkheden bij één persoon liggen, kunnen expertise en continuïteit onder druk komen te staan. Als die bij meer personen liggen is er het risico op versnippering en te weinig 'vlieguren' kunnen maken.

Er is geen eenduidig kader voor waar de lokale organisatie aan moet voldoen. Uit de reflectie komen onder meer de volgende bouwstenen naar voren:
- Organisatie-brede antennes om signalen op te pikken.
- Een coördinatievoorziening om signalen intern en extern te verwerken.
- Aanhaking bij de burgemeester.

- Er is voldoende kritieke massa (in samenwerking): ondergrens aan capaciteit, deskundigheid, competenties en vlieguren (met bestuurlijke aanpak bezig zijn).
- Borging van de aanpak in de beleids- en organisatieprocessen (sluiten beleidscyclus, integraal onderdeel alle beleid, etc.).
- Een gedegen informatiehuishouding (intern en extern)

Het valt te overwegen om capaciteit en deskundigheid – met lokale inzet - (regionaal) te bundelen.

Samenwerking intensiever en meer richting
De samenwerking tussen gemeenten, politie en RIEC's is geïntensiveerd. Wat de samenwerking oplevert is nog diffuus voor gemeenten. De samenwerking heeft meer richting gekregen en toont meer slagkracht. Bijvoorbeeld tussen bestuur, strafrechtelijke partners en de belastingdienst bij het 'ophalen' van crimineel geld.

De RIEC's hebben sinds 2012 bijgedragen aan:
- Meer inzicht en bewustzijn door het opstellen van ondermijningsbeelden;
- Het bevorderen van de samenhang en samenwerking tussen de verschillende partijen;
- Het ondersteunen bij het aanpakken van concrete zaken;
- Het 'pushen' van gemeenten om de bestuurlijk aanpak steviger op de agenda te zetten en passende organisatorische voorzieningen te treffen.

De RIEC's treden bij het 'pushen' van gemeenten soms in de bestuurlijk-politieke arena. Dat heeft risico's. Het is raadzaam dat de RIEC's zich beperken tot informeren en attenderen.

Voor de RIEC samenwerking ligt er de komende jaren een ontwikkelopgave van pionieren naar structureren. Een mogelijk risico is de onduidelijkheid 'van wie het RIEC is'. Met het oog op de continuïteit lijkt het verstandig de bestaande subsidieregeling vanuit het Rijk voort te zetten en een meer programmatisch karakter te geven (focus op organisatieontwikkeling).

Terughoudendheid over beleidseffectiviteit; aanpak in breder perspectief
Over de effectiviteit van de aanpak heerst enige terughoudendheid: instrumenten laten een direct resultaat zien (pand gesloten), maar of het effect daarvan beklijft (criminaliteit geen voet aan de grond) moet nog blijken. Er zijn bovendien uiteenlopende beelden over wanneer het resultaat goed is: teruggedrongen maatschappelijke effecten zoals gevoel onveiligheid of 'bij de wortel uitgeroeid hebben' van georganiseerde criminaliteit? Er is ook nog weinig ervaring met het echt meten van de beleidseffectiviteit van de aanpak.

Gemeenten zien een samenloop tussen het voet aan de grond krijgen van georganiseerde criminaliteit en opgaven op andere terreinen zoals de (jeugd)zorg, werk- en inkomen en armoedebeleid. Dit maakt de positionering van 'de bestuurlijke aanpak' zowel duidelijker ('wat voegt het toe aan het realiseren van integrale lokale opgaven?') als complexer ('dynamische samenhang de integrale taakstelling van de gemeente'). Bijvoorbeeld als zorgvragen en criminaliteit samenkomen in een multi-probleemgezin. Wat wordt dan de lijn: uit de woning zetten of hulp bieden? Hier ligt ook nog een organisatie-ontwikkelingsopgave voor de gemeenten.

Vervolgmeting
Bij een volgende meting lijkt het verstandig om naast de digitale vragenlijst een meer kwalitatief diepte-onderzoek te doen naar actuele en specifieke thema's en vraagstukken georganiseerde criminaliteit. Daarbij dient de respondentgroep verbreed te worden: de bevraging van de ambtelijke coördinatoren/hoofden OOV zal niet perse een zelfde beeld opleveren als een bestuurlijke bevraging, bijvoorbeeld van de burgemeesters.

Smits, J., Struiksma, N., & Schudde, B. (2016). *Bestuurlijke aanpak georganiseerde criminaliteit: Onderzoek naar de stand van zaken in 2016*. Arena Consulting en Pro Facto in opdracht van het WODC. Zie https://www.wodc.nl/onderzoeksdatabase/2673-tweede-meting-bestuurlijke-aanpak-georganiseerde-criminaliteit.aspx

Over grenzen op dievenpad. Over de facilitering van mobiele bendes.
Dr. Barbra van Gestel (WODC)

Rondtrekkende dievenbendes stonden afgelopen decennium regelmatig in de belangstelling, mede omdat het sinds de uitbreiding van de Europese Unie makkelijker is geworden over landsgrenzen binnen Europa te reizen. Afgelopen jaren heeft het WODC-onderzoek verricht naar de facilitering van mobiel banditisme. De centrale vraag was op welke wijze mobiele bendes in Nederland worden gefaciliteerd en welke actoren en omstandigheden daarbij kunnen worden onderscheiden. Kennis over facilitering kan door de overheid worden gebruikt om het criminele bedrijfsproces van mobiele bendes te stoppen of te verstoren. Het onderzoek is in twee delen uitgevoerd. Het eerste deel behelsde een research synthese (2015), waarvoor bevindingen uit bestaande wetenschappelijke publicaties over facilitering van mobiele bendes zijn samengevoegd. De bevindingen uit de research synthese konden worden samengevat aan de hand van drie dimensies, te weten 1) legale beroepsgroepen; 2) sociale relaties en 3) ontmoetingsplekken. Het tweede deel behelsde een empirisch onderzoek naar de inhoud van vijftien strafrechtelijke opsporingsdossiers. In deze bijdrage worden de belangrijkste empirische bevindingen uit dat onderzoek beschreven. Maar eerst volgen enkele kenmerken van verdachten en strafbare feiten uit de vijftien bestudeerde opsporingsdossiers.

Kenmerken verdachten en criminele activiteiten
In de vijftien bestudeerde opsporingsdossiers komen in totaal 100 verdachten voor; 79 mannen en 21 vrouwen. Ongeveer de helft van de verdachtengroepen bestaan alleen uit mannen, in de andere helft zijn ook vrouwen vertegenwoordigd. Zeven verdachtengroepen komen hoofdzakelijk uit Roemenië, twee groepen komen uit Litouwen, twee groepen uit Albanië, één groep komt uit Servië, één groep hoofdzakelijk uit Bulgarije en tot slot bestaat één groep uit Roemenen en Nederlanders. In de bestudeerde casussen maken verdachten zich schuldig aan georganiseerde winkeldiefstal (vijf zaken), inbraken in woningen en bedrijven (vijf zaken), georganiseerde straatroof/zakkenrollerij (twee zaken), (pogingen tot) overvallen (twee zaken) en georganiseerde autodiefstal (een zaak). De verdachten zijn strafrechtelijk vervolgd voor diefstal, diefstal in vereniging gepleegd of diefstal met geweld (Art. 310, 311, 312 WvSr.), vaak in combinatie met opzetheling en heling (Art. 416, 417 WvSr). In drie zaken zijn verdachten ook vervolgd wegens deelname aan een criminele organisatie (Art. 140 Sr.)

Beroepsgroepen als faciliteerders
Als legale beroepsgroep die een faciliterende rol voor mobiele bendes speelt, komt vooral de marktkraamsector aan het licht. Marktkraamhouders die in de bestudeerde strafdossiers in beeld komen, spelen een sleutelrol bij de heling van gestolen goederen uit winkels. Ze onderhouden intensief contact met bendeleden over vraag en aanbod van producten en zorgen voor continuïteit van georganiseerde winkeldiefstal. Terwijl verdachtengroepen hier kort verblijven en snel rouleren, zorgen marktkraamhouders er door hun tussenkomst voor dat er een constant aanbod is van gestolen producten. Het zijn lokaal ingebedde personen, Nederlands ingezetenen, die een schakel vormen tussen mobiele bendes uit het buitenland en lokale markten. Ze zorgen voor verwevenheid tussen bovenwereld en onderwereld en regelen voortdurende toegang tot lokale legale markten. Daarnaast zorgen ze soms ook voor tijdelijke huisvesting van bendeleden.

In de bestudeerde dossiers komen nog andere beroepsbranches in beeld, zij het minder prominent. Het gaat om opslagbedrijven, telefoonwinkels, makelaars en autoverhuurbedrijven. Auto's worden ook aan katvangers verhuurd, op namen van personen die niet aan het loket van de verhuurder verschijnen. Autosloperijen spelen een rol door onderdelen van gestolen auto's op te kopen. De autobranche komt expliciet in beeld als sprake is van diefstal van auto's; als opslagplaats voor gestolen auto's, als bewerker van auto's en als verkoper van gestolen auto's.

Sociale relaties
In de bestudeerde opsporingsdossiers zijn geen relaties zichtbaar met arbeidsmigranten uit het herkomstland van verdachten. Er blijkt geen sprake te zijn van etnische gemeenschappen die in Nederland als springplank fungeren en een faciliterende rol spelen voor mobiele bendes. Wel hebben

de meeste mobiele bendes relaties met een of enkele personen die hier al langer wonen en lokaal zijn ingebed. Deze lokaal ingebedde personen zijn in Nederland al langer actief in de criminaliteit en helpen de verdachten actief, bijvoorbeeld bij het verkrijgen van huisvesting of vervoermiddelen. Op die wijze vormen ze een verbinding tussen mobiele bendes en de Nederlandse samenleving. Vaak betreft het mensen uit het herkomstland van bendeleden, maar niet altijd.

Daarnaast onderhouden mobiele bendes sociale relaties met mensen uit het herkomstland die elders in Europa verblijven en crimineel actief zijn. In de dossiers komt naar voren dat bendeleden onderdeel vormen van een internationaal crimineel circuit waarbij men informatie uitwisselt over lokale markten, lokale contactpersonen en mogelijkheden voor nieuwe samenwerking. Werving van nieuwe bendeleden vindt niet zozeer hier in Nederland plaats maar vooral internationaal en in het herkomstland. Ook bij heling spelen internationale sociale contacten van bendeleden en bindingen met het herkomstland een rol.

Ontmoetingsplekken
Als ontmoetingsplek voor mobiele bendes komen in de bestudeerde dossiers vooral recreatieparken naar voren. Het zijn semipublieke legale plekken waar landgenoten samenkomen, nieuwe samenwerkingsverbanden ontstaan, spullen worden opgeslagen, helers langskomen om zaken te doen en waar internationale postbedrijven een tussenstop maken om pakketten op te halen. Recreatieparken vormen een vaste structuur voor talrijke stappen die mobiele bendes moeten nemen, ze bieden een gelegenheid voor verschillende fasen van het criminele bedrijfsproces. Als bendes of individuele bendeleden na korte tijd weer verder trekken, blijven de recreatieparken een constante factor voor nieuwe groepen en voor de lokaal opererende helers. Ook hier kan gesproken worden van lokaal ingebedde actoren die als schakel fungeren tussen legaliteit en illegaliteit.

Daarnaast vormen sociale media een virtuele ontmoetingsplaats voor bendeleden. In de opsporingsdossiers is met name zicht op de sociale netwerksite Facebook. Via Facebook vindt de (internationale) communicatie tussen bendeleden plaats, de site wordt onder meer gebruikt om elkaar op de hoogte te houden van verblijfsplaatsen, criminele activiteiten en reisplannen. Ook voor het tonen van gestolen spullen en voor vraag en aanbod wordt Facebook gebruikt.
Daarnaast komen nog andere ontmoetingsplekken in beeld, maar minder prominent: in enkele casussen zien we woningen die dienst doen als 'doorgangshuis' en in enkele strafdossiers is zicht op hotels en pensions waar bendeleden verblijven en leden elkaar ontmoeten. Tot slot is in één casus de openbare bibliotheek van een grote stad de vaste ontmoetingsplek voor bendeleden.

Gestel, B, van, Kouwenberg, R.F (2016) *Over grenzen op dievenpad. Een onderzoek naar de facilitering van mobiele bendes*. Den Haag: WODC. Zie: https://www.wodc.nl/onderzoeksdatabase/2625-faciliteerders-van-mobiele-bendes.aspx

Georganiseerde cybercrime in Nederland; bevindingen uit empirisch onderzoek en de implicaties voor de rechtshandhaving.
Dr. G. Odinot (WODC), dr. M.A. Verhoeven (WODC), mr. R.L.D. Pool (WODC) & prof. dr. C.J. de Poot (WODC, VU)

Bijna dagelijks lezen we nieuwsberichten over cybercriminaliteit. De kans om hier slachtoffer van te worden neemt toe en dit is een zorg van burgers, van rechtshandhavers en van beleidsmakers. Over de aard en organisatie van deze vorm van criminaliteit is echter nog niet veel bekend. Om meer inzicht te verkrijgen in de vraag hoe criminele samenwerkingsverbanden op, via en tegen het internet te werk gaan heeft het WODC-onderzoek gedaan. Onderzocht zijn de manieren waarop (georganiseerde) cybercrime wordt opgespoord en de kansen en knelpunten die hierbij bestaan. Ook ging de aandacht in dit onderzoek uit naar de vraag in hoeverre het internet nieuwe '*windows of opportunity*' biedt voor illegale activiteiten en of dit heeft geleid tot structurele veranderingen in de georganiseerde criminaliteit. Om inzicht te verschaffen in deze kwesties zijn verschillende onderzoeksmethoden gebruikt. Zo is er een analyse gemaakt van politiedossiers van opsporingsonderzoeken naar georganiseerde cybercriminaliteit en zijn functionarissen van politie en justitie geïnterviewd.

Traditionele groepen en nieuwe allianties
In de bestudeerde zaken zien we dat traditionele criminele groepen die betrokken raken bij cybercrime hun (traditionele) criminele activiteiten door het internet efficiënter of geavanceerder kunnen uitvoeren. Zoals bijvoorbeeld het online aanbieden van drugs, of het gebruik van het internet of encryptie bij hun 'interne' communicatie. Maar ook zien we nieuwe groepen die heel specifiek cyber-gerelateerde activiteiten ontwikkelen zoals bijvoorbeeld het verspreiden van malware, ransomware en het uitvoeren van Ddos-aanvallen.

Ontwikkelingen op het gebied van internet en informatie- en communicatie technologieën zorgen voor nieuwe vormen en uitvoeringsmogelijkheden van criminaliteit. Het gaat dan bijvoorbeeld om anonimiteit, crime-as-a-service en de mogelijkheid om fora te gebruiken. Ook zorgen deze ontwikkelingen voor nieuwe manieren om slachtoffers te bereiken, voor meer efficiëntie in de uitvoering en voor vergroting van de financiële opbrengst van criminaliteit. Deze ontwikkelingen zorgen ervoor dat criminaliteit waarbij coördinatie van verschillende activiteiten is vereist, in feite eenvoudiger en toegankelijker lijkt te zijn geworden voor grotere groepen mensen. Dit leidt, afgezien van veranderingen in de modus operandi en de veranderingen in de toegang tot slachtoffers, tot nieuwe spelers in het veld, nieuwe vormen van samenwerking en nieuwe economische structuren. Een voorbeeld van nieuwe spelers zijn faciliteerders die bewust of onbewust en gewild of ongewild criminaliteit faciliteren. Zoals bijvoorbeeld hosting providers, online reclamebureaus, webshops, koeriersbedrijven en telecommunicatiebedrijven. Maar ook zagen we faliciteerders die helpen om zaken af te schermen, zoals dekmantel-ondernemingen, bitcoin handelaren en money mules.

Samenwerking
De manier waarop verdachten met elkaar samenwerken is voor een deel vergelijkbaar met andere vormen van georganiseerde misdaad. Maar er zijn ook aspecten van de georganiseerde cybercriminaliteit die enigszins verschillen. Zo kunnen online activiteiten anoniem worden uitgevoerd en zijn offline contacten tussen 'partners in crime' niet perse nodig om criminaliteit te plegen. Ook nieuw is het aspect *crime-as-a-service* waarbij bepaalde taken of diensten online kunnen worden gekocht. ICT-geschoolde mensen kunnen hun diensten verkopen. Binnen zo'n samenwerking ondernemen verschillende individuen specifieke activiteiten. De noodzaak om offline, face-to-face contact te hebben bestaat niet meer. Fora, online communicatie platforms, spelen hier een belangrijke rol in. Hier weet men elkaar te vinden en wordt kennis, software, scripts, goederen en producten gedeeld en aangeboden. Er kunnen contacten gelegd worden die betrekking hebben op criminele activiteiten (op het internet). Het feit dat men hierbij anoniem kan blijven, blijkt een belangrijk aspect.

Verdeelde verantwoordelijkheden en de rol van vertrouwen
In tegenstelling tot de meer traditionele georganiseerde misdaadgroepen, lijken nieuwere groepen binnen cybercriminaliteit te verschillen in hun lange termijn perspectief binnen de samenwerking. Individuen hebben weliswaar een lange termijn perspectief ten aanzien van hun eigen activiteiten, maar de samenwerkingsverbanden lijken minder stabiel en kennen in mindere mate een lange termijn perspectief voor het uitvoeren van illegale activiteiten. Het wederzijds vertrouwen dat in de offline criminaliteit een belangrijke rol speelt, lijkt het bij online samenwerkingsverbanden minder noodzakelijk te zijn om een stabiele groep te vormen. De kwaliteit van iemands kennis en kunde speelt een belangrijkere rol en door de anonimiteit is samenwerking minder riskant. Binnen deze lossere netwerken kan samenwerking tussen verdachten de vorm hebben van een keten, waarbinnen mensen die betrokken zijn bij verschillende activiteiten aan elkaar gekoppeld zijn, waarvan de verschillende activiteiten samen een strafbaar feit opleveren. In deze keten-achtige samenwerkingen, werken verdachten wel met elkaar samen, maar zijn zij slechts verantwoordelijk voor een onderdeel van de criminele activiteit. Dit lijkt een nieuw kenmerk van georganiseerde criminaliteit op het terrein van cybercrime, wat een verandering zou betekenen voor de inhoud van het concept georganiseerde criminaliteit.

Het opsporen van georganiseerde cybercrime
De afgelopen jaren is er flink geïnvesteerd in de opsporing van cybercrime en het Team High Tech Crime is de afgelopen jaren hard gegroeid. Echter, het grote aanbod van zaken noodzaakt de politie ertoe om prioriteiten te stellen bij het signaleren en opsporen van zaken. De opsporing is vaak complex en kan het best vergeleken worden met het leggen van een ingewikkelde puzzel waarbij het internet zelf ook vaak als belangrijke informatiebron dient. De vele mogelijkheden om anoniem te acteren maken het lastig en soms onmogelijk om de identiteit van verdachten te achterhalen. Bijzondere opsporingsbevoegdheden worden dan ook regelmatig ingezet in de pogingen om de identiteit van verdachten te kunnen achterhalen. Deze bevoegdheden worden zowel online als offline ingezet.

Om grip te krijgen op traditionele georganiseerde criminele groepen, beschikt de Nederlandse politie over een speciale eenheid, de Criminele Inlichtingen Eenheid (CIE). Een soortgelijke eenheid, waarin rechercheurs van de CIE undercover kunnen samenwerken met mensen in een criminele groep en op deze manier informatie vergaren over criminele activiteiten bestaat echter nog niet voor de online wereld. Het creëren van een goede informatiepositie zou in de toekomst waardevol zijn in de strijd tegen cybercrime.

Aangezien een verdachte zich overal ter wereld kan bevinden, het internet kent immers geen grenzen, vergt het identificeren, lokaliseren, arresteren en uiteindelijk het veroordelen van verdachten vaak een intensieve internationale samenwerking. De rol van Europol bij internationale opsporingsonderzoeken in een zogenaamd Joint Investigation Team (JIT) wordt gewaardeerd. In zaken die daarentegen niet de formele status van een JIT hebben, is men veel tijd kwijt aan rechtshulpverzoeken. Door verschillende prioriteiten, ingewikkeld papierwerk of procedures, worden verzoeken vaak behandeld met een tempo dat onverenigbaar is met de snelheid van het internet. Het overwinnen van dit soort problemen zou aanzienlijke winst kunnen opleveren in de opsporing van (georganiseerde) cybercrime.

Odinot, G., Verhoeven, M.A., Pool, R.L.D. & de Poot, C.J., (2017). *Organised Cyber-Crime in the Netherlands - Empirical findings and implications for law enforcement*. Cahier 2017-1, Den Haag: Boom Juridische uitgevers. Zie https://www.wodc.nl/binaries/Cahier%202017-1_Full%20text_tcm28-244615.pdf

Cybercrime en witwassen: Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware
mr. R.L.D. Pool (WODC)

Over het witwassen bij cybercrime is, vergeleken met witwassen bij andere delicten, relatief weinig bekend. Bij veel delicten verdienen criminelen geld in contanten. Verdiensten uit cybercrime lijken echter in toenemende mate met digitale betalingsmiddelen te worden witgewassen. Met de groei van cybercrime in de laatste jaren is het van groot belang om zicht te krijgen op het witwasproces en de betrokken actoren. Om die reden is dit onderzoek gericht op het witwasproces en het in kaart brengen van de betrokken actoren bij banking malware en ransomware. Banking malware is, kort gezegd, kwaadaardige software die bedoeld is om slachtoffers geld afhandig te maken via betalingen met internetbankieren. Ransomware is kwaadaardige software waarmee iemands computersysteem (of bestanden die zich daarop bevinden) wordt 'gegijzeld' en losgeld wordt geëist om het systeem te ontsleutelen. Sinds een paar jaar is een variant van ransomware in opkomst, genaamd cryptoware, waarbij bestanden op een computer versleuteld worden en het losgeld in de virtuele valuta Bitcoin wordt geëist.

Relatie tussen cybercrime en witwassen
Cybercrime heeft steeds vaker een financieel motief. Bij banking malware wordt elektronisch geld buitgemaakt en bij ransomware wordt het losgeld veelal betaald met vouchers of (in toenemende mate en vooral bij cryptoware) met bitcoins. Het witwassen van deze opbrengsten bestaat uit het verbergen of verhullen van de criminele herkomst van het geld. Kort gezegd, is witwassen in Nederland strafbaar gesteld als opzetwitwassen (art. 420bis Sr), gewoontewitwassen (art. 420ter Sr) en schuldwitwassen (art. 420quater Sr). Bij opzetwitwassen worden de versluierhandelingen (het verbergen of verhullen) van de oorsprong van het 'voorwerp', de plaatsingshandelingen (verwerven, voorhanden hebben, overdragen of omzetten) en omzettingshandelingen (omzetten en gebruikmaken) van een voorwerp uit misdrijf verkregen strafbaar gesteld. Bij schuldwitwassen gaat het om de versluierhandelingen en verplaatsingshandelingen van een voorwerp, waarbij de verdachte redelijkerwijs moet vermoeden dat het voorwerp uit misdrijf afkomstig is. Bij gewoontewitwassen (art. 420ter Sr) worden zwaardere strafmaxima gesteld voor degenen die van het plegen van witwassen een gewoonte maken. De typologieën die zijn ontwikkeld om opzet bij opzetwitwassen te bewijzen, hebben echter vooral betrekking op contant geld bij (veelal) drugsdelicten. In de praktijk bestaat daardoor regelmatig onduidelijkheid over de vraag op welke moment bij transacties of bezit van grote sommen virtuele betalingsmiddelen kan worden gesproken van opzet bij witwassen.

Elektronisch en virtueel geld
Veel typen digitale betalingsmiddelen kunnen worden gebruikt om de verdiensten uit cybercrime wit te wassen. In dit onderzoek wordt een onderscheid gemaakt tussen elektronisch geld en virtueel geld. Elektronisch geld is de digitale weergave van echt geld, terwijl virtueel geld niet door de overheid is gefiatteerd. Virtueel geld kan op zijn beurt centraal of decentraal beheerd zijn en wel of niet inwisselbaar zijn tegen echt geld. Inwisselbaar, decentraal beheerd virtueel geld betreft cryptocurrencies. Veruit de bekendste cryptocurrency is Bitcoin, met 90% van de totale marktwaarde van virtuele valuta.

Banking malware
Bij banking malware wordt vaak gebruik gemaakt van *money mules*. Het geld wordt in dat geval vanaf de rekening van het slachtoffer van banking malware overgemaakt naar een rekening van een *money mule*. Vervolgens neemt de *money mule* het bedrag zo snel mogelijk op bij een geldautomaat (de zogenoemde 'cash-out'). Deze wijze van witwassen kan deels worden verklaard door de voorkeur van criminelen om contant geld in bezit te hebben. Toch wordt uit het dossieronderzoek en de kwantitatieve analyse ook helder dat direct vanaf de rekening van slachtoffers van banking malware, goederen, diensten en/of bitcoins worden aangekocht met behulp van de financiële gegevens van het slachtoffer.

Ransomware
Bij ransomware wordt het losgeld doorgaans in online vouchers of bitcoins geëist. Bij vouchers wordt de waarde van de vouchers doorgaans bijgeschreven op een online account van een e-wallet dienst, waarna het geld verder kan worden witgewassen. Het is ook mogelijk de vouchers door te verkopen of direct te besteden bij een online dienstverlener. Indien het geld in bitcoins is geëist kan de organisatie achter de malware trachten de herkomst van de bitcoins te verhullen door gebruikmaking van een mixing service. Met behulp van een experiment is tevens meer informatie verkregen over mixing services en online witwasdiensten die hun diensten beschikbaar stellen via het 'dark web'. Mixing services maken het mogelijk om bitcoins tegen een commissie om te wisselen tegen andere bitcoins. De bitcoins kunnen vervolgens direct worden besteed of worden omgewisseld bij een fysieke bitcoin handelaar of Bitcoin exchange. Ten slotte zijn er ook gespecialiseerde illegale online dienstverleners aanwezig die bereid zijn digitale en virtuele betalingsmiddelen tegen een commissie om te ruilen voor een betaling naar keuze.

Actoren
Uit de modellen in dit onderzoek kunnen de volgende actoren worden geïdentificeerd: (1) banken, (2) *money mules*, (3) geldtransfer kantoren, (4) Payment Service Providers, (5) webwinkels, (6) voucherdiensten, (7) e-walletdiensten, (8) Bitcoin exchanges, (9) mixing services, en (10) bitcoinhandelaren. Om in kaart te brengen met welke partijen de politie tijdens opsporingsonderzoeken in aanraking zou kunnen komen, zijn in dit rapport de kenmerken van deze actoren beschreven. Met behulp van de transactiegegevens van phishing en banking malware is het mogelijk geweest op gedetailleerde wijze de kenmerken van *money mules* in Nederland in kaart te brengen. Uit dit onderzoek komt bovendien naar voren dat criminelen er in veel gevallen nog steeds voor kiezen om contant geld te gebruiken. Dit komt omdat contant geld snel en anoniem verplaatst kan worden. De omvang van witwassen met contant geld is dan ook vele malen

groter dan het witwassen met digitale betalingsmiddelen waar in deze studie de nadruk op ligt. Of dat in de toekomst zal veranderen, hangt sterk af van de ontwikkelingen rondom digitale betalingsmiddelen en maatregelen die bedrijven en instellingen nemen om witwassen te bestrijden.

Aanbevelingen
Het verdient aanbeveling te overwegen om Nederlandse Bitcoin exchanges te reguleren. Nederlandse Bitcoin exchanges hebben op vrijwillige basis al een uitgebreid palet aan maatregelen genomen om witwassen tegen te gaan. Door regulering zouden zij bijvoorbeeld ook een melding aan de FIU kunnen doen, hetgeen kan bijdragen aan de opsporing van witwassen met de virtuele valuta. Het reguleren van Bitcoin exchanges blijft echter een uitdaging, gezien het feit dat online betalingsdiensten wereldwijd hun diensten kunnen aanbieden en daarbij gevestigd kunnen zijn in jurisdicties met minder strenge regelgeving of een gebrek aan toezicht of handhaving. Daarnaast moeten ook andere partijen, inclusief burgers, technische maatregelen nemen om de kwaadaardige software al aan de voorkant van het proces aan te pakken. Concreet kan daarbij gedacht worden aan het monitoren van netwerkverkeer (ook op phishing e-mails). Burgers en organisaties zouden daarbij in de basis een goede cyberhygiëne moeten aanhouden en regelmatig backups moeten maken. Daarnaast is het ook van belang bewustzijn bij computergebruikers over cybercrime, in het bijzonder ransomware, verder te intensiveren door voorlichting te geven.

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: WODC. Onderzoek en beleid 319. Zie voor de volledige tekst https://www.wodc.nl/binaries/O%26B319_Volledige%20tekst_tcm28-228990.pdf

(Verkeerd) verbonden in een slimme samenleving. Het Internet of Things: kansen, bedreigingen en maatregelen.
Mr. J.J. van Berkel, Mr. R.L.D. Pool, dr. M. Harbers, Mr. dr. J.J. Oerlemans, dr. M.S. Bargh en dr. S.W. van den Braak (WODC)

Het *Internet of Things* (hierna IoT) is een netwerk van 'slimme' apparaten, sensoren en andere objecten die met elkaar en met het internet verbonden zijn. Nu al worden verschillende IoT-toepassingen veelvuldig gebruikt in onze samenleving en in de toekomst zal de adoptie van het IoT alleen nog maar verder toenemen. Het IoT biedt enerzijds kansen door nieuwe technologische mogelijkheden. Anderzijds brengt het ook bedreigingen met zich mee, bijvoorbeeld op het gebied van cyber security. Om de kansen van het IoT te benutten en de bedreigingen te minimaliseren moet hier tijdig op worden ingespeeld. Om deze reden heeft het WODC, in opdracht van de Cybersecurity Raad (CSR), een onderzoek uitgevoerd naar het IoT, de impact ervan op de maatschappij en de handelingsperspectieven van relevante stakeholders. In dit artikel worden kort de belangrijkste bevindingen uit het onderzoek op het gebied van veiligheid en het IoT besproken.

Veiligheid
Het gebrek aan een voldoende veiligheidsniveau blijkt de belangrijkste zorg bij het IoT. Basale veiligheidsmaatregelen zoals het vermijden van standaard gebruikersnamen en wachtwoorden worden nu vaak niet genomen door bedrijven, waardoor het hacken van IoT-apparaten aanzienlijk makkelijker wordt. Een ander probleem is dat IoT-apparaten niet altijd van updates worden voorzien, waardoor ze in de loop der tijd vatbaar worden voor nieuwe veiligheidslekken. Hierdoor blijken de producten die op de markt worden gebracht keer op keer kwetsbaar te zijn voor aanvallen door kwaadwillende personen, waarbij op afstand toegang kan worden verkregen tot het apparaat. Uit een selectie van nieuwsberichten uit de afgelopen maanden blijkt onder meer dat het mogelijk is om een slimme thermostaat op afstand te versleutelen, de beveiliging van een slim slot te doorbreken, de motor van een auto op afstand uit te zetten, en slimme lampen over te nemen. Vervolgens kunnen bijvoorbeeld de instellingen van dat apparaat worden gewijzigd of persoonsgegevens worden gestolen. Criminelen kunnen zo geld verdienen met de exploitatie van IoT-apparaten. Het is bijvoorbeeld goed denkbaar dat een IoT-apparaat wordt versleuteld met ransomware, waarbij losgeld door criminelen wordt geëist alvorens het apparaat weer ontsleuteld wordt. De recente Wannacry-aanval is in dit kader slechts een voorbode van wat er in de toekomst zal kunnen gebeuren met IoT-apparaten.

Oorzaken en maatregelen
Op dit moment worden er door bedrijven onvoldoende maatregelen getroffen om de veiligheid van het IoT te vergroten. Ook de overheid zou (nog) meer kunnen doen om de veiligheid van het IoT te stimuleren. Dit kan worden verklaard door een combinatie van verschillende factoren: 1) de complexiteit van het IoT, 2) een gebrek aan kennis en bewustzijn, 3) een gebrek aan prikkels, en 4) een gebrek aan toezicht en handhaving.

Complexiteit
De complexiteit van het IoT omvat de technologie zelf, de verwerkte data en het speelveld hieromheen. De heterogeniteit van IoT-technologie maakt het lastig om algemene veiligheidsmaatregelen te formuleren. Dit zorgt ervoor dat lokale oplossingen door hun beperkte reikwijdte aan effectiviteit hebben moeten inboeten. De grote rol van data binnen het IoT draagt bij aan de complexiteit door onduidelijkheid over waar data zijn opgeslagen, wie toegang heeft tot en gebruikmaakt van de data en hoe invulling wordt gegeven aan rechten die aan data kunnen worden ontleend. Het speelveld brengt complexiteit met zich mee door de grote hoeveelheid aan (veelal buitenlandse) spelers op de IoT-markt, waardoor het aan overzicht ontbreekt over wie waar verantwoordelijk voor is. Dit probleem wordt verergerd doordat overheden verschillende regels en standaarden hanteren en daarnaast ook andere belangen hebben. Deze complexiteit vraagt om internationale samenwerking waarbij afspraken worden gemaakt over de beveiliging van IoT-toepassingen en de omgang met data die worden gebruikt en geproduceerd door IoT-toepassingen.

Gebrek aan kennis en bewustzijn
Het treffen van maatregelen om veiligheidsrisico's tegen te gaan wordt ook bemoeilijkt door een gebrek aan kennis en bewustzijn over (risico's rondom) het IoT en ICT in het algemeen. Dit geldt voor zowel de overheid, burgers, als het bedrijfsleven. Door dit gebrek aan kennis en bewustzijn zullen deze partijen niet altijd de meest effectieve maatregelen treffen. Het investeren in onderwijs is een belangrijk instrument om veilig internetgebruik en digitale vaardigheden in Nederland te vergroten. Dit geldt voor het basis- en voortgezet onderwijs, maar ook voor het om- en bijscholen van werknemers.

Afwezige prikkels
Het nemen van veiligheidsmaatregelen wordt ook sterk belemmerd door een gebrek aan prikkels bij gebruikers en bedrijven. Gebruikers zijn zich vaak niet bewust van veiligheidsrisico's en ondervinden in veel gevallen ook geen hinder door aanvallen (IoT-apparaten blijven vaak zonder problemen functioneren). Voor bedrijven ontbreekt er een economische prikkel om producten voldoende te beveiligen. Beveiliging kost in de meeste gevallen meer dan het oplevert. Hoewel bij beide partijen prikkels ontbreken, mogen gebruikers er redelijkerwijs van uitgaan dat fabrikanten deugdelijke producten verkopen. Om dit te bewerkstelligen kan de zorgplicht verder worden versterkt. Onder de zorgplicht kan ook de beveiliging van IoT-producten vallen. Aansprakelijkheid op basis van schade veroorzaakt door IoT-producten kan eveneens een belangrijke prikkel zijn voor bedrijven en daarnaast ook dienen als grond voor de zorgplicht.

Waar is toezicht en handhaving?
Het effect van de hierboven beschreven maatregelen wordt beperkt door een gebrek aan toezicht en handhaving. Zonder deze stok achter de deur zijn maatregelen zoals zorgplicht en aansprakelijkheid minder effectief. Middelen voor toezicht en handhaving schieten nu echter (vaak) nog tekort. Meer investeren in toezicht en handhaving ligt daarom voor de hand, maar het gewenste (acceptabele) niveau en de inrichting van toezicht en handhaving zal nader moeten worden bepaald. Tenslotte moet worden opgemerkt dat de (open) normen van de zorgplicht en aansprakelijkheid nu nog vaak tekortschieten. Over de invulling van de zorgplicht voor leveranciers van hard- en software zal verder onderzoek en discussie nodig zijn.

Conclusie
Bedrijven zijn als producent verantwoordelijk voor het realiseren van vei-

lige IoT-toepassingen. Op dit moment gebeurt dat nog onvoldoende door de grote complexiteit van het IoT en een gebrek aan kennis, prikkels, toezicht en handhaving. De overheid kan bedrijven stimuleren door maatregelen te treffen. Geen van de bovenstaande maatregelen vormt op zichzelf een oplossing voor de bedreigingen van het IoT. In plaats daarvan zijn er verschillende samenhangende maatregelen nodig die pas effectief zijn als zij als geheel worden doorgevoerd. Dit vereist een gedragen overheidsvisie, waarbij er één instantie wordt aangewezen als hoofdverantwoordelijke die dit beleid coördineert en stuurt.

Van Berkel, J.J., Pool, R.L.D., Harbers, M., Oerlemans, J.J., Bargh, M.S. & Van den Braak, S.W. (2017). *(Verkeerd) verbonden in een slimme samenleving. Het Internet of Things: kansen, bedreigingen en maatregelen*. WODC Cahiers nr. 2017-08. Den Haag: WODC. Voor meer informatie zie: www.wodc.nl/onderzoeksdatabase/2734-kansen-en-bedreigingen-internet-of-things.aspx

Onderzoek in het buitenland

Orgaanhandel en mensenhandel met het oogmerk van orgaanverwijdering
Dr. Frederike Ambagtsheer (Erasmus MC) & drs. Jessica de Jong (Landelijke Eenheid van de Nationale Politie)

Sinds de jaren tachtig is orgaantransplantatie een slachtoffer geworden van haar eigen succes. Het huidige aantal transplantaties vervult minder dan 10 procent van de wereldwijde behoefte. Onder invloed van de globalisering heeft het orgaantekort patiënten uit geïndustrialiseerde landen naar ontwikkelingslanden gedreven, waar arme individuen hun organen 'doneren' in ruil voor geld. Hoewel het kopen en verkopen van organen (d.w.z. orgaanhandel) wereldwijd verboden is (met uitzondering van Iran), ondervinden journalisten en wetenschappers dat de handel zich in steeds meer landen voordoet. De orgaanschaarste heeft geleid tot een winstgevende zwarte markt waar ongeoorloofde handelingen (zoals rekrutering) en dwangmiddelen (zoals misleiding) worden toegepast met het doel van uitbuiting (d.w.z. mensenhandel met het oogmerk van orgaanverwijdering).

Literatuur
Gezien de illegale aard van de handel zijn er geen betrouwbare gegevens over de omvang. Op basis van de complexe aard van de criminele activiteiten wordt gesteld dat wereldwijd actieve en goed georganiseerde criminele netwerken zijn betrokken, maar literatuur die deze claim ondersteunt is schaars. Het grootste deel van de empirische studies is medisch, gepubliceerd door artsen die schrijven over de uitkomsten van commerciële orgaantransplantaties die door hun patiënten in het buitenland zijn ondergaan (transplantatietoerisme), dan wel antropologisch van aard, gepubliceerd door wetenschappers en NGO's die schrijven over de ervaringen en sociaaleconomische gevolgen van orgaanverkoop vanuit het perspectief van donoren. De meeste publicaties over transplantatietoerisme bevatten geen informatie dat de organen zijn gekocht en daarom illegaal zijn verkregen, laat staan dat ze zijn verkregen door middel van mensenhandel gefaciliteerd door criminele netwerken. Evenzo, binnen de grotere hoeveelheid artikelen die zijn geschreven over donoren die een nier verkocht hebben, bevatten de meeste geen informatie over de omstandigheden waaronder de verkoop plaatsvond en geen aanwijzingen voor mensenhandel, of presenteren enkele aanwijzingen zonder te verwijzen naar (een duidelijke definitie van) mensenhandel. Empirisch onderzoek vanuit het perspectief van andere actoren die (in)direct bij het misdrijf zouden zijn betrokken, zoals handelaren en transplantatiespecialisten, is nauwelijks beschikbaar.

HOTT project
Het zogenaamde internationale HOTT project (getiteld 'Combating trafficking in persons for the purpose of organ removal') dat tussen 2012 en 2015 door de Europese Commissie werd gefinancierd, beoogde deze kennisklоof te verkleinen. Het project had drie doelstellingen: meer kennis en informatie verwerven over mensenhandel met het oogmerk van orgaanverwijdering, meer bewustwording creëren bij stakeholders zoals politie, justitie, beleidsmakers en artsen, en de handhaving van het misdrijf verbeteren. Gedurende het project werden verscheidene studies met diverse onderzoeksmethoden (literatuurstudies, interviews, enquêtes, observaties en documentanalyse) verricht in Zweden, Macedonië, Nederland, Engeland, Israël, Kosovo, VS en Zuid-Afrika. Dit resulteerde in vele publicaties die zijn te vinden op www.hottproject.com, waaronder twee proefschriften die hier worden samengevat: Orgaanhandel geschreven door Frederike Ambagtsheer en Mensenhandel met het oogmerk van orgaanverwijdering geschreven door Jessica de Jong.

Orgaanhandel, Frederike Ambagtsheer
Uit de literatuur blijkt dat bijna alle patiënten waarvan bekend is dat zij (vermoedelijk) organen kochten, hiervoor naar een ander land reisden. Tussen 1971 en 2013 werd van ruim 6000 patiënten gerapporteerd dat zij naar het buitenland reisden voor een niertransplantatie. De meeste reisden naar China, Pakistan en India en ontvingen een nier van een genetisch onverwante donor. Echter, van slechts 1238 (21%) patiënten werd gerapporteerd dat zij voor de transplantaties betaalden. De literatuur geeft dus geen volledig beeld van het daadwerkelijk aantal gekochte nieren.

Verder werden er interviews verricht met 22 patiënten die vanuit Zweden, Macedonië/Kosovo en Nederland naar Pakistan, India, Iran, Rusland, Colombia, China en Irak reisden voor betaalde niertransplantaties. De patiënten die uit Zweden en Nederland vertrokken, waren in het buitenland geboren, hadden veelal een etnische affiniteit met hun bestemmingsland en regelden hun transplantaties met behulp van vrienden en familie thuis of in het buitenland. Drie patiënten uit Macedonië vertelden dat zij hun transplantatie met behulp van handelaren geregeld hadden. Zes patiënten ondergingen zogenoemde pre-emptieve niertransplantaties. Dit betekent dat zij op het moment van hun transplantatie niet op de wachtlijst stonden en geen dialysebehandelingen ondergingen. Dit toont aan dat een lange wachttijd en dialyse-gerelateerde complicaties niet altijd de primaire redenen zijn waarom patiënten naar een ander land reizen voor een niertransplantatie. Patiënten betaalden tussen de €6000 en €45000 voor hun transplantaties. Zes patiënten vertelden dat ze daarnaast hun donoren hadden betaald. Hoewel er vermoedens bestaan dat niet alle nieren legaal verkregen zijn, is de vraag onbeantwoord gebleven of (alle) donoren zijn uitgebuit of betaald.

Uit enquêteonderzoek onder 241 transplantatieprofessionals (hierna TPs) in Nederland bleek dat bijna de helft tussen 2008 en 2013 patiënten behandeld heeft die naar een ander land reisden voor niertransplantaties en waarvan vermoed werd dat ze de nieren hadden gekocht. De meerderheid gaf aan een conflict van plichten te ervaren wanneer zij vermoedden dat hun patiënt een nier ging kopen, omdat ze de koop niet konden voorkomen of de donor niet konden beschermen. Uit meer dan 40 interviews bleek verder dat TPs liever niet willen weten of hun patiënten de nieren gekocht hebben omdat ze zich niet schuldig willen voelen over de mogelijke uitbuiting van donoren en niet belast willen worden met kennis en informatie die ze toch niet mogen melden.

Eén van de aanbevelingen is een meldpunt die het mogelijk maakt voor TPs om anoniem vermoedens van orgaanhandel te rapporteren bij politie en justitie, waarbij de bescherming van de identiteit van patiënten gewaarborgd blijft. Het doel is om politie en justitie te ondersteunen bij het opsporen en berechten van orgaanhandel. Ook wordt er gewaarschuwd voor de negatieve implicaties van het wereldwijd toenemende repressieve beleid tegen orgaanhandel. Een andere aanbeveling is dan ook een door de overheid gereguleerd systeem van financiële stimulering van orgaandonoren. Het doel van een dergelijk systeem is om het aantal orgaandonaties te vergroten en uitbuiting in huidige ongereguleerde markten tegen te gaan.

Mensenhandel met het oogmerk van orgaanverwijdering, Jessica de Jong
Strafzaken in Kosovo, Israël, de Verenigde Staten en Zuid-Afrika tonen dat het verbod op orgaanhandel en de toenemende vraag naar organen sindsdien tot een zeer winstgevende ondergrondse markt heeft geleid waar ontvangers en donoren worden uitgebuit door de toepassing van ongeoorloofde handelingen en dwangmiddelen met het doel van orgaanverwijdering. Ontvangers en donoren zijn gerekruteerd en vervoerd naar het land waar het transplantatiecentrum is gevestigd en/of overgebracht naar een accommodatie of direct naar een medische voorziening waar ze zijn ontvangen en/of geherbergd in afwachting van de transplantatie. Daarbij hebben criminele actoren misbruik gemaakt van hun kwetsbare positie;

ontvangers en donoren worden gedreven door een levensbedreigende ziekte of onafwendbare armoede in hun 'keuze' om een orgaan te kopen of te verkopen. Hun kwetsbaarheid is verder aangetoond door de respectievelijk hoge en lage bedragen die zij hebben moeten betalen en zijn beloofd te ontvangen, en de afwezigheid van een wettelijk mechanisme om hun betaling te verkrijgen indien (gedeeltelijk) achtergehouden of hun geld terug te krijgen als de transplantatie niet is uitgevoerd. Bovendien zijn velen van hen kort na de operatie in een zwakke lichamelijke toestand ontslagen, waarna sommigen postoperatieve complicaties en een (verdere) verslechtering van hun gezondheid hadden en de meeste donoren geen toegang hadden tot nazorg. Criminele actoren hebben ook andere dwangmiddelen toegepast, zoals dwang door te vereisen dat toestemmingsformulieren worden ondertekend zonder tijd te geven de inhoud te begrijpen, en geen redelijke mogelijkheid te bieden de operatie te weigeren, zelfs bij ernstige twijfels, en misleiding door hen niet te informeren over de procedure, de risico's en langetermijngevolgen.

Criminele netwerken en actoren

De criminele netwerken en actoren die op internationaal niveau hun krachten bundelen om illegale transplantaties te faciliteren zijn zeer goed georganiseerd. Dit blijkt uit de betrokkenheid van orgaanhandelaren, de snelheid waarmee de werving en overdracht van meerdere ontvanger-donor-koppels uit verschillende landen naar een medische voorziening in een derde land wordt uitgevoerd en het korte tijdsbestek waarmee de locatie van de transplantatie wordt verplaatst bij tussenkomst van wetshandhavingsinspanningen. Er is vertrouwen tussen netwerkleden op basis van gemeenschappelijke etnische of religieuze achtergronden. Het effectieve risico op arrestatie wordt sterk verminderd door het succesvol verhullen van de illegale aard van de transplantaties, de zwijgzaamheid van ontvangers en donoren en betrokkenheid of omkoping van transplantatiespecialisten en/of politie en justitie. De opsporing van het misdrijf wordt verder belemmerd door het internationale karakter, het beginsel van medische vertrouwelijkheid en het gebrek aan kennis en ervaring van politie en justitie, die de ervaringen van donoren vaak als milde vormen van misbruik zien en terughoudend zijn in het identificeren van ontvangers als potentiële mensenhandelslachtoffers vanwege hun 'actieve' rol. Dit moet echter worden beoordeeld in het licht van het gebrek aan opties en informatie over de procedure, en sluit niet uit dat een dwangmiddel is toegepast, in welk geval het verlenen van toestemming voor de beoogde uitbuiting irrelevant is.

Frederike Ambagtsheer promoveerde op 6 juni 2017 cum laude op haar proefschrift getiteld '*Organ Trade*' aan de Erasmus Universiteit Rotterdam. Jessica de Jong hoopt op 20 oktober 2017 te promoveren op haar proefschrift '*Human trafficking for the purpose of organ removal*' aan de Universiteit Utrecht.

Signaleringen

Ambagtsheer, F. (2017). *Organ Trade*. Dissertatie Erasmus Universiteit Rotterdam. Rotterdam: Erasmus Universiteit Rotterdam.

Berkel, J.J. van, R.L.D. Pool, M. Harbers, J.J. Oerlemans, M.S. Bargh, & S.W. van den Braak. (2017). *(Verkeerd) verbonden in een slimme samenleving. Het Internet of Things: kansen, bedreigingen en maatregelen*. WODC Cahiers nr. 2017-08. Den Haag: WODC.

Bijlenga, N., & E.R. Kleemans (2017). Criminals seeking ICT-expertise: an exploratory study of Dutch cases. *European Journal on Criminal Policy and Research* (online first: August 2017).

Bijleveld, C., & P. van der Laan (eds.) (2017). *Liber Amicorum Gerben Bruinsma*. Den Haag: Boomcriminologie.

Boerman, M. Grapendaal, F. Nieuwenhuis, & E. Stoffers (eds.) (2017). *Nationaal Dreigingsbeeld 2017. Georganiseerde criminaliteit*. Zoetermeer: Dienst Landelijke Informatieorganisatie.

Gestel, B. van, & R.F. Kouwenberg (2016). *Over grenzen op dievenpad. Een onderzoek naar de facilitering van mobiele bendes*. Den Haag: WODC.

Gestel, B. van, m.m.v. M. A. Verhoeven (2017). *Verkennende voorstudie liquidaties.* Den Haag: WODC.

Kleemans, E.R., & M.J. Soudijn (2017). Organised crime. In: N. Tilley & A. Sidebottom (eds.). *Handbook of Crime Prevention and Community Safety* (pp. 394-406). London / New York: Routledge.

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

Leukfeldt, R. (ed.) (2017). *Research Agenda The human factor in cybercrime and cybersecurity*. The Hague: Eleven International Publishing.

Leukfeldt, E.R., E.R. Kleemans, & W.P. Stol (2017). Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks. *British Journal of Criminology 57(3): 704-722.*

Leukfeldt, E.R., E.R. Kleemans, & W.P Stol (2017). A typology of cybercriminal networks. From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change 67(1): 21-37.*

Leukfeldt, E.R., E.R. Kleemans, & W.P Stol (2017). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change 67(1): 39-53.*

Leukfeldt, E.R., A. Lavorgna, & E.R. Kleemans (2017). 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 (online first).*

Nelen, H., & D. Siegel (eds.) (2017). *Contemporary organized crime. Developments, challenges and responses*. New York: Springer.

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

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

Riccardi, M., E. Savona, R. Milani, D. Camerini, E.R. Kleemans, J. Ferwerda, M. Hopkins, & N. Shelton (2017). Assessing the risk of money laudering in Europe. *Final report of project IARM.* Milan: Transcrime.

Smits, J., N. Struiksma, & B. Schudde (2016). *Bestuurlijke aanpak georganiseerde criminaliteit: Onderzoek naar de stand van zaken in 2016.* Arena Consulting en Pro Facto in opdracht van het WODC.

Staring, R., R. van Swaaningen, & K. van Wingerde (2017). *Over de muren van stilzwijgen. Liber amicorum Henk van de Bunt*. Den Haag: Boomcriminologie.

Verhoeven, M. (2017). *Government policies and sex work realities: Human trafficking in the regulated sex industry*. Dissertatie VU Amsterdam. Amsterdam: Vrije Universiteit.

CIROC studiedagen

11 oktober 2017 Liquidaties: verschijningsvormen en aanpak
Paushuize, Utrecht

13 december 2017 Corruptie in de rechtshandhaving
Raadzaal Universiteit Utrecht

COLOFON

Redactie: prof. dr. E.R. Kleemans en prof. dr. R. Staring

CIROC Secretariaat:
Universiteit Utrecht /
Willem Pompe Instituut
Boothstraat 6
3512 BW Utrecht

email: ciroc@uu.nl
tel: 030 2537120 / 7137

www.ciroc.nl