1 Signaleringen

1.1 Inleiding

De doelstelling van het Nationaal dreigingsbeeld is tweeledig: het moet een rationele basis bieden voor de keuze van de criminele hoofdactiviteiten die bij de aanpak prioriteit zullen krijgen, en het moet nieuwe ontwikkelingen en andere opmerkelijke zaken signaleren waarmee bij de bestrijding van de georganiseerde criminaliteit rekening moet worden gehouden. We putten voor deze signaleringen uit de deelrapporten die aan dit NDB ten grondslag liggen. Het gaat om aspecten van georganiseerde criminaliteit die opvallen zonder dat er in de meeste gevallen speciaal onderzoek naar gedaan is en waarvan we denken dat ze in de (nabije) toekomst een belangrijke rol gaan spelen. Soms gaat het om gelegenheden, soms gaat het om (technologische) ontwikkelingen en in andere gevallen om veranderingen in de criminele praktijk. Zo zijn elf signaleringen geselecteerd, die in een viertal clusters zijn ondergebracht:

- *De rol van de overheid*
  Horizontaal toezicht
  Wet- en regelgeving in de milieusector
- *Digitale technologie*
  Internet of Things
  Cloudcomputing
  Crowdfunding
  Blockchain, bitcoin en payment service provider
- *De criminele praktijk*
  Do-it-Yourself
  Crime-as-a-Service
  Criminele uitbesteding en professionalisering
  Criminele veelzijdigheid
- *Georganiseerde criminaliteit in de wijken: onaantastbaarheid en normvervaging*

Aan elk van deze clusters is in dit hoofdstuk een paragraaf gewijd.

1.2 De rol van de overheid

In deze paragraaf wordt de rol van de overheid vanuit twee invalshoeken belicht. De ene betreft de verschuiving van toezicht en controle van de overheid naar private partijen. We zien deze verschuiving vooral in de milieusector en bij de belasting- en accijnsinning. De andere heeft betrekking op de complexiteit van wet- en regelgeving op het terrein van milieuhandhaving.

Horizontaal toezicht

Sinds 2003 zet de overheid in op certificering en accreditatie bij de naleving van wet- en regelgeving.

Zo bestaat er inmiddels binnen het milieudomein een scala aan certificerende instellingen (CI's), die op hun beurt onder toezicht staan van de Raad van Accreditatie (RvA). Certificerende instellingen geven – na een initiële audit – certificaten uit waaruit blijkt dat een bedrijf aan bepaalde eisen voldoet. Ook adviseren zij bedrijven over de wijze waarop deze ervoor kunnen zorgen dat ze aan de eisen voldoen. Bedrijven met zo'n certificaat worden minder gecontroleerd dan andere bedrijven. De CI's worden betaald door de ondernemingen die zij moeten certificeren, het zijn commerciële bedrijven. De Raad van Accreditatie is er om erop toe te zien dat de certificaten op correcte wijze worden verstrekt. Het 'verticale' toezicht (door de overheid op bedrijven) is goeddeels vervangen door 'horizontaal' toezicht (HT).

De inspecties die actief zijn op de milieumarkt (de Voedsel- en Warenautoriteit, de Inspectie Leefomgeving en Transport en de Inspectie Sociale Zaken en Werkgelegenheid) wijzen erop dat de controles van de CI's vaak tekortschieten en niet goed genoeg geregistreerd worden. Ook blijkt dat CI's veelal zeer terughoudend zijn bij het nemen van maatregelen. Zo behouden bedrijven hun certificaat, ook bij herhaalde overtreding. De inspecties verklaren deze bevindingen onder andere uit de marktsituatie bij de certificatie. De CI's zijn commerciële bedrijven die moeten concurreren om opdrachten van bedrijven binnen te halen. De bedrijven zoeken en contracteren CI's die tegen de laagste kosten de ruimste certificaten afgeven. Dit leidt ertoe dat de eerste audit op basis waarvan een certificaat wordt afgegeven niet altijd even streng wordt uitgevoerd. Ook bij vervolgaudits moet de CI er rekening mee houden dat de klant altijd naar een andere CI kan overstappen als deze naar verwachting soepeler zal omspringen met de condities. Wanneer er financiële afhankelijkheid bestaat, is de vereiste onafhankelijkheid van de CI's in het geding.

Vormen van horizontaal toezicht beperken zich niet tot de milieusector, ook bij de belastingheffing en douaneprocedures zien we vormen van horizontaal toezicht. Zo sluit de Belastingdienst HT-convenanten met individuele ondernemingen waarin vastgelegd wordt wat ieders verantwoordelijkheden zijn en welke verwachtingen ieder mag koesteren. Bij horizontaal toezicht werkt de Belastingdienst samen met externe partijen en verschuift het toezichtproces van controle achteraf naar afstemming vooraf. Bij horizontaal toezicht met fiscaal dienstverleners steunt de Belastingdienst op het werk dat de fiscaal dienstverlener voor zijn klant (de ondernemer) doet. De controle wordt in feite uitbesteed aan deze dienstverlener.

Bij de douane krijgt het horizontale toezicht gestalte in de zogenoemde Authorized Economic Operator (AEO). Een AEO is een import- of exportbedrijf dat als veilig en betrouwbaar te boek staat en dat, nadat het op bepaalde criteria is getoetst, als zodanig door de douane gecertificeerd wordt. Deze bedrijven worden minder vaak fysiek en/of administratief gecontroleerd en hebben daardoor minder oponthoud bij het passeren van grenzen. Een AEO-certificaat is in de gehele Europese Unie geldig. Nederland moet dus certificaten van andere lidstaten accepteren en deze bedrijven als veilig en betrouwbaar behandelen, en andere lidstaten moeten op dezelfde manier omgaan met door Nederland gecertificeerde bedrijven. De douane hoeft zich bij deze bedrijven niet meer af te vragen of zij (of hun goederen) diepgaand gecontroleerd moeten worden.
Het is evident dat bij dergelijke vormen van toezicht het risico van misbruik bestaat. In het milieuveld wordt melding gemaakt van fraude bij certificerende instellingen. Ook lijken fiscaal dienstverleners op malafide wijze in te spelen op de toezichtsstrategie van de Belastingdienst. Verder vermoeden experts een verband tussen het aantal teruglopende douaneonderzoeken in Rotterdam en de toepassing van horizontaal toezicht. Door de verminderde controle zouden ook minder overtredingen worden geconstateerd. Ten slotte wordt in het deelrapport over arbeidsuitbuiting gewezen op het gevaar dat een terugtredende overheid en de daarmee gepaard gaande afname van toezicht kunnen leiden tot een toename van de gelegenheden voor arbeidsuitbuiting.

Wet- en regelgeving in de milieusector

Bij milieucriminaliteit gaat het om overtreding van gecompliceerde wet- en regelgeving. Op de inhoud en handhaving hiervan hebben diverse overheden invloed: de landelijke overheid, de provincies en de gemeenten. Daar komt bij dat veel Nederlandse regelgeving voortkomt uit de implementatie van Europese regelgeving. Vanuit de branches wordt niet zelden succesvol gelobbyd voor meer uitzonderingen en nuances in de wet- en regelgeving. Dat maakt alles nog ingewikkelder en maakt handhaving nog moeilijker. Soms bestaat het nettoresultaat uit regels die elkaar gedeeltelijk overlappen of zelfs met elkaar in tegenspraak zijn.
De regelgeving voor transport bijvoorbeeld ziet toe op gevaarlijke stoffen en heeft het veilig vervoeren van de lading tot doel, terwijl milieuregelgeving over gevaarlijke *afval*stoffen spreekt en bescherming van mens en milieu tot doel heeft. Doordat bij het transport van gevaarlijke afvalstoffen niet alleen de gevarenclassificatie komt kijken maar ook afvalstoffenwetgeving, zijn er twee manieren waarop stoffen en mengsels worden ingedeeld. Hierdoor ontstaat in de praktijk nogal eens ‘verwarring’ en worden stoffen foutief ingedeeld, met alle veiligheids- en milieurisico’s van dien.
Het indelen van gevaarlijke (afval)stoffen is bijzonder lastig en kan gemakkelijk fout gaan. Bestanddelen en fysische en chemische eigenschappen van stoffen kunnen doorgaans niet eenvoudig worden bepaald, terwijl een correcte identificatie essentieel is voor de juiste indeling en voor de regels die van toepassing zijn. Bedrijven kunnen economisch voordeel behalen door die indeling te kiezen waarvoor minder eisen zijn gesteld aan transport en verwerking van stoffen.

Hiaten, overlap en onduidelijkheid in de toepassing van wet- en regelgeving bij het transport van gevaarlijke (afval)stoffen vormen een fundamenteel probleem.
De complexe wet- en regelgeving rond milieuproblematiek vormt een niet te onderschatten gelegenheidsstructuur. In combinatie met de verminderde controle ten gevolge van het hierboven beschreven horizontale toezicht, kan deze gelegenheidsstructuur worden beschouwd als een belangrijke criminogene factor. Milieucriminaliteit bestaat immers voor een belangrijk deel uit het nalaten van dingen die volgens de regels hadden moeten gebeuren, en deze regels laten door de invloed van de branches veel ruimte voor interpretatie.

1.3 Digitale technologie

Er zijn relatief veel signaleringen met een digitale component. Dat is niet vreemd in een tijd waarin de samenleving in toenemende mate digitaliseert en ontwikkelingen elkaar razendsnel opvolgen. De impact ervan is waarschijnlijk groot, maar zal pas op langere termijn ten volle duidelijk worden. Ofschoon we deze digitale signaleringen in deze paragraaf individueel behandelen, interacteren ze met elkaar, en daardoor worden de effecten ervan versterkt. De hier genoemde digitale signaleringen voorzien in een legale en legitieme behoefte. Wanneer ze echter gebruikt worden voor criminele doeleinden, gaat er van de gecombineerde en interacterende ontwikkelingen een duidelijke dreiging uit.

Internet of Things

Internet of Things (IoT) verwijst naar de trend om allerlei 'dingen' via wifi of andere draadloze verbindingen aan het internet te koppelen. Het begon allemaal toen naast het internetprotocol versie 4 (IPv4) in 2012 IPv6 werd geïntroduceerd. Dit protocol breidde het aantal mogelijke IP-adressen uit van zo'n 4 miljard tot 50 quadriljard adressen per persoon ($3{,}4 \times 10^{38}$)[41]. Hierdoor werd het aantal toe te wijzen IP-adressen schier onuitputtelijk en ontstond de mogelijkheid om 'alles met alles' te verbinden. En dat heeft dus ook een aanvang genomen. Zo zijn beveiligingscamera's en de daarbij behorende digitale videorecorders aangesloten op het internet, thermostaten laten via een app op de smartphone de verwarming starten, koelkasten geven door welke artikelen over de houdbaarheidsdatum zijn of aanvulling behoeven, hartpatiënten krijgen monitorapparatuur geïmplanteerd die via internet aan de arts laat weten hoe het ermee staat, e-pleisters analyseren de transpiratie en stellen remedies voor, insulinepompen en pacemakers worden via een app bediend, diagnostische robotjes worden door het lichaam gestuurd waarna de gegevens online worden gedeeld met het ziekenhuis, de vuilcontainer geeft aan de gemeente door dat hij geleegd wil worden en bidons maken de eigenaar er met een notificatie op attent dat het tijd is aandacht te besteden aan de vochtbalans. De voorbeelden worden alleen gelimiteerd door onze beperkte fantasie.
Er zijn diverse schattingen van het aantal apparaten dat in de nabije toekomst verbonden zal zijn met het globale IoT. Het consultancy- en adviesbureau Gartner schat dat dit aantal rond

41 Internet Protocol versie 6 (s.d.). In *Wikipedia*. Geraadpleegd op https://nl.wikipedia.org/wiki/Internet_Protocol_versie_6

2020 op 21 miljard zal liggen.[42] Anderen[43] gaan verder en komen uit op 50 tot 100 miljard apparaten. Hoe het ook zij, duidelijk is in ieder geval dat het IoT de komende jaren een enorme groei te zien zal geven.

Met een toename van 'dingen' die met het internet verbonden zijn, neemt het aantal potentiële doelwitten van cyberaanvallen exponentieel toe. Bovendien kunnen deze 'dingen' ook deel gaan uitmaken van botnets die gebruikt worden voor het plegen van cybercrime. Voor de consumenten is vaak niet duidelijk welk apparaat besmet is met malware. De mate waarin cyberaanvallen zullen gaan plaatsvinden, is afhankelijk van de aandacht voor de technische beveiliging en de mate waarin van deze aanvallen een crimineel verdienmodel kan worden gemaakt. Steeds duidelijker wordt echter dat de 'dingen' die met het internet verbonden zijn, een notoir slechte beveiliging kennen. Ze hebben vaak software die niet geüpdatet wordt en er worden van fabriekswege standaardwachtwoorden gebruikt die vaak niet te wijzigen maar wel eenvoudig te kraken zijn. In oktober 2016 heeft een hackersgroep hiervan gebruikgemaakt door grote aantallen beveiligingscamera's en digitale videorecorders (van een bepaald merk) te hacken en ze in een botnet te plaatsen waarmee een DDoS-aanval gepleegd werd op belangrijke servers aan de oostkust van de Verenigde Staten. Dit resulteerde in een massieve interruptie van populaire internetdiensten zoals Twitter, Amazon, Reddit, Spotify, PayPal, Airbnb, Pinterest en Vox Media. Nu valt te verdedigen dat dit vooral vandalisme is en voor een beperkte tijd wat overlast heeft gegeven bij diensten die niet bepaald tot de cruciale onderdelen van de vitale infrastructuur behoren, maar het maakt wel duidelijk welke (criminele) mogelijkheden het IoT in zich bergt. Zo is het denkbaar – en wat denkbaar is binnen de ICT-wereld gebeurt waarschijnlijk ook – dat op dezelfde manier ransomware verspreid wordt. Dat zal niet alleen financiële consequenties hebben, maar kan ook leiden tot verlies van belangrijke (persoonlijke) gegevens en verstoring van ICT-systemen. Verder bieden de vele apparaten die met internet verbonden zijn, mogelijkheden om via hacking bij de eigenaren van die apparaten mee te kijken en te luisteren naar alles wat zich afspeelt in huis, bedrijfs- of overheidsgebouw. In potentie resulteert dit in een schending van de privacy die haar weerga niet kent.

In het centrum van deze wereldwijde innovatie staan niet zozeer al die apparaten als wel de 'verbonden mens' die al die apparaten gebruikt; er is sprake van een 'Internet of People'. Dit leidt tot dataficatie, een enorme toename van data over menselijk gedrag – al dan niet vrijwillig afgestaan – en registratie, opslag en analyse hiervan door bedrijven en overheden. Er zijn veel toepassingen mogelijk, al dan niet met behulp van bigdata-technieken, voor de analyse van grote hoeveelheden gegevens. Behalve voor deze bedrijven zelf, zijn al deze gegevens om uiteenlopende redenen ook interessant voor 'digitale criminelen'. Ze kunnen bijvoorbeeld gebruikt worden voor identiteitsfraude, ze kunnen gegijzeld worden en alleen

42 Gartner (2015, 10 november). *Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015* (Press release). Geraadpleegd op http://www.gartner.com/newsroom/id/3165317

43 Ch. Adams jr. (2014, 15 december). The Internet of Things and the connected person (Blogpost). Geraadpleegd op http://insights.wired.com/profiles/blogs/the-internet-of-things-iot-and-the-connected-person

tegen betaling vrijgegeven, de data kunnen gevoelige persoonlijke of financiële gegevens en wachtwoorden bevatten die tot afpersing of diefstal kunnen leiden. Hoewel militaire spionage en bedrijfsspionage niet tot het NDB-domein gerekend worden, willen we er wel op wijzen dat het IoT ook op deze terreinen talloze gelegenheden biedt.

Cloudcomputing

Een belangrijke ontwikkeling binnen het internetlandschap is *cloudcomputing*. Er is geen vastomlijnde definitie van cloudcomputing, maar de essentie ervan is dat ICT-infrastructuren, platforms, softwarediensten en data niet langer lokaal (op de eigen pc of server) maar via het internet worden opgeslagen, benaderd en gebruikt. Daarbij is van belang dat het gegevensbeheer of de computerapplicaties aan een dienstverlener worden uitbesteed, en dat gegevens verspreid over verschillende servers worden opgeslagen – meestal zonder dat de gebruiker de regie heeft over de precieze locatie.

Cloudcomputing gaat met diverse veiligheidsrisico's gepaard. Zo kan de cloud zowel doelwit van als middel voor cybercriminaliteit zijn. Als doelwit is de cloud interessant, omdat clouddiensten over een schat aan informatie beschikken. Vooral financiële gegevens en identiteitsgegevens zijn interessant voor criminelen. Zij kunnen ze gebruiken voor afpersing maar ook voor identiteitsfraude. Vooral clouddiensten die vanaf eenzelfde fysieke locatie worden gefaciliteerd, zijn kwetsbaar. Met één enkele aanval kunnen direct veel gebruikers worden getroffen.

De opslag- en rekencapaciteit van de cloud kan verder worden misbruikt in botnets of voor het uitvoeren van grootschalige DDoS-aanvallen. Daarnaast kunnen clouddiensten een krachtig middel voor de verspreiding van malware zijn. Verder kunnen criminelen de cloud gebruiken om anoniem en niet-traceerbaar te communiceren.

De hoeveelheid mogelijkheden die de cloud aan criminelen biedt, hangt samen met het beveiligingsniveau. Na enkele incidenten is de toegangsbeveiliging verbeterd. Veel diensten zijn inmiddels overgegaan op tweefactor-authenticatie, waardoor de cloud relatief veilig is. Een verschuiving van activiteiten naar de cloud zou gunstig kunnen zijn voor bijvoorbeeld het midden- en kleinbedrijf (MKB). Momenteel is het MKB door de hoge kosten van goede beveiliging en de gefragmenteerde ICT-infrastructuur kwetsbaar voor cybercrime. De cloud is beter beveiligd dan de ICT-voorzieningen die nu over het algemeen gebruikt worden.

Crowdfunding

Crowdfunding is een fenomeen dat sterk in opkomst is. Op allerlei terreinen worden crowdfundingacties opgezet: van het bekostigen van een dure operatie tot het financieren van commerciële start-ups, van kleine sympathieke private projecten zoals een kattencafé in Amersfoort tot de deelname van het vrouwensquashteam aan het WK.

De bedragen waarmee deelgenomen kan worden, variëren sterk. Soms wordt de hoogte van het bedrag aan de investeerder overgelaten, soms wordt een minimumbedrag aangehouden, soms gaat het om een donatie zonder dat een tegenprestatie wordt gevraagd en is

crowdfunding een digitale vorm van collecteren. In 2015 werd hiermee in Nederland een totaalbedrag van 125 miljoen euro opgehaald.
De Autoriteit Financiële Markten (AFM) waarschuwt tegen crowdfunding, omdat de risico's vaak veel groter zijn dan bij 'gewone' beleggingen. Crowdfunding wordt immers gebruikt voor het financieren van projecten waar gewone banken geen brood in zien vanwege de te grote risico's. Er worden schuchtere pogingen ondernomen om de markt te reguleren. Zo mag een consument per crowdfundingplatform niet meer investeren dan 80.000 euro en moeten mensen die voor het eerst investeren en meer dan 500 euro willen inleggen een investeringstoets afleggen. In hoeverre dit de risico's beperkt, moeten we nog afwachten.
Uit diverse deelrapporten blijkt dat crowdfunding ook op minder eerzame manieren gebruikt wordt. In het rapport over horizontale fraude is melding gemaakt van misbruik van crowdfunding als vorm van voorschotfraude. Ook kan crowdfunding gebruikt worden voor witwassen: een witwasser kan een crowdfundingactie opstarten waarbij hij de inleggers zelf van de inleg voorziet. Het geld dat hij daarmee binnenhaalt, heeft door die truc een verklaarbare en schijnbaar legale herkomst.
Al staan de signalen in Nederland op dit moment niet op rood, in het buitenland zijn meerdere meldingen van dergelijk misbruik gedaan. Wanneer de groei echter doorzet – en het heeft er alle schijn van dat dit zal gebeuren – wordt crowdfunding ook voor Nederlandse criminelen een aantrekkelijke mogelijkheid voor frauduleus gebruik.

Blockchain, bitcoin en payment service provider

Hoewel zich de afgelopen jaren al grote veranderingen hebben voltrokken, staat de financiele dienstverlening aan de vooravond van wellicht nog grotere veranderingen. Enkele exponenten van die veranderingen zijn de *blockchaintechnologie*, met als bekendste manifestatie de bitcoin, en nieuwe manieren van betalen, waaronder de *payment service provider* (PSP).

De blockchaintechnologie is de technologie achter de bitcoin en andere cryptocurrency's. Tot voor kort was dit een wat duister fenomeen, dat vooral bekendheid kreeg door de aanvankelijk sterk stijgende koers van de bitcoin, de snel daarop volgende koersval en het gebruik van de bitcoin voor dubieuze zaken zoals het betalen van de losprijs bij gijzeling van computers. Recent heeft een internationaal consortium van veertig banken de blockchaintechnologie echter omarmd, omdat deze voor meerdere doeleinden inzetbaar is. Kort gezegd is een blockchain een openbaar, online register van transacties. Via de blockchain van de bitcoin kan nagegaan worden wie de eigenaar is en of de bitcoin niet twee keer wordt uitgegeven. De toepassingen zijn legio. Zo is voorstelbaar dat deze techniek ook bij de huizenverkoop, aandelentransacties, het opmaken van aktes en autoverhuur zal worden gebruikt.
Er valt veel meer over te zeggen, maar de essentie van de blockchaintechnologie is dat er geen tussenpersoon meer nodig is bij transacties. Doordat het register openbaar is en wereldwijd gedistribueerd wordt, kunnen partijen rechtstreeks met elkaar zakendoen.

Hierdoor worden notarissen, financieel dienstverleners, makelaars en andere intermediairs in beginsel overbodig. Het verdienmodel van banken zou bij algemene toepassing van de blockchaintechnologie een grondige herziening behoeven. Dit verklaart ook de interesse van de banken. Hoewel er veel vragen bestaan over de veiligheid van de blockchains, de softwareontwikkeling en de bereidheid van partijen om de vertrouwde omgangsvormen bij transacties los te laten, zien veel betrokkenen hierin de volgende digitale revolutie.
Ongetwijfeld vinden innovatieve criminele samenwerkingsverbanden of individuele *whizzkids* een manier om misbruik te maken van de mogelijkheden die de blockchaintechnologie biedt. De kernvraag is in hoeverre dit fenomeen in de komende vier jaar al zijn stempel zal drukken op het betalingsverkeer. De deskundigen zijn het daarover niet eens. Er zijn weliswaar voorbeelden te geven van technologische ontwikkelingen die veel sneller gingen dan aanvankelijk gedacht (bijvoorbeeld de toepassingen van internet, smartphones, sociale media en tablets), maar de blockchaintechnologie verkeert nog in een pril stadium. Dat maakt het lastig verwachtingen uit te spreken. Op dit moment zijn de cryptocurrency's bijvoorbeeld nog geen wettig betaalmiddel, terwijl dat wel een voorwaarde is om breed ingang te vinden bij alledaagse betalingen. Hoe het ook zij, het lijkt een buitengewoon relevant fenomeen dat het volgen waard is. Alleen zo kunnen we tijdig het hoofd bieden aan eventuele criminele toepassingen.

Recent is in opsporingsonderzoeken naar witwassen de *payment service provider* (PSP) opgevallen. Een PSP is een online betaaldienst die de betalingen aan winkeliers afhandelt. Het voert hier te ver om alle technische varianten ervan te behandelen. Relevant is dat uit opsporingsonderzoeken is gebleken dat het gebruik van een PSP de crimineel kan helpen bij het verhullen van de herkomst van zijn omzet. Dat komt doordat een PSP vaak verschillende transacties opspaart om deze in één keer bij de bank aan te leveren. Doordat de transacties dan niet meer op consumentenniveau uitgesplitst zijn, kan de bank niet controleren wie de transacties hebben verricht en of de regels zijn nageleefd (*compliance*). De compliance ligt daarom bij de PSP, maar deze is vaak in het buitenland gevestigd en ziet te weinig details. Een nieuwe ontwikkeling op dit gebied is dat verdachten zelf de beschikking over een PSP hebben en dus de compliance volledig in eigen beheer hebben. Daarmee ontstaat voor criminelen een goede mogelijkheid hun cliënten of omzet te verhullen. De drempel om een PSP te beginnen is relatief laag. Iemand met enige technologische *knowhow* kan er al een opstarten en anders kan hij de expertise wel inhuren. De rol van PSP's zal in de nabije toekomst belangrijker worden. Het is een vorm van uitbesteding die tot grote besparingen leidt.

1.4 De criminele praktijk

In deel 2 zijn, per afzonderlijk thema, uiteenlopende aspecten van de criminele praktijk besproken. Hier worden enkele meer algemene ontwikkelingen belicht waarvoor geldt dat de relevantie niet beperkt blijft tot de criminele praktijk binnen een enkel thema, maar bredere toepassing kent binnen het terrein van de georganiseerde criminaliteit.

Allereerst zijn dat drie ontwikkelingen die iets zeggen over de mate waarin criminelen hun omgeving inschakelen bij hun criminele activiteiten: *Do-it-Yourself, Crime-as-a-Service* (CaaS) en criminele uitbesteding. Do-it-Yourself kenmerkt zich door zelfstandigheid. Zo gebruikt men bestaande technieken en informatie om zelf producten te vervaardigen. Dat zijn in dit verband producten die kunnen worden misbruikt of die van zichzelf al illegaal zijn. Bij CaaS worden instrumenten gebruikt die anderen hebben ontwikkeld en aangeboden om criminaliteit te faciliteren. En in het geval van criminele uitbesteding worden anderen ingehuurd om een deel van de criminele activiteiten uit te voeren. We besteden bij de bespreking hiervan ook aandacht aan de vraag of ontwikkelingen in de afgelopen jaren iets zeggen over de mate waarin criminele samenwerkingsverbanden (csv's) op een professionele manier werken (al dan niet professionalisering[44]).
Ten slotte bespreken we de criminele veelzijdigheid van daders. Worden criminelen veelzijdiger dan ze voorheen waren?

Do-it-Yourself

Do-it-Yourself (DIY) is een maatschappelijke ontwikkeling die al enige tijd gaande is. Het is een ontwikkeling waarbij individuen hun wensen trachten te realiseren door daaraan, zo veel als mogelijk, zelf invulling te geven, zonder de hulp van experts of professionals. Manifestaties van DIY zijn bijvoorbeeld bands en artiesten die hun muziek uitbrengen op platenlabels die zij zelf financieren of door hun fans laten financieren via crowdfunding, reizigers die hun accommodatie zelf online regelen via Airbnb, en wijkbewoners die elkaar informeren over duurzame energie en gezamenlijk zonnepanelen inkopen en installeren.
Technologie wordt steeds compacter en goedkoper, informatie wordt overal en voor iedereen toegankelijk. De bredere beschikbaarheid van veel technieken en informatie zal steeds meer mogelijkheden creëren voor individuen. DIY zal daarom de komende jaren alleen maar toenemen. En dit sluit aan bij de groeiende behoefte van consumenten aan producten op maat en de wens om minder afhankelijk te zijn van anderen om in de eigen behoefte te voorzien.
Naar verwachting zullen binnen DIY ook steeds meer criminele toepassingen te zien zijn. Zelfvervaardigde producten kunnen illegaal zijn of misbruikt worden. Zo circuleren er handleidingen en filmpjes op internet met behulp waarvan explosieven gemaakt kunnen worden en maken biotechnologische ontwikkelingen het binnenkort mogelijk opiaten te kweken op een manier die vergelijkbaar is met het bierbrouwproces. Met het oog op een toekomstig tekort aan pijnstillers startten synthetisch biologen in 2004 met het maken van morfineproducerende gist. Daarvoor zijn meerdere stappen nodig. Binnenkort kunnen met één soort gist alle zeventien reacties naar morfine in één keer efficiënt worden uitgevoerd met suiker als grondstof. Passend in de DIY-trend zou eenieder daarmee in principe in de eigen kelder opiaten kunnen kweken.

44 Een professionele manier van werken betekent hier het vakkundig, effectief en efficiënt organiseren van de criminele bedrijvigheid. Professionalisering houdt in dat een professionele manier van werken vaker voorkomt dan voorheen.

Een andere recente manifestatie van DIY op het terrein van drugs is de particuliere drugsproducent. Deze werkt geheel zelfstandig, zonder link met georganiseerde misdaad. Hij beschikt wel over kennis van IT, die hij aanwendt om via internet grondstoffen en hardware aan te schaffen en de synthetische drugs, na productie in eigen beheer, aan te bieden.

Een technologische ontwikkeling die naadloos in deze trend past, is het driedimensionaal printen (3D-printen). Met een 3D-printer kunnen aan de hand van digitale instructies in een CAD-bestand (*Computer Aided Drawing*) exacte driedimensionale kopieën gemaakt worden. De kosten van 3D-printers gaan in sneltempo omlaag (in enkele jaren van 50.000 euro naar 1000 euro in de loop van 2016) waardoor de technologie snel bredere toepassing zal krijgen. In de toekomst zal de vervanging van onderdelen van apparaten door middel van een CAD-bestand plaatsvinden. De producent stuurt het bestand per mail naar de aanvrager en die print het benodigde onderdeel zelf uit; nooit meer naar Ikea voor een kapot onderdeeltje. Distributie van ontwerpen gebeurt via internet, alleen de grondstoffen worden nog fysiek vervoerd. Er zullen websites komen die CAD-bestanden van talloze producten verkopen. Dit botst met het intellectueeleigendomsrecht.
Artikelen die tot dusver gebrekkig werden nagemaakt, zullen in de nabije toekomst worden geperfectioneerd met behulp van *ultrahigh resolution* 3D-scanning en -printing, zodat het resultaat niet meer van echt te onderscheiden is. Door middel van CAD-bestanden en 3D-printing kunnen belastingen en importheffingen worden ontdoken. Vindingrijke criminelen zullen steeds meer toepassingen van de 3D-printer ontdekken waarmee zij hun activiteiten kunnen faciliteren. Bij het plegen van ladingdiefstallen is al gebruikgemaakt van veiligheidsverzegelingen die met een 3D-printer vervaardigd zijn.

De Do-it-Yourselftrend en de voortschrijdende digitalisering hebben consequenties voor de criminele samenwerking. Personen zijn zelfstandig tot veel meer in staat dan voorheen. Het zwaartepunt in daderschap verschuift daardoor van groepen naar individuen. Voor zover individuen anderen nog nodig hebben, vinden de contacten niet meer *face to face* plaats, maar via internet. Het contact is niet meer plaatsgebonden; de criminele samenwerking internationaliseert. Dit alles heeft consequenties voor de opsporing. De verschuiving van het werkterrein van de opsporing naar het digitale domein vereist andere expertise dan de traditionele opsporingskennis en -vaardigheden. Verder zullen daders steeds vaker vanuit of via het buitenland opereren. Daardoor wordt de opsporing in Nederland steeds meer afhankelijk van toestemming en medewerking van buitenlandse instanties.

Een ontwikkeling die in belangrijke mate bijdraagt aan de mogelijkheden voor individuen om zelfstandig criminele activiteiten te ontplooien, is Crime-as-a-Service. Hieraan besteden we aandacht in het volgende tekstblok.

Crime-as-a-Service

In de ondergrondse economie is een vorm van dienstverlening ontstaan die wordt aangeduid als Crime-as-a-Service (CaaS): het aanbieden van kant-en-klare, eenvoudig te gebruiken softwarepakketten waarin de functionaliteiten om diverse vormen van cybercrime te plegen zijn voorgeprogrammeerd. CaaS maakt het mogelijk om bijvoorbeeld DDoS-aanvallen uit te voeren, ransomware te verspreiden en *Remote Access Tools* (RAT's) te gebruiken zonder te beschikken over bijzondere digitale vaardigheden. Het vereiste softwarepakket om bijvoorbeeld een DDoS-aanval uit te voeren is relatief gemakkelijk toegankelijk via marktplaatsen op het darkweb. De drempel om cybercrime te plegen wordt hierdoor verlaagd, wat het aantal potentiële aanvallers vergroot. Door CaaS zijn het niet alleen beroepscriminelen en statelijke actoren die cybercrime plegen, maar ook individuen zonder bijzondere technische kennis. Het risico bestaat dat jongeren via games of anderszins in aanraking komen met tools voor cyberaanvallen. Voor sommige van deze jongeren kan dit de start betekenen van een geheel andere dan een gamecarrière.

De dienstverlening wordt professioneler. Niet alleen wordt cybercrime gefaciliteerd door het aanbieden van software en tools, er komen ook steeds meer handleidingen en zelfs helpdesks voor de toepassing ervan en voor het regelen van de uitgaande kasstromen. Er zijn kant-en-klare moneymule-netwerken te koop. Zoals eerder in dit NDB werd beschreven, stellen moneymules hun bankrekening ter beschikking om daarop inkomsten te ontvangen die uit criminele activiteiten afkomstig zijn. Vaak betreft het individuele overeenkomsten tussen dader en moneymule of katvanger. In het geval van omvangrijker cybercriminaliteit is het belangrijk dat de inkomsten gespreid worden over buitenlandse moneymules, zodat de herkomst moeilijk te achterhalen is en het risico gespreid wordt.

Het Nationaal Cyber Security Centrum geeft aan dat het aantal dienstverleners toeneemt en de aangeboden diensten talrijk zijn geworden. De concurrentie die hierdoor ontstaat, zorgt ervoor dat de dienstverleners steeds betrouwbaarder en goedkoper worden en een steeds completer 'dienstenpakket' aanbieden.

Criminele uitbesteding en professionalisering

Voor veel criminele samenwerkingsverbanden is het moeilijk om alle essentiële deeltaken van een crimineel bedrijfsproces (zoals productie, transport, afzet, communicatie, afscherming, witwassen) te realiseren met uitsluitend inzet van eigen mensen en middelen. Het kan een csv bij het uitvoeren van deeltaken ontbreken aan benodigde kennis en vaardigheden, vereiste papieren, ruimtelijke voorzieningen, menskracht, materieel en materiaal.[45] Voor sommige deeltaken is het dan, vanwege een gemis of tekort, noodgedwongen aangewezen op uitbesteding. Ook overwegingen van risicobeperking kunnen een csv ertoe doen besluiten bepaalde onderdelen van het criminele bedrijfsproces uit te besteden.[46] Door het inschakelen van anderen die bijvoorbeeld risicovolle smokkeltrajecten voor hun rekening nemen, kunnen csv's zelf buiten schot proberen te blijven.

45 H. Moerland & F. Boerman (1999). *Georganiseerde misdaad en betrokkenheid van bedrijven* (Politiestudies nr. 25). Deventer: Gouda Quint.

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

In de deelstudies die voor dit dreigingsbeeld zijn verricht, treffen we diverse voorbeelden aan van het inhuren van anderen voor het uitvoeren van onderdelen van de criminele bedrijvigheid. De belangrijkste voorbeelden van dergelijke criminele uitbesteding zijn de volgende:

- het verwerven van panden door makelaars, verhuurbemiddelaars en notarissen ten
- behoeve van hennepteelt;
- het inrichten van locaties voor hennepteelt door hokkenbouwers en elektriciens;
- het bouwen van koelers, destillatieapparatuur, drukvaten, reactievaten, kristallisatie-, filtratie- en mengapparatuur door hardware-bouwers ten behoeve van het vervaardigen van synthetische drugs;
- het dumpen van afvalstoffen van synthetischedrugsproductie door specialistische dumpers;
- het uithalen van verdovende middelen in de havens;
- het bieden van serverruimte door malafide *subcontractors* van hostingproviders ten behoeve van criminele activiteiten;
- het beschikbaar stellen van kennis van de beveiliging van nieuwe typen auto's;
- het aanbieden van apparatuur en software voor het manipuleren van beveiligingssystemen van voertuigen;
- het op bestelling leveren van gestolen auto's die zijn geprepareerd voor het uitvoeren van een ramkraak;
- het leveren van valse documenten door criminele specialisten die gebruikmaken van geavanceerde technieken;
- het verzenden van wapens en munitie door tussenkomst van een *parcel forwarding service*;
- het herstellen van onklaar gemaakte vuurwapens door technische experts;
- het wegsluizen en witwassen van criminele opbrengsten door gespecialiseerde csv's;
- het gebruikmaken van de diensten van payment service providers voor witwassen;
- het plannen en uitvoeren van criminele afrekeningen;
- het op bestelling leveren van automatische vuurwapens en vluchtauto's.

Bij criminele uitbesteding schakelen criminelen anderen in vanwege hun criminele specialisme. Deze werkwijze draagt doorgaans bij aan een betere organisatie van de criminele bedrijvigheid en getuigt daarmee van een zekere mate van professionaliteit. De hennepteelt en de synthetischedrugscriminaliteit in ons land kunnen wat dit betreft als professioneel worden beschouwd: zowat elk facet van de criminele bedrijvigheid wordt uitgevoerd door specialisten die meestal zelfstandig hun bijdrage leveren aan het geheel. Dit bemoeilijkt de aanpak van de organisatoren achter de schermen. Een specifieke aanpak gericht op het uit de markt halen van personen met een bepaald specialisme (bijvoorbeeld elektriciens) kan bewerkstelligen dat de criminele bedrijfsketen voor een bepaalde tijd wordt verstoord. In hoeverre dit resulteert in langdurige verstoring hangt af van de flexibiliteit van de criminele gemeenschap.

Hoewel uitbesteding in de hennepteelt en de synthetische drugs zeker niet iets van de laatste jaren is, bestaat wel de indruk dat het is toegenomen. Uit casuïstiek komt in elk geval het

beeld naar voren dat de uitbesteding ten behoeve van de hennepteelt zich wijder heeft verbreid; de branche is verder geprofessionaliseerd.
De uitbesteding van conflictbeslechting is hoofdzakelijk gelieerd aan de drugshandel. Dat opdrachtgevers specialisten inschakelen, is een teken van professionaliteit. Dit neemt niet weg dat het die 'specialisten' bij de uitvoering aan professionaliteit kan ontbreken, gezien de dodelijke persoonsverwisselingen die zich hebben voorgedaan.

Autofabrikanten laten hightech beveiligingssystemen ontwikkelen als preventieve maatregel tegen autodiefstal. In reactie hierop is een crimineel specialisme ontstaan: het analyseren en ontleden van de beveiliging van nieuwe typen auto's. Bestrijding en technologische vooruitgang aan de ene kant leiden tot de noodzaak tot aanpassingen aan de andere kant. Om succesvol te blijven moeten csv's innoveren. De georganiseerde autodiefstal kent niet alleen een complexe logistieke keten, een hoge organisatiegraad en criminele uitbesteding, maar de professionaliteit van deze csv's blijkt ook uit hun vermogen om op onderdelen de werkwijze aan te passen en te vernieuwen.

De mogelijkheden voor beveiliging die de technologie biedt, nopen niet alleen de georganiseerde illegale autobranche tot professionalisering. Ook bij het vervaardigen van valse documenten en vals geld moeten criminelen over steeds meer expertise en steeds geavanceerdere technieken beschikken om succesvol te zijn.
Een bijzonder geval vormt in dit verband de drugssmokkel via de Rotterdamse haven. Steeds meer van de bedrijvigheid in de haven, waaronder de doorgang van containers, gebeurt geautomatiseerd. Door de verregaande automatisering en robotisering is manipulatie van het computersysteem de enige manier waarop criminelen erachter kunnen komen waar een container zich bevindt. Door manipulaties kunnen ze niet alleen zien waar containers staan, ze kunnen deze ook laten verplaatsen, ze 'op groen' zetten zodat de douane ze niet controleert, of pincodes achterhalen die noodzakelijk zijn voor het ophalen van een container. Dat betekent dat criminelen toegang moeten krijgen tot deze systemen, hetzij door hacken (zelf of door het inhuren van hackers) hetzij door het omkopen van kantoorpersoneel of opsporingsambtenaren.
In eerdere dreigingsbeelden is al beargumenteerd dat met de toenemende automatisering en robotisering de mens hoe langer hoe meer de zwakste schakel wordt. Die constatering is juist gebleken en lijkt alleen maar meer van toepassing geworden, gelet op de gevallen van corruptie die de laatste tijd aan het licht zijn gekomen. Door de voortschrijdende automatisering van het havenbedrijf zal het aantal corruptiegevallen vermoedelijk verder groeien. Ook de toename van smokkel in de gemanifesteerde lading draagt hieraan bij, omdat deze methode niet zonder betrokkenheid van de zendende en ontvangende partij kan worden uitgevoerd. De druk op werknemers in de logistieke sector en bij toezichthoudende en controlerende instanties zal naar verwachting alleen maar groter worden.
Het gebruik van corruptie binnen de georganiseerde criminaliteit is in vorige dreigingsbeelden in den brede aan de orde gesteld. In dit dreigingsbeeld is een afzonderlijk onderzoek naar deze criminele werkwijze achterwege gelaten.

Voor meer inzicht in dit fenomeen verwijzen we naar het onderzoek naar corruptie dat aan de Universiteit Maastricht wordt uitgevoerd. Hier beperken we ons tot de signalering dat corruptie bij drugshandel (cocaïne, heroïne, hennep) nog immer een belangrijke rol speelt, en dat er in toenemende mate gebruik wordt gemaakt van corruptie bij drugssmokkel met containervervoer via de havens van Rotterdam en Antwerpen.

Op nog twee terreinen zien we professionalisering: mensensmokkel en cybercrime. Een restrictiever migratiebeleid (bijvoorbeeld ten aanzien van gezinshereniging) en striktere handhaving aan de grenzen van de Europese Unie en in Nederland maken migratie lastiger. Irreguliere migranten raken daardoor (nog) meer afhankelijk van mensensmokkelaars. De smokkelaars moeten professioneler te werk gaan om succesvol te kunnen zijn. Zij moeten immers hogere barrières in de vorm van grenscontroles aan de binnen- en buitengrenzen zien te nemen.
De dienstverlening gericht op het faciliteren van cybercrime (CaaS) is professioneler geworden. Dit blijkt uit de eerder besproken toename en verbreding van het aanbod en de grotere concurrentie onder aanbieders.

Ter afsluiting van dit tekstgedeelte een opmerking over witwassen. Door de vele witwasconstructies die worden gebruikt om de herkomst van crimineel geld te versluieren is het niet eenvoudig om wederrechtelijk verkregen voordeel te ontnemen. Uitbesteding van witwassen compliceert de aanpak van witwassen nog verder. Dat geldt eens te meer als er via die uitbesteding buitenlandse banken betrokken zijn. Sommige van dergelijke instituties zijn voor Nederlandse opsporingsinstanties namelijk moeilijk benaderbaar. Ook in dit verband draagt internationalisering bij aan de uitdaging waarvoor de opsporing zich gesteld ziet. De uitbesteding aan facilitatoren met een geheimhoudingsplicht, zoals advocaten en notarissen, compliceert de aanpak van witwassen eveneens. Dergelijke facilitatoren kunnen door criminelen onder druk worden gezet (corruptie, afpersing) om hun diensten in te zetten voor witwassen. De aanpak van deze facilitatoren wordt bemoeilijkt doordat hun diensten in beginsel onder de wettelijke geheimhoudingsplicht vallen.

Criminele veelzijdigheid

Het algemene beeld dat criminele samenwerkingsverbanden zich bezighouden met een breed scala aan criminele activiteiten, wordt in de deelstudies die ten grondslag liggen aan dit Nationaal dreigingsbeeld meer dan eens bevestigd. De traditionele indeling van csv's naar criminele hoofdactiviteiten lijkt achterhaald. Voorheen waren de csv's vaak samengesteld langs etnische lijnen. Was de etnische achtergrond of de nationaliteit van een csv bekend, dan gold dit vaak tegelijkertijd voor zijn criminele bezigheden. Wat dit betreft, lijken zich veranderingen te hebben voltrokken.

Zo zijn Turkse csv's veelzijdiger geworden: ze zijn niet meer uitsluitend actief in de heroïnehandel. In Brabant houden criminele Turkse familienetwerken zich bezig met hennep, cocaine, synthetische drugs, arbeidsuitbuiting, illegaal gokken en witwassen. Er vindt 'branche-

vervaging' plaats. De voorheen redelijk gescheiden markten zijn vermengd geraakt. Een reden voor de grotere veelzijdigheid zien sommigen in de opkomende markten in Turkije: het gebruik van cocaïne en ecstasy is daar toegenomen en de traditionele Turkse netwerken voorzien in de vraag.
Daarnaast zien we al langere tijd dat de heroïnemarkt in Nederland krimpt en inmiddels bescheiden van omvang is. In Europa is er nog een aanzienlijke markt, maar het aantal gebruikers daalt langzaam. De perspectieven om geld te verdienen met heroïnehandel nemen dus af. Het is goed mogelijk dat de Turkse netwerken gekozen hebben voor diversificatie als bedrijfsstrategie om de teruglopende inkomsten uit de heroïnehandel te compenseren. De genoemde factoren (groeiende vraagmarkt in Turkije en krimpende markt in Nederland) kunnen in combinatie verantwoordelijk zijn voor de geconstateerde diversificatie.

Diversificatie vinden we niet uitsluitend bij de Turkse csv's, het is een bredere trend in het Nederlandse criminele landschap. Uit opsporingsdossiers blijkt dat fraudeurs niet alleen allerlei soorten fraude plegen, maar zich bezighouden met veel verschillende vormen van criminaliteit: het een wordt gepleegd (fraude) om het andere (drugs) te bekostigen, waarna de criminele opbrengsten worden witgewassen (in vastgoed) en de organisatie kan groeien. Ook binnen de georganiseerde vermogenscriminaliteit zien we de specialisaties vervagen. Vaak worden verschillende vermogensdelicten gecombineerd, maar ook andere combinaties zijn mogelijk, zij het dat we die in mindere mate aantreffen. Internationaal opererende dadergroepen maken zich bijvoorbeeld schuldig aan diefstal, overvallen, straatroof, voertuigcriminaliteit, drugshandel, oplichting, mensenhandel en openlijke geweldpleging. Hoe professioneler de dader, des te eerder hij zich met midden- en zware criminaliteit gaat bezighouden. Europol ziet in de veelzijdigheid van deze dadergroepen een belangrijke verklaring voor hun 'succes'.
Vuurwapenhandel is van oudsher een branche die op zichzelf niet buitengewoon winstgevend is, maar 'meelift' met andere vormen van grensoverschrijdende criminaliteit. Dat werd ook al geconstateerd in het NDB2012. Vrijwel alle verdachten van vuurwapensmokkel houden zich ook met andere vormen van criminaliteit bezig, zoals de handel in verdovende middelen en het plegen van liquidaties. Het beeld van de criminele veelzijdigheid van vuurwapenhandelaars dat al jaren bestaat, blijft intact.
Illegale teelt van en handel in hennep levert veel geld op. Dat wordt aangewend om andere criminele activiteiten te financieren. Voorbeelden daarvan zijn de aankoop van grondstoffen voor synthetische drugs en de inkoop van een partij cocaïne. Geconstateerd wordt dat de hennepteelt en -handel eenvoudig toegankelijk is en voorkomt bij veel criminele samenwerkingsverbanden, ook wanneer deze zich primair met een andere vorm van criminaliteit bezighouden. Inherent aan de georganiseerde hennepteelt en -handel zijn de criminele activiteiten met betrekking tot witwassen en fraude. De illegale winsten worden witgewassen via diverse constructies. Fraude wordt dikwijls gepleegd om bepaalde aspecten van de hennepteelt te faciliteren. Voorbeelden daarvan zijn hypotheekfraude, faillissementsfraude en fraude met betrekking tot identiteitsdocumenten en werkgeversverklaringen voor het verwerven van panden.

Zo zijn er legio voorbeelden te geven van de diversificatie in de criminele bedrijfsvoering.

Het belang van deze signalering betreft niet alleen een verandering in het algemene beeld van de georganiseerde criminaliteit, maar ook en misschien wel vooral de consequenties ervan voor de aanpak van criminele netwerken en samenwerkingsverbanden en de daarvoor benodigde expertise.

1.5 Georganiseerde criminaliteit in de wijken: onaantastbaarheid en normvervaging

In 2014 verscheen een rapport van Tops en Van der Torre waarin verslag wordt gedaan van een onderzoek naar de resultaten van de zogenoemde wijkenaanpak.[47] Een belangrijk thema in het rapport is de manier waarop georganiseerde of ondermijnende criminaliteit zich manifesteert in woonwijken en welke gevolgen dat heeft. Dit rapport heeft raakvlakken met het NDB, en wel zodanige raakvlakken dat in de deelprojecten die ten behoeve van het NDB zijn uitgevoerd, speciale aandacht besteed is aan de vraag welke gevolgen 'de' georganiseerde criminaliteit heeft op wijkniveau. Deze gevolgen hebben meegewogen bij de kwalificatie van dreiging van de criminele verschijnselen die in deel 2 van dit NDB zijn behandeld. Ze staan daar verspreid over de tekst, waardoor het belang ervan gemakkelijk aan de aandacht kan ontsnappen. Onder de noemer 'georganiseerde criminaliteit in de wijken' brengen we daarom in deze paragraaf een aantal van die gevolgen bij elkaar.

Tops en Van der Torre concluderen onder andere dat in kwetsbare wijken een cumulatie van problemen bestaat die een voedingsbodem voor criminele activiteiten vormt. Voor een deel bestaan die criminele activiteiten uit 'zichtbare' aangiftecriminaliteit, voor een ander deel uit minder zichtbare deelname aan georganiseerde vormen van criminaliteit zoals hennepteelt, fraude, productie van synthetische drugs, arbeidsuitbuiting en witwassen. Tops en Van der Torre zeggen daarover onder meer: "Er zijn aanwijzingen dat in een dergelijke context een symbiotische verhouding tot vormen van (georganiseerde) criminaliteit kan ontstaan (...). Activiteiten van criminelen (niet zelden ook van criminele families), worden dan met de mantel der liefde bedekt. Vanwege verschillende redenen hebben criminelen een positief imago. Zij weten de autoriteiten uit te dagen. Als ze aan jouw kant staan springen ze bij, wanneer je het nodig hebt. Soms is er ook sprake van intimidatie. Meestal is er sprake van een mix van deze factoren" (p. 8). De georganiseerde criminaliteit biedt een "alternatieve kansenstructuur"; waarom zou je je inzetten voor een lang niet zekere respectabele en productieve carrière, wanneer je buurjongen met betrekkelijk geringe inspanningen over een mooie auto en dito vriendin beschikt? Maar het gaat niet alleen om min of meer actieve deelname aan criminele activiteiten. Het gaat ook om iets wat kan worden aangeduid als 'normvervaging' bij bewoners die niet actief aan criminaliteit deelnemen, maar er in het grijze gebied tussen legaal en illegaal van profiteren en in voorkomende gevallen 'de andere kant op kijken'. Deze conclusie wordt goeddeels bevestigd door observaties in verschillen-

47 P.W. Tops & E. van der Torre (2014). *Wijkenaanpak en ondermijnende criminaliteit.* S.l.: s.n.

de NDB-deelrapportages, zoals die over hennep, afpersing, georganiseerde vermogenscriminaliteit, cocaïne, heroïne en arbeidsuitbuiting. Een greep daaruit bespreken we hier.

De ondermijning van de leefbaarheid in toch al kwetsbare wijken is een zorgpunt. Hennepkwekerijen komen overal voor, zowel in 'goede' als in 'zwakke' wijken. Vooral de kwetsbare en zwakke wijken blijken echter vruchtbare voedingsbodems voor criminele netwerken. Hierdoor ontstaat een samenleving waarin criminaliteit en crimineel geld als 'normaal' worden beschouwd. Mensen zien dat er veel geld wordt verdiend, zonder dat daar belasting over wordt betaald. De morele acceptatie in combinatie met hoge opbrengsten, een lage pakkans en milde straffen maakt dat het toetreden tot de hennepindustrie voor veel mensen aantrekkelijk is.
Een negatief aspect van drugshandel is de (vermeende) onaantastbaarheid van personen die zich daarmee bezighouden. Bij drugshandel is de pakkans relatief gering, terwijl de winsten enorm zijn. De rijkdom en status die met de handel bereikt zijn, vertalen zich vaak in patsergedrag: het bezit van grote hoeveelheden contant geld en de aanschaf van dure sieraden of kleding. Omdat jongeren voldoende bewijs zien dat deze route loont, heeft de drugshandel een aanzuigende werking op hen.
In verschillende sectoren, zoals de haven- en de transportsector, is soms sprake van normvervaging. In deze sectoren heerst (van oudsher) een cultuur die zich kenmerkt door een sterke onderlinge verbondenheid en geslotenheid ten opzichte van de buitenwereld. Mensen of bedrijven kennen elkaar en zijn sterk op elkaar gericht. Een ongeschreven regel is dat er geen informatie wordt gedeeld met buitenstaanders, en er lijkt een taboe te liggen op 'uit de school klappen' en op het melden van misstanden. Hier lijken ook andere normen en waarden te heersen ten aanzien van criminaliteit. Dit schept gelegenheid voor het plegen en afschermen van criminele activiteiten.
Bij een opkoper, bij een autohandelaar of op lokale markten lijken veel afnemers goedkope goederen met een bedenkelijke herkomst inmiddels te appreciëren. Dat blijkt bijvoorbeeld uit de casus van een markthandelaar die daarop inspeelt bij het aanprijzen van zijn waar. Hij ontdoet de goederen in zijn kraam juist niet van diefstalkenmerken: de sticker met prijs en winkelketen. Daardoor verkopen ze beter. Er blijkt immers uit dat het om echte (merk)artikelen gaat. Van enige scrupules of angst om bij het kopen of verkopen van een gestolen goed – een misdrijf – betrapt te worden, lijkt geen sprake. Blijkbaar is het voor zowel verkopers als kopers heel gewoon dat er gestolen waar wordt verkocht. Markten en opkoopbedrijven waar deze praktijken veelvuldig plaatsvinden, zijn aan te merken als locaties die aanleiding geven tot normvervaging. Dat leidt tot meer heling en tot een toename van de criminele activiteiten die daaraan voorafgaan.

Normvervaging die het gevolg is van de criminele activiteiten van malafide autohandelaars hangt vooral samen met het feit dat veel van deze ondernemers al decennialang in dezelfde wijken redelijk ongemoeid kunnen opereren. Veel consumenten en bedrijven zijn al jaren klant en kennen de schimmige praktijken. Er is in de loop der jaren een groot vertrouwd netwerk van afnemers ontstaan bij wie de periode van kritisch vragen stellen over de

herkomst van aangeboden waar allang verstreken is. Een aantal malafide autohandelaars hebben in de voorbije jaren een gezaghebbende positie in de lokale gemeenschap opgebouwd en spreiden dat ook ten toon. Zij vertonen binnen die lokale gemeenschap openlijk patsergedrag, bijvoorbeeld door in dure auto's rond te rijden. De gemeenschap rondom dit soort criminelen is buitengewoon gesloten. Er is een groep burgers die niet durft te getuigen uit angst voor represailles. Anderen trekken profijt van de opbrengsten van deze criminelen omdat zij klant zijn. In een paar gevallen profiteert ook de gemeenschap als geheel van de opbrengsten van deze csv's. In twee opsporingsonderzoeken bleken twee csv's ieder een lokale voetbalclub te sponsoren. Beide voetbalclubs hadden een vermoeden omtrent de herkomst van de sponsorgelden maar stelden geen vragen.
In een aantal steden of regio's zijn er groepen die zich onaantastbaar gedragen of hebben gedragen. Deze groepen hebben zich daarbij ook schuldig gemaakt aan afpersing. Afpersing is vaak een onderdeel van een breder criminaliteitsprobleem, waar andere vormen van georganiseerde en ernstige criminaliteit, zoals financieel-economische fraude, een rol kunnen spelen. Het ultieme risico bestaat dat er illegale economieën en zogenoemde (etnische) monoculturen ontstaan waar de politie en andere opsporingsdiensten nauwelijks een informatiepositie (meer) hebben.

De aanwezigheid van georganiseerde criminaliteit in kwetsbare wijken heeft een heel scala aan (in)directe gevolgen, variërend van gelaten acceptatie tot openlijk strafbaar gedrag. Vooral het patsergedrag, de dure auto en de gepercipieerde onaantastbaarheid komen in verschillende deelrapportages naar voren. Alle manifestaties bij elkaar resulteren in een subcultuur binnen de betreffende wijken waarin georganiseerde criminaliteit een geaccepteerd fenomeen is. Er is sprake van een verschuiving van normen. In deze wijken wordt tegen de meest succesvolle criminelen opgekeken en is de grens tussen 'goed' en 'kwaad' niet duidelijk waarneembaar. Hierdoor kunnen bewoners ook tegen hun wil betrokken raken bij strafbare praktijken.
Juist de veelheid aan symptomen met hun eigen dynamiek maakt duidelijk dat de exclusieve aanpak ervan door politie en Openbaar Ministerie niet tot de gewenste resultaten zal leiden. Dat wordt hier niet voor de eerste keer gesignaleerd. Daarom is in veel gemeenten gekozen voor een integrale aanpak waarbij politie, Openbaar Ministerie, openbaar bestuur, bedrijfsleven, Belastingdienst en welzijnswerk gezamenlijk onderzoek doen en actie ondernemen. Deze samenwerking krijgt onder meer gestalte in de Regionale Informatie en Expertise Centra (RIEC's). Over heel Nederland zijn er daarvan tien actief. De RIEC's brengen op gezette tijden bestuurlijke criminaliteitsbeeldanalyses uit, waarin zij verslag doen van de belangrijkste problematiek in de regio waarin zij actief zijn, en suggesties doen voor de aanpak ervan.