Criminele geldstromen en ICT: over innovatieve werkwijzen, oude zekerheden en nieuwe flessenhalzen

Edwin Kruisbergen, Rutger Leukfeldt, Edward Kleemans en Robby Roks[*]

Criminele netwerken gebruiken ICT op tal van manieren: voor onderlinge communicatie, om capabele mededaders en 'tools' te vinden, om afzetmarkten te vergroten, om een groter aantal potentiële slachtoffers te bereiken, en ook om criminele geldstromen af te schermen. Het regelen en afschermen van geldstromen is een essentiële opgave voor daders in de georganiseerde criminaliteit. Georganiseerde criminaliteit is primair ingegeven door financieel gewin. Maar criminele verdiensten brengen risico's met zich mee, vooral als je succesvol bent en je criminele activiteiten grote opbrengsten genereren. Criminele verdiensten en de besteding daarvan kunnen immers tot aandacht van de autoriteiten leiden, met arrestatie en inbeslagname van vermogen als mogelijke gevolgen.
Dit artikel biedt empirisch inzicht in hoe daders binnen de georganiseerde criminaliteit ICT gebruiken voor het regelen van hun geldstromen. We richten ons daarbij niet uitsluitend op cybercrime, maar verkennen juist het gebruik van ICT én de consequenties daarvan voor een breder scala van soorten georganiseerde criminaliteit, dus ook 'traditionele' georganiseerde criminaliteit zoals drugssmokkel. De empirische data die aan dit artikel ten grondslag liggen, bestaan uit

* Dr. E.W. Kruisbergen is als onderzoeker verbonden aan het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het ministerie van Justitie en Veiligheid. Dr. R. Leukfeldt is senior-onderzoeker cybercrime bij het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving en lector Cybersecurity in het mkb bij de Haagse Hogeschool. Prof. dr. E.R. Kleemans is hoogleraar zware criminaliteit en rechtshandhaving aan de Vrije Universiteit Amsterdam. Dr. R. Roks is universitair docent aan de Erasmus Universiteit Rotterdam.

doi: 10.5553/JV/016758502018044005003

dertig grootschalige opsporingsonderzoeken die zijn bestudeerd voor de Monitor Georganiseerde Criminaliteit.[1]
Hieronder lichten we eerst de onderzoeksopzet en de gebruikte bronnen toe. Vervolgens bespreken we de empirische resultaten van onze studie. Daarbij gaan we in op de criminele verdiensten zelf, maar met name op de besteding ervan en het afschermen van criminele inkomsten. We eindigen het artikel met conclusies. Aan de ene kant leidt ICT ook wat betreft het beheer van criminele geldstromen tot nieuwe werkwijzen. Aan de andere kant laten analyses zien dat oude zekerheden nog steeds een prominente rol spelen in keuzes van daders. Zo blijkt contant geld nog steeds een dominante factor in criminele geldstromen, zowel bij traditionele georganiseerde criminaliteit als bij cybercriminaliteit. Bovendien blijkt het omwisselen van digitale valuta voor contant geld een belangrijke flessenhals te zijn voor het criminele bedrijfsproces van daders die online opereren.

Onderzoeksopzet en gebruikte bronnen

Aan de basis van dit artikel liggen uitgebreide zaaksbeschrijvingen die zijn gemaakt na analyse van dertig opsporingsonderzoeken in de meest recente, vijfde ronde van de Monitor Georganiseerde Criminaliteit.[2] Elk van de dertig zaken bevat informatie over verschillende, soms tientallen verdachten. De selectie van de dertig zaken kwam tot stand na een intensieve inventarisatie van zaken bij centrale, regionale en gespecialiseerde eenheden van de politie en het Openbaar Ministerie (zie kader). Bij die selectie speelden verschillende criteria een rol:
- Er is sprake van een crimineel samenwerkingsverband.
- Het opsporingsonderzoek is afgerond (de belangrijkste verdachten zijn aangehouden) in 2011 of later.
- De zaak is rijk aan informatie.
- De zaak heeft toegevoegde waarde; er moet spreiding zijn over verschillende delicttypen.

1 Dit artikel is gebaseerd op een rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit. Voor een uitgebreide bespreking van de onderzoeksmethode, de gebruikte bronnen en de uitkomsten van empirische analyses op drie verschillende deelthema's, zie Kruisbergen e.a. 2018.
2 Vijf zaken op het terrein van cybercrime/ICT-gerelateerde georganiseerde criminaliteit zijn ook geanalyseerd in onderzoek van Odinot e.a. (2017).

doi: 10.5553/JV/016758502018044005003

Voor iedere zaak is het volledige opsporingsdossier bestudeerd aan de hand van een uitgebreide checklist.[3] De zaken beslaan verschillende soorten georganiseerde criminaliteit, onder meer verschillende typen drugsproductie en -handel, mensensmokkel/-handel, witwassen en cybercriminaliteit. Op basis van de rol die ICT speelt binnen een zaak, onderscheiden we vier categorieën zaken. De eerste categorie bevat 23 zaken van *traditionele georganiseerde criminaliteit*, dat wil zeggen zaken zonder een sterke ICT-component. Het gaat dan om gevallen van offline drugshandel, mensenhandel/-smokkel en andere (combinaties van) misdrijven.

De tweede categorie betreft *traditionele georganiseerde criminaliteit met ICT als belangrijk vernieuwend element* in de modus operandi. Het gaat om drie zaken. De eerste zaak betreft een dadergroepering die door middel van een hack in het netwerk van een haventerminal de afhandeling van binnenkomende containers manipuleert. De tweede zaak draait om betrokkenen bij een online marktplaats (een *darknet market*) waarop onder meer drugs worden verhandeld. In de derde zaak staat een moderne variant van witwassen centraal: het omwisselen van met criminaliteit verdiende bitcoins voor contante euro's.

De derde categorie betreft twee zaken van *georganiseerde low-tech cybercriminaliteit*. De eerste zaak richt zich op een variant van *skimmen* (ook wel *shimmen* genoemd). In de tweede zaak staan *phishing-operaties* centraal, waarbij daders toegangsgegevens van slachtoffers voor internetbankieren proberen te verkrijgen.

De vierde categorie ten slotte omvat twee gevallen van *georganiseerde high-tech cybercriminaliteit*. Beide zaken draaien om *banking malware*, waarbij daders via kwaadaardige software betalingen via internetbankieren manipuleren.

Waar dat relevant is, maken we bij de bespreking van de onderzoeksuitkomsten onderscheid tussen de vier genoemde categorieën. Vanwege de beperkte ruimte die dit artikel heeft, zullen we echter lang niet alle zaken individueel kunnen bespreken.[4]

3 Voor meer informatie over de (selectie van) zaken, zie Kruisbergen e.a. 2018, p. 22-31. In dezelfde publicatie is de gebruikte checklist integraal opgenomen (als bijlage).

4 Er is enige overlap tussen de categorieën (traditionele georganiseerde criminaliteit, (low-tech/high-tech) cybercriminaliteit, etc.) enerzijds en het te analyseren vraagstuk (hoe gaan daders om met criminele geldstromen?) anderzijds. Bij cybercriminaliteit is immers het digitale aspect in de modus operandi tot op zekere hoogte een gegeven. Echter, dat het gronddelict (bijv. drugshandel of banking malware) al dan niet digitaal van aard is, betekent niet automatisch dat de financiële component dat ook in dezelfde mate is.

doi: 10.5553/JV/016758502018044005003

De zaken die voor de Monitor Georganiseerde Criminaliteit worden geanalyseerd, vormen geen aselecte steekproef van *de* georganiseerde criminaliteit in Nederland. Ten eerste is iedere mogelijke steekproef van gevallen van georganiseerde criminaliteit nu eenmaal afhankelijk van opsporingsactiviteiten van de politie, en daarmee per definitie niet aselect. Ten tweede bestaat er geen geschikt centraal overzicht van alle zaken die hebben gespeeld in Nederland, waarmee een steekproefkader dus ontbreekt (en wat de inventarisatie van zaken ook tijdrovend maakt). Ten derde is het ook onverstandig om een aselecte steekproef van zaken te analyseren. Zou dat wel gebeuren, dan is de kans namelijk groot dat vooral zaken worden bestudeerd die relatief weinig kennis over georganiseerde criminaliteit toevoegen, bijvoorbeeld omdat ze delicttypen betreffen waarover al veel bekend is (bepaalde vormen van drugshandel), of omdat de zaak heel klein is en er weinig is doorgerechercheerd. Voor de inventarisatie van zaken zijn gesprekken gevoerd met (landelijke) specialisten op het terrein van cybercrime, cocaïne en heroïne, synthetische drugs en hennep, fraude en witwassen, overvallen, ram- en plofkraken, mensenhandel en Hollandse netwerken. Verder zijn zaken geïnventariseerd bij (andere) regionale en landelijke eenheden. Uiteindelijk zijn behalve landelijke eenheden alle tien regio's van de politie/het Openbaar Ministerie (OM) bij de inventarisatie betrokken. De inventarisatie leidde tot een 'longlist' van ongeveer zeventig zaken, waarvan er dertig zijn geselecteerd.

Criminele verdiensten en besteding

Vragen naar (besteding van) criminele verdiensten behoren tot de moeilijkste onderzoeksvragen op het terrein van de georganiseerde criminaliteit, simpelweg omdat een goed zicht op de financiële positie van daders vaak ontbreekt (Kleemans e.a. 2002, p. 124). Dit laatste geldt grosso modo ook voor de dertig zaken uit de meest recente, vijfde ronde van de Monitor Georganiseerde Criminaliteit. Dit is waarschijnlijk enerzijds het gevolg van succesvolle pogingen van daders om hun verdiensten en vermogen te onttrekken aan het zicht van de opsporing. Zo vermoedt een zaaksofficier in een drugszaak dat veel criminele verdiensten naar het land van herkomst van de daders zijn gestroomd. Anderzijds zijn er ook zaken waarin informatie erop wijst dat daders (nog) weinig verdiensten hebben gegenereerd op het

doi: 10.5553/JV/016758502018044005003

moment dat de politie ingreep.[5] Hoewel de financiële positie van daders in de georganiseerde criminaliteit verre van transparant is, bieden de dertig bestudeerde zaken, dankzij de inzet van soms verregaande opsporingsinstrumenten, toch veel interessante inzichten.
Waar besteden daders hun geld aan? Besteding valt grofweg uiteen in consumptie en investeringen. Op beide punten laten de analyses geen grote verschillen zien ten opzichte van eerder onderzoek (Kruisbergen e.a. 2015) en ook geen grote verschillen tussen traditionele en cybercriminaliteit. We beginnen met consumptie.
In verschillende zaken van offline en online criminaliteit zien we daders die er een uitbundige levensstijl en navenant uitgavenpatroon op na houden. Zo wordt in een van de casussen die zich op banking malware richten meer dan twee ton uitgegeven aan boten (casus 155).[6] Bij een crimineel samenwerkingsverband dat zich bezighoudt met het omwisselen van bitcoins voor euro's wordt informatie gevonden die wijst op verschillende grote uitgaven, onder meer aan auto's en helikoptervluchten (173). Er zijn echter ook daders bij wie er weinig of geen opvallende uitgavenposten worden vastgesteld. Sommigen lijken zelfs moeite te hebben om rond te komen. Dit laatste valt bijvoorbeeld af te leiden uit afgeluisterde gesprekken tussen twee verdachten in een drugszaak (casus 175).
Als een dader na consumptie en het voortzetten van criminele activiteiten geld over heeft van zijn criminele inkomsten, kan hij dat investeren in de reguliere economie.[7] Die investeringen in de legale economie zijn in zeker opzicht interessanter dan het consumptiepatroon van daders. De opbouw van posities in de reguliere economie, en meer in het algemeen de wisselwerking tussen 'onder-' en 'bovenwereld', vormt namelijk een belangrijke aanleiding tot beleidsmaatrege-

5 In verschillende zaken was het (financieel) onderzoek nog niet afgerond op het moment dat de zaak werd bestudeerd. Opsporingsonderzoeken waarin op het moment van bestuderen wel berekeningen waren gemaakt van de criminele verdiensten beslaan een grote bandbreedte: van een ton of enkele tonnen tot (vele) miljoenen.
6 De nummering is dezelfde als die is gebruikt in de monitorrapportage (Kruisbergen e.a. 2018). In die rapportage worden in een bijlage alle casussen afzonderlijk toegelicht. Omdat in de vijf rondes van de Monitor Georganiseerde Criminaliteit inmiddels 180 zaken zijn geanalyseerd, zijn de 30 zaken uit de vijfde ronde genummerd van 151 t/m 180.
7 Onder investeringen in de legale economie verstaan we onder meer onroerend goed, bedrijven, aandelen, obligaties en opties. Luxe goederen als auto's en horloges en andere juwelen hebben we in onze analyses niet meegenomen als investeringen. Ook het aanhouden van contant geld en tegoeden op bankrekeningen hebben we niet als investering meegenomen.

doi: 10.5553/JV/016758502018044005003

len tegen georganiseerde criminaliteit en tot antiwitwasbeleid in het bijzonder.

Voor de dertig zaken is gekeken naar bezittingen in de legale economie die aan daders zijn te relateren. Concreet gaat het daarbij om (gedeeltelijk) bezit van bedrijven en onroerend goed (al dan niet afgeschermd door bijvoorbeeld het gebruik van katvangers). Deze analyses zijn gebaseerd op alle informatie die in opsporingsdossiers aanwezig is over investeringen en bezittingen. Daarbij zijn de inbeslagnames meegenomen, maar ook informatie afkomstig uit andere bronnen, zoals bijvoorbeeld verhoren, observaties en undercoveroperaties.

Het patroon dat we in het grootste deel van de dertig zaken zien wat betreft de aard, omvang, plaats en het gebruik van de bezittingen in de legale economie komt overeen met het patroon dat werd gevonden bij eerdere analyses (Kruisbergen e.a. 2015). Dit investeringspatroon lijkt vrij conservatief, waarbij de fysieke en/of sociale afstand tussen een dader en zijn bezittingen vaak klein is. Zo investeren daders veel in het land waarin ze wonen en/of het land waar ze via een migratieachtergrond mee verbonden zijn. Verder investeren ze vooral in tastbare, 'bekende' vermogensbestanddelen, dat wil zeggen huizen en ander onroerend goed en bedrijven uit sectoren als groot-/detailhandel, horeca en transport. Ze gebruiken die bedrijven bovendien vaak ter ondersteuning van hun criminele activiteiten (zie Bruinsma & Bovenkerk 1996). Bedrijven worden daarbij ingezet voor logistieke doeleinden (zoals vervoer, opslag, ontmoetingen), voor het verhullen van criminele activiteiten (het bieden van een dekmantel van legaliteit voor illegale activiteiten) en voor witwasdoeleinden (door bijvoorbeeld te doen alsof inkomsten die feitelijk zijn verdiend met criminaliteit door legale bedrijfsactiviteiten zijn voortgebracht). De portfolio's van daders bestaan dus vooral uit onroerend goed en het genoemde type bedrijven. Daarentegen lijken minder tastbare, puur financiële bezittingen, zoals obligaties, opties en aandelen in bedrijven waarin daders níét persoonlijk betrokken zijn (bijvoorbeeld in beursgenoteerde bedrijven), veel minder vaak voor te komen. De zeven zaken van georganiseerde criminaliteit met een duidelijke ICT-component laten zoals gezegd geen grote verschillen zien met de andere, meer traditionele zaken.

doi: 10.5553/JV/016758502018044005003

Witwassen

Criminele geldstromen moeten worden afgeschermd. Wil een dader voorkomen dat zijn geld, en ook hijzelf, onderwerp van politieaandacht wordt, dan moeten dat geld en/of de illegale herkomst ervan verborgen blijven. Welke rol speelt ICT hierbij in de verschillende zaken?[8]

In hoe daders hun criminele inkomsten afschermen, zien we belangrijke verschillen tussen traditionele georganiseerde criminaliteit enerzijds en ICT-gerelateerde criminaliteit anderzijds. Bij de 23 zaken van traditionele georganiseerde criminaliteit zien we witwasmodaliteiten zoals die in eerdere publicaties zijn beschreven. Zo komen rudimentaire vormen voor als het verbergen en verplaatsen en het, al dan niet via stromannen of facilitators, uitgeven van grote bedragen aan contant geld aan bijvoorbeeld (het leasen van) auto's of het huren van onroerend goed (afgeschermde consumptie). Dit laatste zien we bijvoorbeeld in een zaak die draait om drugsproductie en -handel. De hoofdverdachte betaalt € 20.000 contant voor de huur van een Nederlands huis, betaalt meer dan € 20.000 contant voor de aankoop van een Mercedes, rekent vele duizenden euro's contant af voor de aanschaf van (water)scooters en laat een relatie bijna € 9.000 contant afrekenen voor een vakantiereis (casus 161). Ook meer complexe witwasconstructies worden in de zaken aangetroffen. Het gaat dan bijvoorbeeld om het fingeren van legale inkomsten uit dienstbetrekking of bedrijf, loan-backconstructies of het doorsluizen van geld via buitenlandse rechtspersonen.

Ook daders die zich bezighouden met traditionele georganiseerde criminaliteit zouden gebruik kunnen maken van nieuwe, door ICT mogelijk gemaakte betaal- en witwasmogelijkheden, zoals cryptovaluta. Een dader die bijvoorbeeld actief is in offline drugshandel zou de aanschaf van bitcoins kunnen gebruiken in een constructie om zijn geldstromen af te schermen, of als investering waarbij wordt gespeculeerd op

8 Voor een toelichting op wat witwassen is en welke varianten te onderkennen zijn, zie Kruisbergen & Soudijn 2015.

doi: 10.5553/JV/016758502018044005003

koersstijging.[9] In de 23 zaken van traditionele georganiseerde criminaliteit zien we echter nergens het gebruik van bitcoins of andere cryptovaluta. Wel wordt in een van de zaken geconstateerd dat daders gebruikmaken van prepaid cards, ook een zogenoemde *new payment method* (casus 165). De financiële innovatie van cryptovaluta ontbreekt dus in zaken van traditionele georganiseerde criminaliteit. Als het om witwaspatronen gaat, zijn de daders in deze 23 zaken van traditionele georganiseerde criminaliteit dus nog behoorlijk 'traditioneel'. Misschien zijn deze daders onbekend met de nieuwe mogelijkheden, zijn ze beducht voor de nadelen van cryptovaluta,[10] vinden ze het gewoonweg niet nodig om via ICT hun werkwijze drastisch te veranderen, of wist de politie het gebruik van virtuele munten niet op te sporen.

Bij ICT-gerelateerde criminaliteit zijn de opbrengsten, in tegenstelling tot veel vormen van traditionele georganiseerde criminaliteit, in eerste instantie vaak digitaal van aard. Drugshandelaren die actief zijn op een darknet market ontvangen de opbrengsten van hun handel vaak in een cryptomunteenheid zoals bitcoin. Bij bijvoorbeeld phishing- en malwareaanvallen verkrijgen daders door hun frauduleuze handelingen de controle over het online betalingsverkeer van hun slachtoffers, dat in digitale euro's verloopt. Casus 152 draait om online drugs- en wapenhandel via een darknet market. Online afgesloten drugstransacties worden betaald met bitcoins. In het opsporingsonderzoek wordt bij doorzoekingen beslag gelegd op honderden bitcoins, ter waarde van grofweg een half miljoen euro. Een van de moderators van de marktplaats handelt ook zelf in drugs. In het dossier wordt gemeld dat de genoemde moderator/drugshandelaar contacten heeft bij wie hij bitcoins kan omwisselen in fysieke euro's. Hij gaf er blijkbaar de voorkeur aan in ieder geval een deel van zijn verdiensten in fysieke euro's

9 Bitcoin is digitaal 'geld'. In tegenstelling tot reguliere munteenheden als de dollar en euro wordt deze cryptografische munteenheid niet uitgegeven, beheerd of gecontroleerd door een bank, overheid of een andere centrale actor. De creatie van bitcoins, aangeduid als *mining* (delven), verloopt decentraal, via een peer-to-peernetwerk, namelijk via computers van gebruikers. Zoals een bankbiljet wordt gedrukt en een munt wordt gesmeed, zo ontstaat een bitcoin door toepassing van een algoritme, oftewel een wiskundige formule. Bitcoins hebben geen fysieke vorm en worden bewaard in een *wallet*, een digitale portemonnee die online of bijvoorbeeld op een USB-stick wordt aangehouden (Kruisbergen & Soudijn 2015, p. 18-20).

10 Zoals het risico dat via het internet opgeslagen bitcoins kwijtraken of worden gestolen, de begrenzing van de anonimiteit waarmee bitcointransacties kunnen worden gedaan (Meiklejohn e.a. 2013; Ron & Shamir 2013; Oerlemans e.a. 2016), de extreem grillige koers en de geringe bruikbaarheid van bitcoin voor betalingen van reguliere goederen en diensten in de offline wereld.

doi: 10.5553/JV/016758502018044005003

aan te houden. Het omwisselen gebeurde via individuele bitcoinwisselaars met wie op openbare plekken werd afgesproken. Er zijn ook verschillende, gemakkelijk toegankelijke online *bitcoin exchanges*, maar wisseltransacties verlopen daar vaak via herleidbare kanalen, wat voor een drugshandelaar natuurlijk niet aantrekkelijk is. Omdat meer online handelaren hun bitcoins willen omwisselen in euro's, is de online handel in illegale goederen gepaard gegaan met een vraag naar bitcoinwisseldiensten, die met een grotere mate van anonimiteit worden aangeboden. Casus 173 richt zich op professionele facilitators die daarin voorzien.

> *De hoofdverdachten wisselen tegen betaling van een commissie aangeleverde bitcoins om voor contante euro's. Vermoedelijk is in ieder geval een deel van de door hen opgekochte bitcoins afkomstig van illegale handel op het darkweb. Aanwijzingen hiervoor zijn: de politie treft bij klanten van de bitcoinwisselaars voorwerpen aan die in verband staan met verzending van drugs; een bitcoin wallet van een klant is te relateren aan online drugshandel; klanten betalen voor het omwisselen een commissie van bijvoorbeeld 7%, veel hoger dan reguliere, online bitcoin exchangers rekenen.*
> *De bitcoinwisselaars ontmoeten hun klanten met name in lokale vestigingen van hamburger- of koffieketens (met wifi). Nadat een klant zijn bitcoins heeft overgeboekt naar een door de wisselaar gecontroleerde bitcoin wallet, krijgt de klant contant geld. De grote hoeveelheid bitcoins die de wisselaars aldus verkrijgen, levert voor henzelf ook een omwissel- en witwasprobleem op. De aangekochte bitcoins worden deels omgewisseld voor euro's bij reguliere bitcoin exchangers. Laatstgenoemden storten de euro's op rekeningen die onder controle staan van de wisselaars. Het geld wordt contant opgenomen en weer gebruikt voor de aankoop van bitcoins. In totaal zijn met de wisseldienst die de daders aanbieden miljoenen euro's gemoeid (casus 173).*

De zojuist besproken casussen 152 en 173 maken samen met casus 151 deel uit van de categorie traditionele georganiseerde criminaliteit met ICT als belangrijk vernieuwend element. Casussen 154 en 156 scharen we onder georganiseerde low-tech cybercriminaliteit. Ook hier zien we dat digitale valuta, in dit geval euro's, worden omgewisseld in fysieke, contante euro's. In casus 154, een al wat oudere zaak, manipuleren de daders kaartlezers van een grote Nederlandse bank om gegevens van rekeninghouders af te lezen. Met zelfgemaakte betaalpassen wordt vervolgens in meer dan tien verschillende landen

doi: 10.5553/JV/016758502018044005003

contant geld opgenomen, waarna het via fysiek vervoer of via *money transfers* wordt verplaatst. Casus 156 richt zich op daders die phishing-aanvallen uitvoeren. Daarbij wordt geld van de rekening van een slachtoffer overgeboekt naar de rekening van een zogenoemde *money mule*. Vervolgens wordt het geld contant opgenomen, door de money mule zelf of een ronselaar. Het gebruik van cryptovaluta, prepaidkaarten of andere innovaties zien we in de twee zaken niet.
Casussen 153 en 155 draaien beide om daders die betrokken zijn bij banking malware, hetgeen we als georganiseerde high-tech cybercriminaliteit hebben geclassificeerd. Het criminele samenwerkingsverband in casus 153 besmet computers en mobiele telefoons met software om banktransacties te manipuleren. De daders passen verschillende methoden toe om de criminele verdiensten af te schermen.[11] Zo wordt geld afkomstig van bankrekeningen van slachtoffers wel gebruikt om onder meer bitcoins, *WebMoney* en vouchers te kopen. De bitcoins worden vervolgens (ten dele) omgewisseld voor euro's. Een andere afschermingsmethode bestaat eruit dat met het geld online goederen zoals computers en telefoons worden aangekocht. Daarnaast komt het voor dat geld van de slachtoffers wordt overgeboekt naar rekeningen van money mules, waarna het contant wordt opgenomen.
In casus 155 gebruiken daders eveneens rekeningen van money mules en wordt geld vervolgens *gecasht*. Bovendien kopen ook deze daders bitcoins met een deel van het gestolen geld. Daarbij wordt bovendien een zogenoemde *bitcoin mixing service* gebruikt, om het spoor tussen zend- en ontvangstadres van een bitcoin te verhullen en aldus de identiteit van (in dit geval) de ontvanger te beschermen. In deze zaak wordt verder meer dan € 300.000 contant geld in beslag genomen. In deze twee zaken van cybercrime met een sterkere technische component (casus 153 en 155) worden dus wel 'nieuwe' betaalmethoden zoals bitcoins gebruikt. Tegelijkertijd zien we ook in deze zaken de centrale rol die contant geld speelt.

Cash is (still) king

Die centrale rol van contant geld is een overheersend, gemeenschappelijk kenmerk van veel van de door ons bestudeerde zaken, zowel op

11 Zie ook Oerlemans e.a. (2016, p. 78-79) voor een beschrijving van de werkwijze in deze zaak.

doi: 10.5553/JV/016758502018044005003

het terrein van traditionele als op het terrein van ICT-gerelateerde georganiseerde criminaliteit. Daders verbergen bijvoorbeeld contant geld of zorgen dat het in andere landen terechtkomt. Verder zagen we in ons casusmateriaal online drugshandelaren en daders van phishing- of banking-malwareaanvallen die hun digitale valuta omwisselen voor fysieke euro's (zie ook Leukfeldt 2014; Leukfeldt e.a. 2017; Oerlemans e.a. 2016; Europol 2015). Ten slotte gebruiken daders contant geld om kostbare goederen en diensten af te rekenen. Bij deze contante geldstromen maken daders gebruik van een breed scala aan dienstverleners, die onbewust, zonder veel vragen te stellen, of juist doelbewust daders helpen. Voor het verplaatsen van geld kunnen daders terecht bij ondergrondse bankiers of personen die gespecialiseerd zijn in de fysieke smokkel van geld. Voor het discreet omruilen van met drugshandel verdiende bitcoins voor contante euro's gebruiken daders bitcoinwisselaars. Dat deze dienstverleners waardevol zijn, komt terug in de prijs die hun klanten bereid zijn te betalen. Soudijn en Reuter (2016) berekenden de totale kosten voor cocaïnehandelaren van contant-geldsmokkel op 10 à 17% van het gesmokkelde bedrag. De prijs die klanten moeten betalen voor de diensten van de professionele bitcoinwisselaars die wij in casus 173 zagen, lijkt te variëren en ligt bijvoorbeeld op 7%, een stuk hoger dan bij reguliere bitcoin exchangers.[12]

Naast het verplaatsen en wisselen van criminele verdiensten is het accepteren van betalingen met contant geld een soort 'dienstverlening' die daders benutten. In de vijfde, maar ook in eerdere rondes van de monitor zien we aanbieders van goederen en diensten in de reguliere economie die schijnbaar zonder vragen te stellen contante betaling accepteren van (zeer) hoge bedragen (Kruisbergen e.a. 2012). Zij stellen daders in staat om hun criminele verdiensten ongestoord te consumeren. Het kan daarbij gaan om autobedrijven, aanbieders van woonruimte, elektronicawinkels, aannemers, reisbureaus en andere aanbieders van kostbare goederen en diensten.

12 Verder wordt, zoals we zagen, voor cashen van geld bij phishing- en banking-malwareaanvallen gebruikgemaakt van money mules. Zij zijn eerder katvangers dan professionele facilitators en hebben een meer inwisselbare positie in de periferie van criminele netwerken. Uit onderzoek blijkt dat ze vooral worden gerekruteerd onder jongvolwassenen uit armere wijken in stedelijke gebieden (Oerlemans e.a. 2016). Uit communicatie tussen daders in casus 155 komt naar voren dat zij money mules vooral zoeken onder gemakkelijk beïnvloedbare personen, die bijv. kampen met schulden, psychische problemen of drugsverslaving. In ons casusmateriaal zien we ook dat money mules de hun toegezegde vergoeding niet altijd krijgen (casus 156).

doi: 10.5553/JV/016758502018044005003

Discussie

In dit artikel bespraken we hoe daders binnen de georganiseerde criminaliteit ICT gebruiken voor het regelen van hun geldstromen. In ons casusmateriaal zagen we dat enerzijds gebruik wordt gemaakt van innovaties, zoals cryptovaluta en aanverwante diensten, maar dat anderzijds veel nog via traditionele patronen lijkt te verlopen, waarbij onder meer de dominante rol van contant geld opviel. Aan het slot van dit artikel benoemen we een aantal methodologische plus- en minpunten van ons onderzoek en gaan we kort in op de mogelijke implicaties van de uitkomsten.

Het onderzoek

Ons onderzoek is gebaseerd op de bestudering van dertig opsporingsonderzoeken. Opsporingsdossiers bevatten de verslaglegging van de inzet van de exclusieve opsporingsbevoegdheden die de politie heeft, zoals het afluisteren van gesprekken, de inbeslagname van goederen en de inzet van undercoveroperaties. Opsporingsdossiers bieden daarmee een rijk inzicht in onder andere de activiteiten van daders en de wijze waarop zij zich tot elkaar en hun omgeving verhouden. De uitgebreide verslagen die van deze opsporingsdossiers zijn gemaakt, stellen ons vooral in staat om onderbouwde, kwalitatieve uitspraken te doen over de *aard* van de georganiseerde criminaliteit in Nederland. Uitspraken over *hoe vaak* bijvoorbeeld een bepaalde werkwijze voorkomt, kunnen alleen binnen de context van de bestudeerde zaken worden gedaan; ze kunnen niet worden veralgemeniseerd naar *de* georganiseerde criminaliteit.[13]
Opsporingsdossiers vormen een rijke bron, maar kennen beperkingen. Zo zijn alleen gevallen van georganiseerde criminaliteit meegenomen die door Nederlandse autoriteiten zijn opgespoord en onder de door ons gehanteerde begripsomschrijving van georganiseerde criminaliteit vallen. Datgene wat buiten het zicht van de Nederlandse opsporings-

13 Wel is vanwege het grote aantal zaken dat inmiddels binnen de Monitor Georganiseerde Criminaliteit is bestudeerd (180, waarin informatie aanwezig is over in totaal honderden verdachten), het doen van kwantitatieve analyses op specifieke deelterreinen mogelijk, mits daarbij het genoemde voorbehoud wordt gemaakt. Voorbeelden hiervan zijn: de analyse van criminele carrières (Van Koppen 2013), analyse van investeringen van daders in de legale economie (Kruisbergen e.a. 2015), analyse van de rechtsgang en de incasso bij ontnemingsmaatregelen (Kruisbergen e.a. 2016) en de analyse van geëiste en opgelegde straffen (Van Wingerde & Van de Bunt 2017).

doi: 10.5553/JV/016758502018044005003

praktijk valt, blijft ook buiten het bereik van ons onderzoek. Voor cybercrime werkt deze beperking mogelijk sterker uit dan bij andere vormen van georganiseerde criminaliteit. Juist bij cybercrime kan in de modus operandi of dadergroepering namelijk sprake zijn van een internationale component en bovendien komen lang niet alle door politie en justitie gepleegde interventies tegen cybercrime uiteindelijk terecht in individuele opsporingsdossiers.[14]

Mogelijke beleidsimplicaties

Cryptovaluta vormen een belangrijke financiële innovatie. Het is ook een belangrijke, door technologie gedreven vernieuwing in de werkwijze bij witwassen. Samen met onder andere prepaidkaarten is het een van de weinige veranderingen binnen opgespoorde witwasvormen, die verder vooral door traditionele, beproefde werkwijzen worden gedomineerd. Dit zien we in ons casusmateriaal, maar komt ook naar voren uit een analyse van vier criminaliteitsbeeldanalyses op het terrein van witwassen, die tezamen een periode van twaalf jaar beslaan (Soudijn 2018).
Cryptovaluta zoals bitcoin zijn op dit moment grotendeels ongereguleerd. Ook aanverwante diensten vallen nu grotendeels buiten financiele regulering en toezicht, waardoor bijvoorbeeld bitcoin exchangers niet meldplichtig zijn in het kader van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). Nieuwe criminele werkwijzen, zoals het gebruik van bitcoin, roepen de vraag op of bestaande wet- en regelgeving voldoende is toegerust voor de nieuwe situatie. Met andere woorden, moeten cryptovaluta worden gereguleerd? Dit is natuurlijk een puur beleidsmatige, politieke keuze. Een voordeel van regulering is dat regulering en toezicht aangrijpingspunten kunnen bieden om witwassen via cryptovaluta tegen te gaan. Online wisselkantoren voor cryptovaluta zouden zo bijvoorbeeld onder het bereik van Nederlandse toezichthouders kunnen worden gebracht. Vanuit antiwitwasperspectief kan regulering echter ook nadelen hebben. De acceptatie van cryptovaluta in de reguliere economie lijkt op dit moment nog laag; wie een glas cola wil kopen, een nieuwe spijkerbroek, een auto of een huis, kan dit meestal niet met bitcoin doen. Regulering kan bijdragen aan normalisering van cryptovaluta en een

14 Voor een meer uitgebreide bespreking, zie Kruisbergen e.a. (2018, p. 24-31, 102-103).

doi: 10.5553/JV/016758502018044005003

hogere acceptatiegraad van deze nieuwe 'munten' als betaalmiddel. Daarmee zouden de mogelijkheden om op criminele wijze verdiende cryptovaluta in de reguliere economie om te zetten, wit te wassen, juist worden vergroot (zie ook Oerlemans e.a. 2016).

Ondanks de innovatie die cryptovaluta (samen met enkele andere vernieuwingen, zie Soudijn 2018) wel degelijk zijn, speelt contant geld nog steeds een hoofdrol in de criminele wereld, ook wanneer de criminelen zich met online activiteiten bezighouden (zie ook Europol 2015; Oerlemans e.a. 2016; Soudijn 2018). De prominente rol die contant geld speelt, biedt verschillende aanknopingspunten voor opsporing en beleid. Bij verschillende vormen van ICT-gerelateerde criminaliteit is het incasseren of omwisselen van de opbrengsten een fase waarin daders kwetsbaar zijn. Deze flessenhals in het criminele bedrijfsproces geldt bijvoorbeeld voor daders van banking malware en phishing die hun digitale euro's willen omwisselen in contanten. Hij doet zich ook voor bij de drugshandelaren die hun op het darknet verdiende cryptovaluta willen omruilen voor contante euro's. De flessenhals bestaat eruit dat daders in deze fase nogal eens, direct of indirect, in contact komen met de reguliere omgeving, zoals het reguliere bankverkeer. Dat biedt kansen voor detectie, opsporing en uiteindelijk preventie.[15] Hebben daders eenmaal contant geld in handen – als directe opbrengst van bijvoorbeeld traditionele offline drugshandel, of indirect nadat daders hun digitale valuta voor fysiek geld hebben omgewisseld –, dan vindt het een bestemmingsdoel.[16] Ons casusmateriaal geeft aanleiding te vermoeden dat veel op criminele wijze verdiend geld in contante vorm zijn weg vindt in de reguliere economie. Ook andere studies tonen dit aan (Soudijn 2017; Kruisbergen e.a. 2012; Soudijn & Akse 2012). Daarbij gaat het om de dagelijkse uitgaven van daders (die al aanzienlijk kunnen zijn), maar ook om uitgaven aan onder meer reizen, auto's, inrichting en woonruimte. Bij dit (afgeschermd) consumeren kunnen daders gebruikmaken van stromannen of gespecialiseerde dienstverleners, die daders bijvoorbeeld in staat stellen om woonruimte of auto's te gebruiken zonder dat dit tot hun

15 Het *cashen* van geld bij bijv. banking malware via money mules houdt in dat deze money mules hun reguliere bankrekening beschikbaar stellen. Ook bij het omwisselen van bitcoins voor euro's kan (indirect) contact met het reguliere betalingsverkeer ontstaan. Dit is bijv. het geval wanneer een individuele bitcoinwisselaar de door hem opgekochte bitcoins zelf ook wil omwisselen en daarvoor (uiteindelijk) van een reguliere partij gebruikmaakt.

16 Die bestemming kan er ook uit bestaan dat het geld in eerste instantie wordt bewaard of verplaatst.

doi: 10.5553/JV/016758502018044005003

persoon herleidbaar is. Daders worden echter ook, bewust of onbewust, gefaciliteerd door verkopers die hun kostbare goederen of diensten zonder problemen contant laten betalen.
Vanwege de dominante rol die contant geld speelt in offline én online criminaliteit, kan ook de aanpak van cybercriminaliteit profiteren van generieke maatregelen tegen contante criminele geldstromen.[17] Het bemoeilijken van onder andere consumptie van criminele verdiensten, door bijvoorbeeld het verhogen van het bewustzijn of het uitbreiden van de meldingsplicht, kan hieraan een zinvolle bijdrage leveren.

Literatuur

Bruinsma & Bovenkerk 1996
G.J.N. Bruinsma & F. Bovenkerk (red.), *De georganiseerde criminaliteit in Nederland: de branches*, Den Haag: Sdu Uitgevers 1996.

Europol 2015
Europol, *Why is cash still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering*, Den Haag: European Police Office 2015.

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

Van Koppen 2013
M.V. van Koppen, *Pathways into organized crime: Criminal opportunities and adult-onset offending* (diss. Amsterdam VU), Alblasserdam: Haveka 2013.

Kruisbergen & Soudijn 2015
E.W. Kruisbergen & M.R.J. Soudijn, 'Wat is witwassen eigenlijk? Introductie tot theorie en praktijk', *Justitiële verkenningen* 41 2015, afl. 1, p. 10-23.

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

17 Het gebruik van grote coupures door daders (en anderen) wordt op termijn bemoeilijkt doordat de ECB in 2018 zal stoppen met de productie van nieuwe € 500-biljetten.

doi: 10.5553/JV/016758502018044005003

Kruisbergen e.a. 2015
E.W. Kruisbergen, E.R. Kleemans & R.F. Kouwenberg, 'Profitability, power, or proximity? Organized crime offenders investing their money in legal economy', *European Journal on Criminal Policy and Research* (21) 2015, afl. 2, p. 237-256.

Kruisbergen e.a. 2016
E.W. Kruisbergen, E.R. Kleemans & R.F. Kouwenberg, 'Explaining attrition: Investigating and confiscating the profits of organized crime', *European Journal of Criminology* (13) 2016, afl. 6, p. 677-695.

Kruisbergen e.a. 2018
E.W. Kruisbergen, E.R. Leukfeldt, E.R. Kleemans & R.A. Roks, *Georganiseerde criminaliteit en ICT. Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit* (Cahier 2018-8), Den Haag: WODC 2018.

Leukfeldt 2014
E.R. Leukfeldt, 'Cybercrime and social ties: Phishing in Amsterdam', *Trends in Organized Crime* (17) 2014, afl. 4, p. 231-249.

Leukfeldt e.a. 2017
E.R. Leukfeldt, E.R. Kleemans & W.P. Stol, 'Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks', *British Journal of Criminology* 2017, DOI:10.1093/bjc/azw009.

Meiklejohn e.a. 2013
S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G.M. Voelker & S. Savage, *A fistful of bitcoins: Characterizing payments among men with no names*, San Diego: University of California 2013.

Odinot e.a. 2017
G. Odinot, M.A. Verhoeven, R.L.D. Pool & C.J. de Poot, *Organised cybercrime in the Netherlands: Empirical findings and implications for law enforcement*, Den Haag: WODC 2017.

Oerlemans e.a. 2016
J.J. Oerlemans, B.H.M. Custers, R.L.D. Pool & R. Cornelisse, *Cybercrime en witwassen: bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware* (O&B 319), Den Haag: Boom criminologie 2016.

Ron & Shamir 2013
D. Ron & A. Shamir, 'Quantitative analysis of the full bitcoin transaction graph', in: A.-R. Sadeghi (red.), *Financial cryptography and data security. Lecture notes in computer science* (Vol. 7859), Heidelberg: Springer 2013, p. 6-24.

Soudijn 2017
M.R.J. Soudijn, *Witwassen. Criminaliteitsbeeldanalyse 2016*, Zoetermeer: Politie, Landelijke Eenheid, Dienst Landelijke Informatieorganisatie 2017.

doi: 10.5553/JV/016758502018044005003

Soudijn 2018
M.R.J. Soudijn, 'Using police reports to monitor money laundering developments. Continuity and change in 12 years of Dutch money laundering crime pattern analyses', *European Journal on Criminal Policy and Research* 2018, DOI:10.1007/s10610-018-9379-0.

Soudijn & Akse 2012
M.R.J. Soudijn & Th. Akse, *Witwassen. Criminaliteitsbeeldanalyse 2012*, Driebergen: KLPD, Dienst Nationale Recherche 2012.

Soudijn & Reuter 2016
M.R.J. Soudijn & P. Reuter, 'Cash and carry: The high cost of currency smuggling in the drug trade', *Crime, Law and Social Change* (66) 2016, afl. 3, p. 271-290.

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

doi: 10.5553/JV/016758502018044005003