# De aard en aanpak van georganiseerde cybercrime

*Bevindingen uit een internationale empirische studie*

Odinot, Geralda; de Poot, Christianne; Verhoeven, Maite

**DOI**
10.5553/JV/016758502018044005002

**Publication date**
2018

**Document Version**
Final published version

**Published in**
Justitiele Verkenningen

# De aard en aanpak van georganiseerde cybercrime

## Bevindingen uit een internationale empirische studie

***Geralda Odinot, Christianne de Poot en Maite Verhoeven****

Ons dagelijks leven is enorm gedigitaliseerd en verweven met het internet. Deze ontwikkeling biedt allerlei nieuwe mogelijkheden voor het plegen van criminaliteit. Cybercriminaliteit is volgens McAfee[1] een *growth industry*, waar de opbrengsten hoog zijn en de pakkansen laag. De opkomst van cybercriminaliteit en de kans om hier slachtoffer van te worden zijn een zorg voor de samenleving, de rechtshandhaving en het beleid van het ministerie van Justitie en Veiligheid (J&V). Over de aard en de organisatie van deze criminaliteit is nog niet veel informatie beschikbaar, terwijl kennis hierover essentieel is om dit fenomeen aan te kunnen pakken. Wie zijn de daders van deze misdrijven en hoe gaan ze te werk? Hoe kan de politie deze criminaliteit opsporen en op welke manieren kan cybercriminaliteit worden tegengegaan?
Om antwoord te vinden op deze vragen hebben onderzoekers uit Duitsland, Zweden en Nederland de handen ineengeslagen en gezamenlijk onderzoek gedaan naar ernstige vormen van georganiseerde cybercriminaliteit.[2] Ten behoeve van dit onderzoek zijn in deze drie landen dossiers bestudeerd van opsporingsonderzoeken die gericht waren op ernstige vormen van georganiseerde cybercriminaliteit. Bij

* Dr. G. Odinot is wetenschappelijk onderzoeker en trainer forensisch interviewen How2Ask. Ten tijde van de uitvoering van het onderzoek waarop dit artikel is gebaseerd, was zij werkzaam als onderzoeker bij het WODC. Dr. C.J. de Poot is als senioronderzoeker verbonden aan het WODC. Zij is tevens hoogleraar Criminalistiek aan de Vrije Universiteit en lector Forensisch onderzoek aan de Hogeschool van Amsterdam en de Politieacademie. Dr. M.A. Verhoeven is als beleidsmedewerker Rechtshandhaving & Ketensamenwerking Cariben verbonden aan het ministerie van Justitie en Veiligheid. Ten tijde van de uitvoering van het onderzoek waarop dit artikel is gebaseerd, was zij werkzaam als onderzoeker bij het WODC.

1 Zie https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/McAfee%20and%20CSIS%20-%20Econ%20Cybercrime.pdf.

2 Zie voor het hele rapport: BKA, WODC & BRA (2016), *Cyber-OC … Scope and manifestations in selected EU member states* (HOME/2012/ISEC/AG/4000004382). Polizei + Forschung, 50.

doi: 10.5553/JV/016758502018044005002

de selectie van de dossiers is uitgegaan van de definities van georganiseerde misdaad van Europol.[3] Daarin wordt onder andere gesteld dat er sprake is van een crimineel samenwerkingsverband wanneer minimaal twee personen gedurende een langere periode samenwerken met als doel geldelijk gewin of macht. Daarnaast zijn enkele zaken geselecteerd die voldeden aan een van de vier categorieën van cybercrime, zoals omschreven door Wall (2007) en Martin (2013). Deze categorisering maakt een indeling die gebaseerd is op de rol die ICT en computers hebben bij het plegen van het delict.

In totaal werden er ten behoeve van dit onderzoek 44 zaken geselecteerd uit de periode 2009-2014, 18 uit Duitsland, 15 uit Zweden en 11 uit Nederland. Deze hadden betrekking op verschillende vormen van georganiseerde cybercriminaliteit, zoals het verspreiden van malware, hacking, het runnen van botnets, phishing, misbruik van het bankwezen, het (digitaal) witwassen van geld en illegale online handel. Alle geselecteerde zaken zijn bestudeerd met een Engelse vertaling van de checklist, die ontwikkeld is voor de Monitor Georganiseerde Criminaliteit (Kleemans e.a. 1998; Kleemans e.a. 2002; Van de Bunt & Kleemans 2007; Kruisbergen e.a. 2012). Ook zijn diepte-interviews gehouden met experts van politie en justitie,[4] zowel om beter zicht te krijgen op de concrete zaken als om meer algemene informatie te achterhalen over de aard en de aanpak van dit fenomeen.

Door de internationale samenwerking en de daarmee gepaard gaande gegevensverzameling in drie landen is een bijzondere en unieke dataset ontstaan waarmee het fenomeen cybercrime op basis van empirische gegevens vanuit een internationaal perspectief kan worden bestudeerd. Dit artikel is gebaseerd op de slotconclusie van het rapport, waarin alle bevindingen van de drie instituten zijn samengevoegd. De focus van dit artikel is gericht op de vraag of traditionele georganiseerde misdaad de weg naar het internet heeft weten te vinden. Gebeurt cybercrime in georganiseerd verband, en zo ja, hoe zien de organisatie en structuur van een dergelijke online organisatie er dan uit? Welke gevolgen heeft dit voor de opsporing van georganiseerde cybercriminaliteit?

3 Europols criteria voor 'organized criminal groups' (Doc 6204/2/97 ENFOPOL 35 Rev 2).

4 De bevindingen zijn ook voor elk land afzonderlijk beschreven. De resultaten en conclusies specifiek voor Nederland zijn te vinden in: Odinot e.a. 2017.

doi: 10.5553/JV/016758502018044005002

## De modus operandi

Het internet heeft inmiddels een prominente plek ingenomen als plaats voor het plegen van criminaliteit. De terminologie waarmee verschillende vormen van cybercrime worden aangeduid, is niet altijd even duidelijk. In het Nederlands wordt vaak gesproken over cybercrime in ruime zin en cybercrime in enge zin.[5] Onder cybercrime in ruime zin wordt traditionele criminaliteit verstaan waarbij gebruik wordt gemaakt van computers of netwerken. Bij cybercrime in enge zin is ICT zowel het doel als het middel. Voor vormen van traditionele criminaliteit waarbij gebruik wordt gemaakt van ICT, zoals het verkopen van illegale spullen, oplichting of bedreiging via internet en het verspreiden van kinderporno, gebruikt Wall (2014) de term *cyber-enabled* criminaliteit. Vaak gaat het bij deze misdrijven om hybride vormen van criminaliteit waarbij het internet zorgt voor schaalvergroting van de afzetmarkt van traditionele misdaden. Daarnaast zorgt het internet ook voor het vergroten en verbreden van het criminele netwerk. Wanneer het internet weg zou vallen, zou de criminaliteit in een andere vorm blijven bestaan. Dit is niet het geval bij cybercrime in enge zin. Daarbij gaat het om criminaliteit die met computers tegen computers wordt gepleegd. Deze criminaliteit wordt door Wall aangeduid met de term *cyber-dependent* criminaliteit. Phishing, hacken, het verspreiden van ransomware en het opzetten, verhuren en/of beheren van een botnet zijn hier voorbeelden van.

Door de anonimiteit die het internet kan bieden is het opsporen van daders die zich schuldig maken aan dit soort delicten bijzonder moeilijk. Om ondervertegenwoordiging van bepaalde misdrijven te minimaliseren zijn daarom ook zaken opgenomen waarin slechts één van de betrokken verdachten kon worden geïdentificeerd en kon worden vervolgd. In dat geval bleek uit het dossier dat er sprake was van een samenwerkingsrelatie met personen van wie de identiteit in het onderzoek niet kon worden achterhaald, of van een misdrijf dat volgens de opsporingsexperts gezien de aard en omvang onmogelijk door één persoon kon worden gepleegd. Er bevinden zich voorbeelden van zowel georganiseerde *cyber-enabled* als van georganiseerde *cyber-dependent* criminaliteit in onze dataset. Daarmee hebben we ons gericht op alle vormen van ernstige georganiseerde cybercriminaliteit.

5 Zie bijv. Cybersecuritybeeld Nederland 2018 van de NCTV.

doi: 10.5553/JV/016758502018044005002

*De cyber lift voor traditionele misdaad*

De bestudeerde casussen laten zien dat het betreden van de digitale wereld en het samenwerken met ICT-specialisten de impact van traditionele misdaad vergroten. In meerdere casussen schakelen verdachten een ICT-specialist in om criminele activiteiten te kunnen plegen. Zo kwamen we een zaak tegen waarin een ICT-specialist samenwerkte met 'traditionele' drugshandelaren en voor hen een digitale marktplaats bouwde die bedoeld was om drugs op het darkweb te verkopen. Als de vakkundigheid en betrouwbaarheid van deze specialist worden gewaardeerd, leidt dit soms tot een intensievere samenwerking. Er zijn ook voorbeelden van zaken waarbij de ICT-specialist een cruciale rol speelde bij het uitvoeren van de criminele activiteiten en waarin deze persoon een significant deel van de opbrengst kreeg. Een mooi voorbeeld daarvan zagen we in een zaak waarin een technicus werd ingezet vanwege zijn specialistische kennis voor het aanpassen van chips in bankpassen. Er zijn echter ook casussen waarin een ICT-specialist voor een enkele dienst werd ingehuurd. In zo'n zaak werd een computersysteem in opdracht gehackt voor het achterhalen van specifieke informatie.

Er bleken echter ook casussen te zijn waarin georganiseerde misdaadgroepen, naast hun traditionele criminelen activiteiten, heel goed in staat bleken om zelf cyberdelicten te plegen die een hoge mate van (technologische) kennis vereisen. Zo wisten criminelen in een zaak zelf mailadressen buit te maken. Vervolgens stuurden ze een e-mail naar die adressen, waarmee de ontvangende computers met malware werden besmet. Deze malware zorgde ervoor dat betalingsverkeer werd omgeleid naar de rekening van de criminelen.

Zoals hierboven al werd beschreven, zorgen de mogelijkheden die ICT en het internet bieden niet alleen voor nieuwe vormen van criminaliteit, maar ook voor een transformatie van traditionele criminaliteit. Dit komt doordat het internet gebruikt kan worden om op een veel grotere schaal actief te zijn. De impact van misdaden als drugshandel, mensenhandel, afpersing, fraude, illegaal gokken en handel in namaakartikelen wordt daarmee groter. Zo kunnen illegale goederen wereldwijd worden verkocht en kan kennis wereldwijd worden uitgewisseld. Deze vergroting van scope, impact en mate van afscherming die de bestudeerde dossiers laten zien, wordt door Wall (2007) aangeduid met de term '*cyber lift*'.

doi: 10.5553/JV/016758502018044005002

Het plegen van cyberdelicten lijkt met de jaren eenvoudiger te zijn geworden. Het vereist minder technische kennis, omdat kennis over modus operandi via fora wordt gedeeld, en specifieke kennis eenvoudigweg kan worden gekocht. Dit leidt niet alleen tot een *lift* van traditionele misdrijven, maar heeft tevens tot gevolg dat traditionele georganiseerde misdaadgroepen ook betrokken raken bij *cybercrime in enge zin*. De dossiers laten zien dat deze groepen specialistische kennis inkopen door specialisten in te huren (*crime-as-a-service*), of door kant-en-klare doe-het-zelfpakketten aan te schaffen. *Crime-as-a-service* lijkt een lucratieve handel en kan als een opzichzelfstaand fenomeen worden gezien, hoewel recent onderzoek laat zien dat de omvang van deze markt beperkt is.[6] Door het gemak waarmee kennis kan worden ingekocht, wordt de drempel voor het plegen van cybercrime verlaagd en de criminele horizon op internet verruimd. Dit biedt kansen voor zowel traditionele georganiseerde misdaadgroepen als nieuwe spelers in het veld.

*Benutten van de digitale infrastructuur*

Traditionele vormen van georganiseerde misdaad kenmerken zich door complexe logistieke processen, waarbij toegang moet worden verkregen tot leveranciers, transporteurs en klanten. Vaak is hierbij sprake van transnationale contacten en handelsstromen, en in alle gevallen moeten verschillende activiteiten in tijd en ruimte op elkaar worden afgestemd. Dankzij het internet kunnen dit soort processen sterk worden vereenvoudigd. Daders van cybercrime kunnen in theorie achter hun computer blijven zitten om samen te werken, contacten te leggen met leveranciers en klanten, en om activiteiten te coördineren.

Uit de bestudeerde casussen bleek dat daders van *cyber-enabled crime* de infrastructuur die nodig is om deze misdrijven te kunnen plegen in het algemeen zelf opbouwen en beheren. Zo verlopen de koop en verkoop in deze zaken regelmatig via zelf gemaakte en beheerde websites en online fora.

Juist bij de technisch meer geavanceerde vormen van *cyber-dependent crime* ligt dit anders. De bestudeerde netwerken blijken voor het verrichten van hun misdrijven veelvuldig gebruik te maken van

6 Zie https://www.tudelft.nl/2018/tu-delft/eerste-grootschalige-marktanalyse-ondergrondse-cybercrime-economie/.

doi: 10.5553/JV/016758502018044005002

bestaande digitale infrastructuren van bedrijven en overheden. In de bestudeerde zaken vonden deze activiteiten vaak op en via het 'gewone' reguliere internet plaats en niet per se op afgeschermde duistere plaatsen van het net. Voor het verkrijgen van toegang tot databases of eigendommen van slachtoffers, door middel van een hack, hoeven niet per se eigen structuren of voorzieningen te worden ontwikkeld. In een van de bestudeerde dossiers werd bijvoorbeeld gebruikgemaakt van reclamefoto's op een bekende website om computers van nietsvermoedende klikkende bezoekers te besmetten met ransomware. Doordat de maatschappij verder is gedigitaliseerd, zijn er meer mogelijkheden ontstaan voor het plegen van transnationale georganiseerde cybercrime. Onervaren daders die niet beschikken over de netwerken, contacten en infrastructuur die nodig zijn voor het plegen van traditionele georganiseerde misdaad, kunnen hierdoor toch relatief eenvoudig in deze geavanceerde vormen van georganiseerde cybercrime instappen.

*Facilitering van georganiseerde misdaad*

Naast de digitale infrastructuur worden ook andere nieuwe gelegenheidsstructuren en faciliteringsmechanismen benut bij het plegen van cybercrime. Hierbij springt allereerst de manier waarop geld kan worden overgedragen en kan worden witgewassen via het internet in het oog (zie ook Oerlemans e.a. 2016). Door gebruik te maken van cryptovaluta's of van geldoverdrachten via webaccounts die als bankrekening kunnen worden gebruikt, is het relatief eenvoudig om wereldwijd afgeschermde geldoverdrachten uit te voeren. Uit de dossiers kon niet worden afgeleid op welke wijze het geld in specifieke zaken precies wordt overgedragen en witgewassen. Wel bleek uit het onderzoek dat het gebruik van cryptovaluta's nieuwe ondergrondse economische structuren met zich meebrengt, die moeilijk te beheersen zijn.

Parallel aan deze nieuwe economische structuren komen er ook nieuwe faciliteerders in beeld, zoals online financiële dienstverleners en handelaren in cryptovaluta's, die de criminele activiteiten bewust of onbewust met hun diensten ondersteunen.

Naast financiële dienstverleners springen in de door ons bestudeerde dossiers ook andere nieuwe faciliteerders in het oog die, al dan niet bewust, cybercrime faciliteren. Denk bijvoorbeeld aan hostingprovi-

doi: 10.5553/JV/016758502018044005002

ders waar dubieuze websites een plek hebben en online reclamebureaus die advertenties plaatsen met verborgen software. Maar ook webwinkels en koeriersdiensten die door verdachten worden gebruikt voor de distributie van goederen en van geld. Daarnaast zagen we ook faciliteerders die we kennen vanuit de traditionele vormen van georganiseerde misdaad, zoals dekmantelondernemingen die dienstbaar zijn bij het afschermen van zaken, geldhandelaren en geldezels die hun rekeningnummers ter beschikking stellen en cash innen.
Soms maken faciliteerders deel uit van het sociale netwerk van de verdachten, maar vaker komen verdachten via het internet met hen in contact. De meeste faciliteerders raken bewust betrokken bij de criminele activiteiten, maar het gebeurt ook onvrijwillig en onbewust. Lang niet alle faciliteerders lijken te weten dat zij met hun diensten criminele activiteiten mogelijk maken, en dat zij hiervoor door de verdachten worden gebruikt. Denk bijvoorbeeld aan koeriersdiensten die wereldwijd pakketten vervoeren en afleveren. Of de eigenaar/beheerder van de populaire website waarop een reclamebureau besmette foto's plaatste om bezoekers te infecteren met malware.

### Structuur en organisatie van cybergroepen

De manier waarop verdachten in de bestudeerde zaken met elkaar samenwerken, komt deels overeen met wat we weten over samenwerking in de traditionele georganiseerde misdaad. Er is sprake van dynamische netwerken; veranderlijke samenwerkingsvormen die worden aangepast aan de criminaliteit die wordt gepleegd. Sociale relaties zijn hierbij van belang. In de bestudeerde casussen spelen familiebanden, vriendschappen, online en offline sociale contacten op allerlei manieren een rol: een bevinding die overeenkomt met eerder onderzoek waaruit bleek dat daders elkaar vaak persoonlijk kennen (Kruisbergen e.a. 2018).
De casussen laten zowel bestaande groepen als nieuwe groepen zien. Cybercrime in enge zin is meestal georganiseerd rond een harde kern, die eventueel ondersteuning zoekt voor zijn activiteiten bij een breed netwerk van mensen. Hierbij kan het gaan om het ronselen van mensen die virtueel geld willen omzetten naar cash, de geldezels, maar ook om het ronselen van mensen met de juiste ICT-vaardigheden, die via het internet gemakkelijk te vinden zijn. Er lijkt hierbij minder te

doi: 10.5553/JV/016758502018044005002

worden geïnvesteerd in relaties met mededaders dan bij traditionele vormen van georganiseerde misdaad. Als je weet waar je moet zoeken, zijn medeplegers met specifieke ICT-vaardigheden blijkbaar gemakkelijk te vinden en daardoor is het minder noodzakelijk om te investeren in bestaande relaties om deze ten behoeve van toekomstige activiteiten te behouden.
De wijze van samenwerking kan het best worden omschreven als losjes, flexibel en opportunistisch, en is minder dan bij traditionele georganiseerde misdaad gebaseerd op langdurige sociale relaties. De samenstelling van het samenwerkingsverband is afgestemd op de kennis en kunde die voor het plegen van een specifiek delict nodig zijn. Nieuwkomers in het veld treden vaak op als 'onderaannemers' of vormen een netwerk waar een persoon of groep weer mee in contact staat. Het wereldwijde karakter van het internet faciliteert het ontstaan van deze netwerken of schakels van mensen. De individuele leden die allen beschikken over specifieke kennis zijn niet per se in staat om de vaak technisch complexe delicten op te zetten en uit te voeren. Het is juist de samenwerking tussen deze individuen, die elkaar weten te vinden op het internet, die de criminele activiteiten mogelijk maakt. Fora, communicatieplatformen op internet, fungeren daarbij als ontmoetingsplaats (Soudijn & Monsma 2012**;** Wall & Williams 2014). Hier worden contacten gelegd en wordt informatie uitgewisseld. Op deze manier kunnen verdachten online relaties opbouwen, samenwerken en communiceren zonder elkaar offline te hoeven ontmoeten. Deze kanalen worden ook gebruikt voor de verkoop en het delen van kennis, software, scripts, goederen, producten en ruw materiaal. Het feit dat online communicatiediensten versleuteld zijn en de gebruiker vaak anoniem kan blijven door het gebruik van anonimiseringssoftware, blijkt een belangrijke motivatie te zijn om deze fora te verkiezen boven de meer traditionele communicatiekanalen. In de bestudeerde dossiers konden we constateren dat er vaak zonder terughoudendheid werd gecommuniceerd over uiteenlopende zaken.

*Vertrouwen*

Bij de losse, flexibele en opportunistische samenwerkingsverbanden die een deel van de dossiers te zien gaf, is de verantwoordelijkheid voor de uitvoering van een misdaad verspreid over meerdere personen. De rol die 'vertrouwen' speelt bij online samenwerkingsverban-

doi: 10.5553/JV/016758502018044005002

den krijgt hiermee een andere vorm dan die we kennen uit de traditionele georganiseerde misdaad. Bij traditionele georganiseerde misdaad zijn langdurige samenwerkingsverbanden en loyaliteit een belangrijk gegeven. In online criminele samenwerkingsverbanden zien we dit niet terug. Vaak zijn deze samenwerkingsverbanden gebouwd op *thin trust*; banden die niet zozeer gebaseerd zijn op sterke of zwakke interpersoonlijke relaties, maar op de reputatie of veronderstelde kwaliteiten van personen, die unieke toegang geven tot middelen en kansen die in de directe sociale kring niet aanwezig zijn (Khodayakov 2007). Terwijl sterke vertrouwensbanden typerend zijn voor de samenwerking binnen een criminele groep, is *thin trust* typerend voor virtuele samenwerking en voor samenwerking met experts die niet beschikbaar zijn in de eigen kring.

In de bestudeerde bestanden komen we zowel voorbeelden tegen van sterke samenwerkingsrelaties, gebaseerd op vertrouwen, loyaliteit en controle door middel van macht en geweld, als voorbeelden van losse, meer 'projectmatige' samenwerkingsrelaties, waarin vertrouwen een heel andere rol speelt. Partners worden in dat geval geselecteerd op grond van prestige en reputatie, die niet alleen gebaseerd zijn op kennis, kunde en eerdere prestaties, maar ook op de mate waarin men zich volgens de referenten aan afspraken houdt. Een goede reputatie wordt opgebouwd met recensies op het internet en met feedback over de geleverde diensten.

Door de anonimiteit van het internet kunnen subjecten op het internet met elkaar samenwerken en vertrouwelijke zaken met elkaar delen. Dit betekent echter niet dat zij elkaar ook in de offline wereld zouden vertrouwen. De anonimiteit van het internet biedt hun bescherming. Deze anonimiteit van het internet heeft echter ook gevolgen voor de wijze waarop mensen elkaars handelingen kunnen controleren, en voor de wijze waarop afspraken kunnen worden afgedwongen. Controle door middel van macht en geweld maakt plaats voor recensies en indien nodig ook cyberaanvallen. Zo hebben we in de dossiers gevallen gezien van verdachten die elkaar bestookten met DDoS-aanvallen.

*Ketenstructuur*

In een deel van de door ons bestudeerde cyberzaken wordt de samenwerking tussen verdachten gekenmerkt door een ketenstructuur. Met

doi: 10.5553/JV/016758502018044005002

name in de lossere netwerken krijgt de samenwerking tussen verdachten de vorm van een ketensamenwerking. Binnen zo'n keten zijn verschillende verdachten betrokken bij verschillende activiteiten, die pas na samenvoeging een strafbaar feit opleveren. In deze ketenstructuren werken verdachten wel met elkaar samen, maar zijn zij slechts verantwoordelijk voor een kleiner onderdeel van de gehele criminele activiteit. Als gevolg hiervan kunnen verdachten betrokken zijn bij georganiseerde criminaliteit, zonder precies te weten van welke misdaden hun activiteiten onderdeel uitmaken. Er kan zelfs ruime tijd zitten tussen de geleverde dienst en het uiteindelijke delict. Een voorbeeld hiervan is software die iemand geschreven heeft en te koop heeft aangeboden. Tussen de verkoop en de daadwerkelijke inzet kan langere tijd zitten.

Binnen deze ketenstructuren heeft elke verdachte in zekere zin macht, en heeft elke verdachte een bepaalde rol, maar tegelijkertijd lijkt iedereen of juist niemand verantwoordelijk te zijn voor de misdaad als geheel. Hierdoor is sprake van fragmentatie van het delict. Dit lijkt een nieuw kenmerk van georganiseerde cybercriminaliteit, en zou een verandering kunnen betekenen voor de inhoud van het concept georganiseerde criminaliteit.

In zo'n ketenstructuur kunnen de verschillende spelers voor zichzelf bezig zijn en individuele doelen hebben. Samen bereiken ze een georganiseerde vorm van criminaliteit, die niet zozeer van bovenaf georganiseerd is, maar veeleer vanuit een bottom-up proces is ontstaan. Op deze manier lijken zowel de criminele activiteiten als de groepen van samenwerkende personen min of meer op toevallige wijze te ontstaan en bepaalde vormen aan te nemen.

Deze ontwikkelingen maken dat georganiseerde cybercrime niet alleen kan worden gepleegd op basis van onderlinge afspraken tussen verdachten die elkaar kennen en samenwerken aan een bepaald project, op basis van een bepaalde verdeling van taken, maar ook in de vorm van de hierboven geschetste ketenstructuur, zonder duidelijke coördinatie. Er bestaat daarmee een diversiteit aan vormen, waardoor het moeilijk kan zijn om na te gaan wie wel en niet tot een criminele groep behoren en om criminaliteit aan specifieke criminele groepen of organisaties toe te schrijven. Ook wordt het daardoor moeilijk om te voorspellen hoe criminaliteitsvormen zich ontwikkelen.

doi: 10.5553/JV/016758502018044005002

*Anonimiteit*

Het internet biedt mogelijkheden om volledig anoniem te acteren. Uit de bestudeerde dossiers blijkt dat verdachten de identiteit van hun medeplegers daardoor niet altijd kennen. Dat geldt vooral voor de *cyber-dependent* zaken. Een verdachte van grootschalige DDoS-aanvallen was bijvoorbeeld zeer verbaasd dat zijn medepleger een 16-jarige jongen bleek te zijn. Ook tijdens verhoren verklaarden verdachten dat ze online contacten hadden, informatie uitwisselden en diensten kochten van personen die zij nooit persoonlijk hadden ontmoet. Dit geldt niet alleen voor kleine flexibele gelegenheidssamenwerkingsverbanden, maar ook voor groepen die langer bestaan en wel enigszins werken in een hiërarchische structuur. Bij *cyber-enabled crime* is er vaak sprake van een vermenging van ICT en traditionele georganiseerde misdaad. Dit brengt met zich mee dat daders van deze misdrijven elkaar vaak wel kennen en elkaar ook offline ontmoeten (Kruisbergen e.a. 2018). Echter, ook bij dit soort misdrijven hebben verdachten online contacten en wordt er ook samengewerkt met personen die ze niet kennen en met wie het nooit tot een fysieke ontmoeting komt. Een pakkend voorbeeld is een verdachte die samen met enkele bekenden een marktplaats wilde bouwen, nadat de website op het darkweb, waarvan hij medebeheerder was, door de eigenaar op non-actief was gesteld. De verdachte verklaarde dat hij deze eigenaar nog nooit had ontmoet en dat communicatie enkel via fora en via de mail verliep. De identiteit van de eigenaar van deze darkweb-marktplaats is nooit in beeld gekomen en het opsporingsteam veronderstelde dat hij zich in het buitenland bevond.

De inbedding van individuele anonieme verdachten in een keten van samenwerkende daders maakt het opsporen van complexe cybercriminaliteit niet eenvoudig. Het in kaart brengen van een samenwerkingsverband wordt verder bemoeilijkt doordat informatie over criminele activiteiten en over de daders gefragmenteerd is. Zoals eerder opgemerkt, speelt de loyaliteit van individuele leden naar een groep geen grote rol op internet en online samenwerkingsverbanden duren soms maar kort. Met het ontmantelen of uitschakelen van een individuele schakel loopt het voortbestaan van de ketenstructuur geen enkel gevaar. In de wereldwijde pool die het internet biedt, is snel doorschakelen mogelijk, hetgeen kenmerkend is voor deze online samenwerkingsverbanden.

doi: 10.5553/JV/016758502018044005002

Het is echter niet ondenkbaar dat bepaalde schakels essentieel zijn voor één of meer samenwerkingsverbanden. Dit zou met name kunnen gelden voor individuen die hoog in aanzien staan of over zeer schaarse kennis beschikken. In de bestudeerde casussen zijn we hiervan overigens geen voorbeelden tegengekomen. Focussen op zo'n specifieke schakel zou lonend kunnen zijn bij het verstoren van de activiteiten van misdaadgroepen. Tegelijkertijd is dit waarschijnlijk ook bijzonder moeilijk, omdat het gaat om individuen die zeer kundig zijn in datgene wat zij doen en daardoor mogelijk ongrijpbaar blijven.

## Ten slotte

Door technologische ontwikkelingen die het mogelijk maken om steeds gemakkelijker anoniem op het internet te acteren vormt de aanpak van georganiseerde cybercrime een steeds groter probleem. Niet alleen omdat daders, bewijsmateriaal, opbrengsten en slachtoffers van georganiseerde cyberdelicten nog ongrijpbaarder worden dan ze al waren, maar vooral ook door de wijze waarop er op internet in de vorm van ketensamenwerking lijkt te worden geopereerd. Wanneer verschillende samenhangende stappen door verschillende mensen in een ketensamenwerking worden gezet, wordt het moeilijk om de aard van een misdrijf te begrijpen, om te zien hoe het misdrijf ontstaat, om de verdachten te identificeren die verantwoordelijk zijn voor stappen of voor het grotere geheel, en om het misdrijf met traditionele middelen op te sporen. De nieuwe Wet computercriminaliteit III,[7] die binnenkort in Nederland in werking treedt, zal de Nederlandse politie nieuwe onderzoeksinstrumenten bieden. Zo biedt deze wet de mogelijkheid om de toegang te krijgen tot systemen en data voordat deze versleuteld zijn. De toekomst zal uitwijzen of de verruimde opsporingsmogelijkheden de gewenste oplossingen kunnen bieden.
Omdat een verdachte op het internet zich overal ter wereld kan bevinden, vergt het identificeren, lokaliseren, aanhouden, vervolgen en uiteindelijk berechten van verdachten vooral een intensieve internationale samenwerking. Om internationaal samen te kunnen werken hebben opsporingsinstanties nog steeds rechtshulpverzoeken nodig om de benodigde informatie of het benodigde bewijsmateriaal te

7 Besluit Wet computercriminaliteit III, *Kamerstukken* I 2017/18, 34372, https://www.eerstekamer.nl/wetsvoorstel/34372_computercriminaliteit_iii.

doi: 10.5553/JV/016758502018044005002

kunnen verkrijgen. Ons onderzoek liet zien dat deze verzoeken door lokale prioriteiten, ingewikkeld papierwerk en omslachtige procedures vaak worden behandeld met een tempo dat onverenigbaar is met de snelheid van het internet. Daarbij ontstaat dan tevens de vraag wáár de verdachte berecht moet worden, omdat een misdaad op internet niet altijd een fysieke locatie heeft. Overheden zullen daarom actief en creatief moeten nadenken over nieuwe manieren om deze moeilijk grijpbare vormen van criminaliteit te kunnen bestrijden. Begrijpen hoe georganiseerde cybercrime in elkaar zit en zich ontwikkelt, is een noodzakelijke eerste stap. We hopen dat het gezamenlijke onderzoeksrapport, geschreven door onderzoekers uit drie Europese landen, bijdraagt aan dit doel.

## Literatuur

**BKA, WODC & BRA 2016**
BKA, WODC & BRA, *Cyber-OC – Scope and manifestations in selected EU member states* (HOME/2012/ISEC/AG/4000004382). Polizei + Forschung 2016, 50

**Van de Bunt & Kleemans 2007**
H.G. van de Bunt & E.R. Kleemans, m.m.v. C.J. de Poot, R.J. Bokhorst, M. Huikeshoven, R.F. Kouwenberg, M. van Nassou & R. Staring, *Georganiseerde criminaliteit in Nederland. Derde rapportage op basis van de Monitor Georganiseerde Criminaliteit*, Den Haag: Boom Juridische uitgevers 2007.

**Khodayakov 2007**
D. Khodayakov, 'Trust as a process: A three-dimensional approach', *Sociology* (41) 2007, p. 115-132.

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

**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*, Den Haag: WODC 2002.

doi: 10.5553/JV/016758502018044005002

**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*, Den Haag: Boom Lemma 2012.

**Kruisbergen e.a. 2018**
E.W. Kruisbergen, E.R. Leukfeldt, E.R. Kleemans & R.A. Roks, *Georganiseerde criminaliteit en ICT. Vijfde ronde Monitor Georganiseerde Criminaliteit* (Cahier 2018-8), Den Haag: WODC 2018.

**Martin 2013**
J. Martin, 'Lost on the Silk Road: Online drug distribution and the "cryptomarket"', *Criminology and Criminal Justice* (14) 2013, afl. 3, 351-367, https://doi.org/10.1177/1748895813505234.

**Odinot e.a. 2017**
G. Odinot, M.A. Verhoeven, R.L.D. Pool & C.J. de Poot, *Organised cyber-crime in the Netherlands. Empirical findings and implications for law enforcement* (Cahier 2017-1), Den Haag: Boom juridisch 2017.

**Oerlemans e.a. 2016**
J.J. Oerlemans, B.H.M. Custers, R.L.D. Pool & R. Cornelisse, *Cybercrime en witwassen* (O&B 319), Den Haag: WODC 2016.

**Soudijn & Monsma 2012**
M.R.J. Soudijn & E. Monsma, 'Virtuele ontmoetingsruimtes voor cybercriminelen', *Tijdschrift voor Criminologie* (54) 2012, afl. 4, p. 349-360.

**Wall 2007**
D.S. Wall, *The transformation of crime in the information age*, Cambridge: Polity Press 2007.

**Wall 2014**
D.S. Wall, '"High risk" cybercrime is really a mixed bag of threats', 2014, https://theconversation.com/high-risk-cyber-crime-is-really-a-mixed-bag-of-threats-34091.

**Wall & Williams 2014**
D.S. Wall & M.L. Williams, *Policing cybercrime. Networked and social media technologies and the challenges for policing*, Oxon, VK: Routledge 2014.

doi: 10.5553/JV/016758502018044005002