Opsporen, vervolgen en tegenhouden van cybercriminaliteit

van den Eeden, C.A.J.; van Berkel, Jasper J.; Lankhaar, C.C.; de Poot, Christianne

published in
Het Tijdschrift voor de Politie
2022

document version
Publisher's PDF, also known as Version of record

OPSPOREN, VERVOLGEN EN TEGENHOUDEN VAN CYBERCRIMINALITEIT

OVER SLIMMERE OMGANG MET INFORMATIE EN OVER DE ROL VAN POLITIE EN OM

Nederland heeft een snelle, stabiele en betrouwbare digitale infrastructuur, waar zowel nationaal als internationaal veelvuldig gebruik van wordt gemaakt. Als gevolg hiervan voltrekken zich ook illegale activiteiten op Nederlandse servers of worden deze (on)bewust gefaciliteerd door in Nederland gevestigde *hosters*. Bij cybercriminaliteit is het opsporen van verdachten ingewikkeld. Daders kunnen anoniem opereren en zijn goed in staat hun identiteit en locatie af te schermen. Daardoor lukt het lang niet in alle zaken om daders te identificeren en te vervolgen. De aanpak van cybercriminaliteit is daarom niet alleen gericht op opsporing en vervolging, maar ook op het verstoren en tegenhouden van deze vormen van criminaliteit.

Tekst: Claire van den Eeden, Jasper van Berkel & Christianne de Poot • Foto: Meesters Multi Media

Dit artikel is een verkorte en vereenvoudigde weergave van het WODC-rapport: Eeden, van den, C.A.J., Van Berkel, J.J., Lankhaar, C.C., & De Poot, C.J. (2021). *Opsporen, vervolgen en tegenhouden van cybercriminaliteit.* Den Haag: WODC. Cahier 2021-23.

Hoewel het in theorie mogelijk is dat een onderzoek van Team High Tech Crime (THTC) start op basis van een aangifte, laat de praktijk zien dat van deze vormen van *hightechcrime* waar THTC zich op richt zelden aangifte wordt gedaan. Dat was ook terug te zien in de dossiers die wij bekeken en sluit aan op bevindingen uit eerder WODC-onderzoek (Odinot et. al., 2017). Voor de opsporingsonderzoeken naar cybercrime die in de regionale eenheden worden gestart, ligt dit anders. Het enige geselecteerde opsporingsdossier uit ons onderzoek dat is gestart naar aanleiding van een aangifte, was een *phishing*-zaak die werd onderzocht door een regionale eenheid. Van de zeven bestudeerde THTC-onderzoeken zijn zes onderzoeken gestart naar aanleiding van een tip van een private partij en/of buitenlandse politiedienst.

Opsporingsmiddelen en -methoden

In de dossiers zagen we terug dat de start van opsporingsonderzoeken vaak digitaal verliep. Bijvoorbeeld door middel van het vorderen en

Hoe zijn we te werk gegaan?
De focus van ons onderzoek lag op complexe zaken, het type zaken dat voornamelijk door Team High Tech Crime (THTC) van de Landelijke Eenheid wordt opgepakt. Ten eerste hebben we literatuuronderzoek uitgevoerd naar de opsporingspraktijk van cybercriminaliteit. Ten tweede hebben we politiedossiers bestudeerd van acht afgeronde opsporingsonderzoeken. Die zaken werden aangedragen door een groep experts. Het ging om onderzoeken waarin de opsporing in enige mate succesvol was en/of waarin sprake was van aspecten die in eerder onderzoek als knelpunt waren geïdentificeerd, zodat we konden nagaan hoe daarmee werd omgegaan. Ten derde hebben we drie publiek-private samenwerkingsprojecten nader bekeken, omdat publiek-private samenwerking (PPS) als een wezenlijk onderdeel van de integrale aanpak van cybercriminaliteit wordt beschouwd. Tot slot hebben we interviews afgenomen met mensen werkzaam in de (opsporings)praktijk. Dat waren zowel algemene interviews als zaakspecifieke interviews. De algemene interviews waren bedoeld om een globaal beeld te krijgen van de aanpak van cybercriminaliteit. De zaakspecifieke interviews om zicht te krijgen op afwegingen die tijdens concrete opsporingsonderzoeken speelden maar niet in het dossier terecht zijn gekomen.

veiligstellen van servergegevens en IP-taps. De informatie die hiermee werd opgedaan, kon worden gebruikt om de verdere richting van een opsporingsonderzoek te bepalen. Hierbij moet worden opgemerkt dat de inzet van deze middelen niet bij elk onderzoek evenveel informatie opleverde. Naast het verschil in hoeveelheid en typen gegevens die op servers stonden, speelt ook de mate van versleuteling van data een rol bij het bepalen van de bruikbaarheid van de gegevens. Onderzoeken verschoven vaak van digitaal naar meer 'traditioneel' wanneer een verdachte in beeld kwam. Dan werden middelen als telefoontaps ingezet en in veel gevallen werd ook financieel onderzoek gedaan.

> De aanpak is ook gericht op het **verstoren** en **tegenhouden** van **cybercriminaliteit**

Daarnaast werd in de opsporingsonderzoeken gebruik gemaakt van undercover bevoegdheden. In vijf van de acht bestudeerde onderzoeken kwamen Nederlandse verdachten in beeld. In alle vijf deze onderzoeken is gebruikgemaakt van bevoegdheden die vallen onder werken onder dekmantel. Deze bevoegdheden werden zowel *online* als *offline* ingezet. Dit is opvallend, gezien het geringe aantal *offline* zaken waarin deze bijzondere opsporingsbevoegdheden normaliter worden ingezet (Kruisbergen & De Jong, 2010), maar sluit wel aan bij bevindingen uit eerder onderzoek naar de opsporing van georganiseerde vormen van cybercriminaliteit door Odinot et al. (2017). Dat kan te maken hebben met de ernst van de bestudeerde zaken. Een andere verklaring kan zijn dat bij de aanpak van dit soort nieuwe vormen van cybercriminaliteit – waarbij traditionele opsporingsstrategieën niet altijd toereikend zijn – ook nieuwe gedachtenvorming plaatsvindt over de inzet en zwaarte van de bestaande opsporingsbevoegdheden.

Beperkte mogelijkheden voor vervolging

Eén respondent merkte op dat je als cybercrime-onderzoeker 'onderdeel van de wereldpolitie' bent. Bij de start van een onderzoek is vaak niet bekend uit welk land een aanval of verdachte afkomstig is. Een deel van de opsporingstaak kan dan ook zijn om met de informatie die naar voren komt uit een onderzoek naar de in Nederland gebruikte infrastructuur, een ander land in stelling te brengen om over te kunnen gaan tot

Over de auteurs
Dr. **Claire van den Eeden** is werkzaam aan het Wetenschappelijk Onderzoek- en documentatiecentrum (WODC) te Den Haag.
Jasper van Berkel, LLM is verbonden aan het Wetenschappelijk Onderzoek- en documentatiecentrum (WODC) te Den Haag.
Prof. dr. **Christianne de Poot** is werkzaam aan de Vrije Universiteit Amsterdam, de Hogeschool van Amsterdam en de Politieacademie.

De **politie** heeft **geen bevoegdheid** om opsporingsmiddelen in te zetten puur ten behoeve van het **verkrijgen** van een betere **informatiebehoefte**

vervolging. Dat kan bijvoorbeeld het land zijn waarin de verdachte woont, of een land waarin slachtoffers zijn gemaakt en dat betere kaarten heeft om over te kunnen gaan tot uitlevering of vervolging. Ook kan het zijn dat de criminele actor een zekere bescherming geniet van een statelijke actor, wat vervolging eveneens lastig maakt.

Een ander probleem doet zich voor wanneer een opsporingsonderzoek eigenlijk te veel verdachten oplevert. Bij de aanpak van illegale dienstverleners – zoals het verhuren van *botnets* voor DDoS-aanvallen – kan de identiteit van een grote groep afnemers (klanten) naar voren komen. Er is dan niet altijd capaciteit om alle verdachten te vervolgen en daarnaast is het de vraag of vervolging in deze gevallen altijd de meest effectieve maatregel is. In deze casuïstiek betreft het regelmatig jonge daders die zich niet altijd bewust zijn van de impact of de strafbaarheid van hun acties, ook al werden door hun handelingen veel mensen gedupeerd. Hoewel met name de onderzoeken naar *high-tech* cybercriminaliteit niet altijd leiden tot vervolgbare verdachten, kan de strafrechtelijke aanpak voor deze moeilijk vervolgbare delicten wel degelijk van meerwaarde zijn. Als interventies zich alleen op de verstoring van de infrastructuur zouden richten, heeft dit kortdurend effect, omdat nieuwe infrastructuren ontstaan en activiteiten elders worden voortgezet (Ladegaard, 2019). Het is daarom juist van belang om een opsporingsonderzoek op te blijven zetten dat erop gericht is om een verdachte te identificeren en vervolgen, ook als signaalfunctie. Verder leverden de onderzoeken naar *facilitators* in een aantal gevallen geen hoofdverdachte op, maar wel informatie over andere vormen van criminaliteit die vervolgens in andere opsporingsonderzoeken kon worden gebruikt.

Tegenhoudmaatregelen en informatiepositie

Een opsporingsonderzoek kan officieel alleen worden gestart als er opsporingsindicatie is, omdat alleen dan opsporingsbevoegdheden mogen worden ingezet. Lang niet alle onderzoeken naar cybercriminaliteit leiden echter tot een verdachte. Soms is dat al snel bij aanvang van een opsporingsonderzoek duidelijk en dan wordt nagedacht of er met de verkregen informatie ook andere doelen bereikt kunnen worden. Andere doelen dan opsporen en vervolgen kunnen bijvoorbeeld zijn: meer zicht krijgen op (vaker gebruikte) modus operandi en op de gebruikte infrastructuur, om met die kennis vervolgens verstoringsacties of preventiecampagnes op te zetten.

Het samenspel tussen opsporen en tegenhouden is van belang omdat kennis uit de opsporingsonderzoeken gebruikt kan worden om inzicht te krijgen in nieuwe vormen van cybercriminaliteit en de daarbij gebruikte modus operandi, en om eerder vergaarde kennis up-to-date te houden. Met alleen tegenhoudmaatregelen blijft slechts een klein deel van het proces zichtbaar, terwijl met een aanhouding of inbeslagname het hele criminele proces gereconstrueerd kan worden.

Voor een gerichte inzet van tegenhoudmaatregelen is een goede informatiepositie nodig. Om haar informatiepositie te vergroten en meer proactief te kunnen handelen volgen politie en OM de actuele ontwikkelingen binnen de cybercriminaliteit. Dit wordt, waar mogelijk, gedaan door data uit eerdere opsporingsonderzoeken te bundelen en contacten te leggen met andere nationale opsporingsdiensten en internationale politiediensten, maar ook door kennis te nemen van de verschillende dreigingsrapporten die periodiek verschijnen en door het aangaan van publiek-private samenwerking.

Aan deze vormen van samenwerking, informatievergaring en informatiedeling kleven echter wat juridische haken en ogen. Zo mag informatie die rechtmatig is verzameld ten behoeve van eerdere opsporingsonderzoeken niet zonder meer gebruikt worden in nieuwe onderzoeken of gedeeld worden met andere partijen. Daarnaast heeft de politie, in tegenstelling

tot inlichtingen- en veiligheidsdiensten, geen bevoegdheid om opsporingsmiddelen in te zetten puur ten behoeve van het verkrijgen van een betere informatiepositie. Een goede informatiepositie is erg belangrijk voor de opsporing, maar kunnen politie en OM formeel alleen creëren door het uitvoeren van opsporingsonderzoeken – met als doel een verdachte op te sporen en te vervolgen. Dat kan problematisch zijn wanneer bij de start van een onderzoek al snel duidelijk is dat er geen dader geïdentificeerd zal kunnen worden, terwijl de maatschappelijke impact van een cyberdelict wel erg groot is. Bijvoorbeeld bij een grootschalige hack. Een belangrijk doel van het onderzoek wordt dan de inzet van tegenhoudmaatregelen, omdat dit het meest effectieve bestrijdingsmiddel is. Desalniettemin kunnen de benodigde bevoegdheden niet enkel voor dat doel worden ingezet en wordt verwezen naar de mogelijkheid – hoe klein die ook is – dat een verdachte wordt geïdentificeerd en strafrechtelijk kan worden vervolgd.

Samenvatting en conclusie

Ons onderzoek laat zien dat het steeds belangrijker wordt om (cyber)criminele fenomenen te begrijpen om zo effectief en efficiënt mogelijk te kunnen ingrijpen. Als het opsporen en vervolgen van daders het uitgangspunt is, dan is het inzetten van opsporingsmiddelen geen probleem. In de praktijk is opsporen en vervolgen van daders echter niet altijd haalbaar en wordt er daarom regelmatig voor gekozen om tegenhoudmaatregelen in te zetten, ook al is daar eigenlijk formeel geen juridische grond voor. Dat roept de vraag op of de huidige wettelijke kaders rond de inzet van opsporingsmiddelen toereikend zijn.

Op voorhand is niet altijd duidelijk welke informatie in een opsporingsonderzoek kan worden vergaard, en in hoeverre opsporing en vervolging tot de mogelijkheden behoort. Maar het is ook niet altijd duidelijk wat de juridische grondslag is voor de meer informatievergarende manier van onderzoek doen zoals dat gebeurt bij de aanpak van cybercriminaliteit. Dat roept verder de vraag op of de fundamentele taak van politie en het OM zoals die nu is geformuleerd toereikend is en of de huidige juridische grondslagen voor het verzamelen, verwerken en analyseren van informatie afdoende zijn voor de beoogde integrale aanpak van cybercriminaliteit.

De bevindingen uit het onderzoek vragen daarom om een bredere discussie over slimme omgang met informatie en over de rol van politie en OM bij de aanpak van cybercriminaliteit. De bevindingen uit ons onderzoek werpen tot slot de vraag op of de huidige wet- en regelgeving rond informatiedeling toereikend is voor de aanpak van cybercriminaliteit. Er lijkt behoefte te zijn aan duidelijkere kaders op basis waarvan informatie kan worden gedeeld tussen de verschillende partijen die betrokken zijn bij de aanpak van cybercriminaliteit, zodat, als er urgentie is, belangrijke informatie ook snel kan worden gedeeld.

> Het is van **belang** om een opsporingsonderzoek op te zetten dat **gericht** is om een verdachte te **identificeren** en **vervolgen**

Literatuur

- Kruisbergen, E.W. & Jong, D. de (2010) *Opsporen onder dekmantel. Regulering, uitvoering en de resultaten van undercovertrajecten.* Den Haag: Boom.
- Ladegaard, I. (2019). Crime displacement in digital drug markets. *International Journal of Drug Policy.*
- Odinot, G., Verhoeven, M.A., Pool, R.L.D., & Poot, C.J. de. (2017). *Organised cybercrime in the Netherlands: Emperical findings and implications for law enforcement.* Den Haag: WODC.
- Van de Sandt, E., Van Bunningen, A., Lenthe, J. van, & Fokker, J. (2021). *Towards data scientific investigations: A comprehensive data science framework and case study for investigating organized crime and serving the public interest.* Rephrain.