Politieoptreden op het dark web

Author(s)
Emmen, Bram; de Poot, Christianne; Stol, Wouter

Publication date
2023

Document Version
Final published version

Published in
Het Tijdschrift voor de Politie

HET TIJDSCHRIFT VOOR DE
Politie
ONAFHANKELIJK OPINIEBLAD • NUMMER 2 • 2023 • WEBSITEVOORDEPOLITIE.NL

ONDERZOEKER WOUTER LANDMAN
OSINT: online vergaren van gegevens
→ pagina 10

INTERVENTIESPECIALIST NICOLE MULDER
Voorkomen en doorbreken van cybercriminele carrières
→ pagina 26

Policing the Internet

DE POLITIE IN EEN DIGITALE SAMENLEVING

Gompel&Svacina

Foto: stockphotosecrets.com

22

Nieuwe kennis en vaardigheden in het politiewerk

Melvin Soudijn en Marc Schuilenburg gingen op zoek naar een antwoord op de vraag welke nieuwe kennis en vaardigheden nodig zijn als de politie wil meebewegen in een gedigitaliseerde samenleving.

Foto: Pexels/Lukas

26

Preventie

Nicole Mulder en Maurice van der Stoel presenteren een innovatieve manier om jongeren te behoeden voor online criminaliteit.

En verder

Columns

En meer ...

Vaste rubrieken

Verder lezen op de website

Advertenties
Irene Schaddelee-Pesch
+31 (0)6 23700323
info@is-acquisitie.com

Abonnementen
Het Tijdschrift voor de Politie verschijnt vier keer per jaar en is gratis voor politiemensen. Overheid/instelling/zakelijk: €179,- Privépersoon: €89,50

Abonnementen lopen per kalenderjaar en worden automatisch verlengd, tenzij uiterlijk 30 dagen voor de vervaldatum bij onze abonneeservice wordt opgezegd.

Abonneren kan via www.website voordepolitie.nl of via onze abonneeservice.

Gompel&Svacina Abonneeservice
Postbus 105
2400 AC Alphen aan den Rijn
Tel. NL: 0031 (0)172476085
Tel. BE: 0032 (0)25888745
E-mail: TVP@spabonneeservice.nl

Gompel&Svacina

Politieoptreden op het dark web

Online criminaliteit stelt de politie voor nieuwe vraagstukken. Zo kunnen daders op het internet met Anonieme Communicatie Netwerken (ACN's) acteren zonder daarbij hun identiteit of locatie prijs te geven. Op die manier kunnen ze bijvoorbeeld illegale goederen verhandelen, kinderporno verspreiden of geld witwassen, terwijl ze zelf buiten beeld blijven. Hoe gaat de (Nederlandse) politie om met deze uitdaging? Dat was de hoofdvraag van het door NordForsk gefinancierde onderzoeksproject *Police detectives on the Tor network*.

Over de auteurs
Drs. **Bram Emmen** is criminoloog en PhD-onderzoeker aan de Open Universiteit binnen het PDTOR-project (contact bram.emmen@ou.nl).
Prof. dr. **Christianne de Poot** is hoogleraar Criminalistiek aan de Vrije Universiteit en lector Forensisch Onderzoek aan de Politieacademie en de Hogeschool van Amsterdam.
Prof. dr. **Wouter Stol** is hoogleraar Politiestudies aan de Open Universiteit en lector Cybersafety aan de Politieacademie en NHL StendenHogeschool.

Tekst: Bram Emmen, Christianne de Poot & Wouter Stol • Foto: Pexels/Lukas

Een van de bekendste ACN's is het Tor-netwerk. Tor is een programma dat gebaseerd is op verschillende lagen van encryptie, waardoor het voor anderen vrijwel onmogelijk is om te detecteren vanaf welk apparaat (welk IP-adres) de communicatie plaatsvindt. Daardoor blijven degenen die via dit netwerk opereren zolang zij zelf hun identiteit of verblijfplaats niet prijsgeven, onbekend en onvindbaar (Dordal, 2018). Het gebruiken van Tor is legaal. Zo wordt het gebruikt door journalisten en dissidenten in onderdrukkende regimes, die dankzij dit netwerk vrij kunnen communiceren. Het wordt echter ook gebruikt door daders die zo hun illegale praktijken afschermen en anoniem samenwerken. Wij bestudeerden welke strategieën en werkwijzen de politie hanteert bij de aanpak van misdrijven die met behulp van het Tor-netwerk worden gepleegd en of dat anders is dan wat de politie bij offline criminaliteit gewend was te doen.
We hielden oriënterende gesprekken met sleutelpersonen van de politie die ervaring hadden met de aanpak van dit soort misdrijven, deden media-analyse om te onderzoeken wat er de afgelopen jaren over de aanpak van 'Tor-zaken' in de media was gerapporteerd en we voerden na onze eerste bevindingen een tweede serie verdiepende gesprekken met sleutelpersonen van politie en OM. Naast medewerkers van het Team High Tech Crime (THTC), het Team ter Bestrijding van Kinderpornografie en Kindersekstoerisme (TBKK) en het voormalige Team Darkweb, bleken ook gewone rechercheurs in de eenheden met Tor-zaken in aanraking te komen. Daarom selecteerden we de sleutelpersonen voor de gesprekken onder andere bij twee avondworkshops over het TOR-netwerk op de Politieacademie, die door de eerste auteur van dit artikel werden gegeven en waarbij deelnemers uit alle eenheden aanwezig waren. In deze bijdrage richten we ons op de belangrijkste onderzoeksbevindingen.

Drie strategieën

De politie hanteert drie strategieën tegen criminaliteit op het Tor-netwerk:
1. opsporing van daders,
2. hulpverlening aan slachtoffers,
3. preventie.

Deze kunnen niet los van elkaar worden gezien. Zo gaat opsporing vaak hand in hand met hulpverlening en heeft het feit dat de politie actief is op het Tor-netwerk mogelijk een preventieve werking. Wat strategieën betreft dus niets nieuws. De veranderingen zitten vooral in de werkwijzen waarmee de politie deze drie strategieën inhoud geeft.

Opsporing

Bij ernstigere misdrijven is opsporing van verdachten de voorkeursstrategie. De strafbare handelingen zijn in veel gevallen eenvoudig online waar te nemen (seksueel kindermisbruik is daarop een uitzondering), maar wie zit er achter? Om daders te kunnen vervolgen moeten hun goed verborgen echte identiteit en/of locatie worden achterhaald. Niet zelden heeft een dader wel een online identiteit (*online ID*) die als aanknopingspunt kan dienen. Ontdekt de politie de échte identiteit (*real ID*), dan richt de opsporing zich vervolgens op het lokaliseren van die persoon. Is er een locatie in beeld gekomen, dan richt de opsporing zich op het identificeren van de persoon die zich op die locatie bevindt, of op het aanhouden van die persoon en daarna de identificatie. Hiervoor wordt vaak langdurig gerechercheerd en worden vaak bijzondere opsporingsbevoegdheden ingezet.

Om de identiteit en/of locatie van de verdachten vast te stellen zoeken politiemedewerkers ten eerste naar fouten in hun operationele beveiliging (zie ook Dordal, 2018). De meeste verdachten zijn wel zo slim dat ze op Tor niet hun werkelijke naam gebruiken, maar soms kunnen hun handelingen hun locatie onthullen. In één zaak waarover politiemensen vertelden, bevatte een cryptomarkt encryptiefouten, waardoor IP-adressen van de server lekten en de werkelijke locatie van die server aan het licht kwam. Ook waren er voorbeelden van aankopen met bitcoin die locatiegegevens bevatten, zoals een opgegeven afleveradres. Met iets eenvoudigs als het bestellen van een pizza kunnen verdachten soms per abuis hun locatie-informatie onthullen. Deze fouten vinden niet alleen online plaats, maar ook in het fysieke domein. Bij het verzenden van goederen via postpakketten kan in sommige gevallen de verzendlocatie worden getraceerd, en als CCTV-informatie kan worden opgevraagd, kan daarmee soms een anonieme verzender worden geïdentificeerd (zie hierover ook Davies, 2020).

Ten tweede maakt de politie gebruik van undercoveroperaties om ID- of locatie-informatie te verkrijgen. De overname van de Hansa-markt, waarbij onder andere veel leveringsadressen voor drugs werden verkregen, is daarvan misschien wel het bekendste voorbeeld. Uit de interviews kwam naar voren dat er in strafrechtelijke onderzoeken naar Tor-zaken relatief vaak online en offline undercoverbevoegdheden worden ingezet, zoals pseudokoop en infiltratie om anonieme handelaren te identificeren. Dit lijkt kenmerkend voor onderzoeken naar Tor-zaken en is in lijn met bevindingen uit eerdere (Nederlandse) onderzoeken naar georganiseerde cybercrime en de aanpak daarvan (Jeffries & Apeh, 2020; Odinot et al., 2018; C. A. J. van den Eeden et al., 2021).

> Politiemedewerkers zoeken **eerst** naar **fouten** in de operationele **beveiliging** van **verdachten**

Hulpverlening

Respondenten die betrokken zijn bij de bestrijding van kindermisbruik, vertellen dat ze in deze zaken niet alleen gericht zijn op het identificeren van daders, maar vooral op het verminderen van (de impact van) deze criminaliteit door de slachtoffers uit handen van de daders te krijgen. Dat gebeurt in het kader van de hulpverleningstaak (artikel 3 Politiewet). Daarom probeert het TBKK anonieme minderjarige slachtoffers te vinden en een einde te maken aan het herhaalde slachtofferschap. Vaak zijn opsporing en hulpverlening verweven. Door zicht te krijgen op de slachtoffers kunnen verdachten in beeld komen, en door zicht te krijgen op verdachten kunnen slachtoffers worden geïdentificeerd. Politiemensen zien het beschermen van de slachtoffers in deze zaken als het primaire doel van hun handelen. Ook bij een mensenhandelzaak wordt hulp aan de slachtoffers genoemd als primair doel. Daders proberen in deze zaken de identiteit van hun slachtoffers te verbergen, om te voorkomen dat zij via de slachtoffers in beeld komen. In kindermisbruikzaken is er vaak beeldmateriaal waarop slachtoffers in beeld zijn, en waarop soms locatie-informatie kan worden ontdekt in de vorm van een specifiek stuk speelgoed of een stopcontact waaruit de plaats (land) van het misbruik kan worden afgeleid.

Verstoring van de infrastructuur en **ondermijning** van het vertrouwen krijgen een **duidelijke** plek

Preventie

Preventie omvat gedragsbeïnvloeding en verstoring. Gedragsbeïnvloeding kan zich richten op potentiële slachtoffers (voorlichting) en op potentiële daders (afschrikking). Verstoring kan zijn gericht op de criminele infrastructuur (*infrastructure policing,* Collier et al., 2022) en op het ondermijnen van het vertrouwen tussen de bij de criminaliteit betrokken personen (bv. daders onderling, daders en facilitators, en daders en potentiële slachtoffers).

De *take down* van de website 'deepdotweb' in mei 2019 kan gezien worden als een verstoring van de infrastructuur. Deze verstoring maakte het (tijdelijk) moeilijker om cryptomarkten te vinden. Een voorbeeld van een werkwijze die het vertrouwen in Tor of tussen Tor-gebruikers ondermijnt, is de onionsite DisrupTor, die wordt beheerd door het Team Cyber Enabled Crime van de politie. Op deze website publiceert de politie verkopers die zijn aangehouden, en namen van personen en diensten die hun aandacht hebben. Zo hoopt zij het vertrouwen in de anonimiteit van Tor te ondermijnen, en de samenwerking met genoemde personen en diensten minder aantrekkelijk te maken. Ook media-aandacht voor zaken waarin de politie daders wist te identificeren kan hieronder worden geschaard. Deze strategie kan gericht zijn op concrete zaken, maar is soms ook gericht op het ondermijnen van het vertrouwen in betaalmiddelen en cryptomarkten. De overname van Hansa, en de media-aandacht daarvoor, is een voorbeeld hiervan en laat zien hoe ook hier opsporing en preventie hand in hand gaan.

Aan verstoren kleeft volgens de politie ook een nadeel omdat daders daardoor uit beeld kunnen verdwijnen en de politie dan haar informatiepositie kwijt raakt die ze (met moeite) heeft opgebouwd. Met name in kindermisbruikzaken is dit een aandachtspunt.

Conclusies en discussie

Opsporen van verdachten, verlenen van hulp aan slachtoffers, en inzetten van preventieve maatregelen om (verdere) misdrijven te voorkomen zijn niet alleen bij traditionele criminaliteit maar ook bij Tor-zaken de strategieën waarmee de politie op misdrijven reageert (zie ook Newburn et al., 2012, p. 2). Het gebruik van Tor betekent echter dat de criminaliteit zichtbaarder is dan voorheen maar dat de ware identiteiten en locaties van verdachten en slachtoffers verborgen blijven achter encryptie. Dat brengt met zich mee dat de werkwijzen waarmee de strategieën uitgevoerd worden, wel wezenlijk anders zijn dan in traditioneel politiewerk.

Het dark web biedt de politie meer mogelijkheden om misdrijven te observeren en te zien hoe daders opereren. Vaak worden activiteiten die op en via het internet plaatsvinden door systemen ook goed geregistreerd. Het reconstrueren van de misdrijven zelf is daardoor eenvoudiger dan voorheen. Door de anonimiteit die Tor biedt, is het echter niet duidelijk wie de daders en slachtoffers zijn, en vanuit welke offline locatie er wordt geacteerd. Opsporingsonderzoeken zijn daarom veelal gericht op het achterhalen van de identiteit van deze anonieme daders en slachtoffers en/of van hun locaties. In zaken waar mensen en plaatsen onbekend zijn en daders ook elkaar vaak niet kennen, vereist dit een andere aanpak dan in de offline wereld, waar mensen en plaatsen de kernelementen vormen van waaruit naar informatie wordt gezocht (De Poot et al., 2004). Bij criminaliteit op het dark web is het zaak om eerst te achterhalen welke ware identiteit er achter een online personage schuilt en op welke fysieke locatie de daders en slachtoffers zich bevinden. Hiervoor wordt er intensief (digitaal) gespeurd naar fouten waardoor de daders hun identiteit of locaties prijsgeven, bijvoorbeeld darkwebinformatie die kan worden gekoppeld aan een gekende persoon op het reguliere internet of een lek in het digitale systeem. Traditionele werkwijzen in de fysieke wereld blijven daarnaast gewoon bestaan.

Naast het identificeren van daders en slachtoffers (opsporen) zet de politie ook in op preventie. Naast traditionele preventie, in de

Literatuur

- Davies, G. (2020). Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers: *The Journal of Criminal Law.* https://doi.org/10.1177/0022018320952557
- De Poot, C.J., Bokhorst, R.J., van Koppen, P.J., & Muller, E.R. (2004). *Rechercheportret: Over dilemma's in de opsporing.*
- Dordal, P.L. (2018). The Dark Web. In H. Jahankhani (Ed.), *Cyber Criminology* (pp. 95-117). Springer International Publishing. https://doi.org/10.1007/978-3-319-97181-0_5
- Jeffries, S., & Apeh, E. (2020). Chapter 7 – Standard operating procedures for cybercrime investigations: A systematic literature review. In V. Benson & J. Mcalaney (Eds.), *Emerging Cyber Threats and Cognitive Vulnerabilities* (pp. 145-162). Academic Press. https://doi.org/10.1016/B978-0-12-816203-3.00007-1
- Lacey, D., & Salmon, P.M. (2015). It's Dark in There: Using Systems Analysis to Investigate Trust and Engagement in Dark Web Forums. In D. Harris (Ed.), *Engineering Psychology and Cognitive Ergonomics* (pp. 117-128). Springer International Publishing.

vorm van voorlichting of afschrikking, hebben twee andere preventievormen een duidelijke plek, namelijk verstoring van de infrastructuur en verstoring of ondermijning van het vertrouwen. Op Tor is vertrouwen een interessant en ingewikkeld fenomeen. Enerzijds is er veel vertrouwen in de anonimiteit die Tor biedt, wat ervoor zorgt dat daders anoniem kunnen samenwerken en elkaar niet kunnen verraden. Anderzijds is er weinig wederzijds vertrouwen, omdat anonimiteit ook betekent dat er geen bescherming is tegen oplichting tussen samenwerkingspartners. Ook betekent de anonimiteit op Tor dat de politie relatief eenvoudig online kan deelnemen aan interacties (Oerlemans, 2018; C. van den Eeden et al., 2022) en vervolgens vanuit die positie het vertrouwen kan ondermijnen.

Opvallend bij verstoring is dat het vaak sterk steunt op informatie die voortvloeit uit opsporingshandelingen en de inzet van bijzondere opsporingsbevoegdheden. In Nederland kunnen deze bevoegdheden enkel worden ingezet in het kader van een strafrechtelijk onderzoek dat als doel heeft daders op te sporen en te vervolgen. Vaak is echter bij aanvang van een Tor-zaak al duidelijk dat de inzet van verstorende of andere preventieve maatregelen kansrijker zijn dan het identificeren van een dader, en dat aldus met verstoren sneller tegen misdrijven kan worden opgetreden. Zoals eerder ook door Van den Eeden e.a. (2022) in dit tijdschrift werd geconstateerd, ontbreekt er momenteel een juridische grondslag voor de inzet van informatie-vergarende methoden met het doel om gericht preventieve maatregelen zoals verstoren in te kunnen zetten.

ACN's zoals Tor zullen niet meer verdwijnen. De politie gaat niet de capaciteit krijgen om alle op het dark web zichtbare misdrijven aan te pakken. Zij zal dus andere werkwijzen moeten ontwikkelen en stappen die reeds zijn gezet moeten doorontwikkelen. Voor de strategie opsporing betekent dit bijvoorbeeld het doorontwikkelen van werkwijzen om *online ID's* te koppelen aan *real ID's*. Onderdeel daarvan kan zijn dat die koppeling pas plaatsvindt na een eventuele veroordeling, een veroordeling dus van een in de offline wereld nog onbekende verdachte. Daarin heeft het OM het voortouw. Hulpverlening aan slachtoffers van seksueel kindermisbruik en mensenhandel is vooral gebaat bij het doorontwikkelen van het vermogen om *real ID's* vast te stellen en offline locaties te bepalen. Hulpverlening kan dus meeliften met de opsporing. Voor preventie moet met name het verstoren verder worden ontwikkeld. De politie dient antwoorden te vinden op de vraag wat precies moet worden verstoord om een bepaald criminaliteitsprobleem effectief tegen te gaan. Die effectiviteitsvraag is een opgave voor de politie én de wetenschap. En natuurlijk dienen nieuwe werkwijzen te steunen op (eventueel nieuwe) bevoegdheden. Daar ligt een opdracht voor de wetgever. •

> Het **dark web** biedt mogelijkheden om misdrijven te **observeren** en te zien hoe daders **opereren**

Literatuur (vervolg)

- Newburn, T., Williamson, T., & Wright, A. (2012). *Handbook of criminal investigation*. Routledge.
- Odinot, G., Poot, C., & Verhoeven, M. (2018). De aard en aanpak van georganiseerde cybercrime. *Justitiële verkenningen*, *44*(5), 9–22. https://doi.org/10.5553/JV/016758502018044005002
- Oerlemans, J.-J. (2018). Facebookvrienden worden met de verdachte. *Justitiële verkenningen*, *44*(5), 83–99. https://doi.org/10.5553/JV/016758502018044005007
- van den Eeden, C.A.J., van Berkel, J.J., Lankhaar, C.C., & de Poot, C.J. (2021). *Opsporen, vervolgen en tegenhouden van cybercriminaliteit*.
- van den Eeden, C., van Berkel, J., & de Poot, C. (2022). Opsporen, vervolgen en tegenhouden van cybercriminaliteit: Over slimmere omgang met informatie en over de rol van politie en OM. *Het Tijdschrift Voor de Politie*, *84*(2), 26-29.