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

Go digital

Dat ontwikkelingen in de digitale wereld snel gaan, is inmiddels een triviale opmerking en bovendien achterhaald. *Snel* lijkt een te eufemistisch woord, het is voor gewone mensen nauwelijks nog bij te houden. Je wordt er onrustig van.

Een vriend vroeg pas aan mij: wat vind jij eigenlijk van ChatGPT? Ik was al blij dat ik wist waar hij het over had. Toen ik onlangs vijf kernwoorden over leiderschap opgaf, kreeg ik in *no time* een tienminutenspeech aangereikt, waar ik het nauwelijks mee oneens was. Maar een antwoord op zijn vraag had ik eigenlijk niet. Mijn vriend was bezorgd; hij zag het als de volgende aanval op wat *waarheid* is. Kennelijk vond hij waarheid iets van mensen, waar mensen voor – horen te – staan, als een deugd. Kan een machine waarheid voortbrengen?

Er zijn overigens veel mensen die denken van wel. Zij vertrouwen op machines. Digitalisering heeft ook goede kanten. Het lijkt een toenemende trend dat beleid datagedreven moet zijn, evidence-based. Bewijs uit big data, dat onstuimig voorhanden is. Machines doen er dingen mee, die slechts enkelen begrijpen – maar *who cares*, ik heb tenslotte ook geen benul van hoe mijn magnetron werkt, maar hij verwarmt wel. Machines leveren feiten op en dat is onmisbaar om verantwoord keuzes te maken. Een feit staat immers voor de waarheid. Je kunt niet *op de tast* koersen.

Toch deelt niet iedereen dit denken. Ik hoor vier problemen. Allereerst legt Miriam Rasch[1] ons uit hoe elke bewerking van data ons verder van de werkelijkheid brengt. Een datumpunt, losgemaakt van zijn context, is al een eerste vervorming en elke bewerking daarna maakt de betekenis mystieker en verder weg van waarheid. Hoe bigger, hoe vager. Daarnaast legt Adriaan van Veldhuizen[2] uit dat data altijd interpretatie vragen, dus begrijpen en verklaren, en dat kan uitsluitend als er kennis is. *Wie zich door data laat drijven, dobbert uiteindelijk stuurloos rond.* Niet datagedreven, maar kennisgedreven dus. Het grenzeloze vertrouwen in datagedrevenheid past in wat Cees Swart[3] in navolging van Habermas de systeemwereld noemt. In de wereld van mensen, de leefwereld, gaat het echter om narratieven, om daadwerkelijk idealisme, om koerszoekend leiderschap, om innerlijk kompas, om integer improviseren, om deugden en om dialogisch leven. Christiaan Kromme[4] zegt het zo: go digital, stay human; zachte of zo je wilt feminiene kwaliteiten zullen meer en meer betekenis krijgen als het quasi-stevige denken door machines wordt overgenomen. Het brengt Kim Putters[5] tot de uitspraak dat de samenleving geen *evidence*, maar een *verhaal* nodig heeft, waarin burgers volwaardig mee kunnen doen, waar mensen zich gezien voelen, met een speciaal oog voor kwetsbaren.

Wat brengt de digitale wereld ons? Veel, zeggen sommigen, heel veel. Anderen zien dreiging. De overheid – en de politie – moet het goede samenleven ook daar handhaven. Het zou kunnen. Maar erger dan de overschatting van het digitale lijkt mij de onderschatting van het menselijke. Als machines het winnen van menselijke kennis en ervaring, van deugden en compassie, als beleidsmakers meer 'operator' dan idealist zijn, als data vóór waarheden uit het *echte* leven gaan, dan zijn we weer terug bij mijn vriend. Erover nadenkend, ben ik het best wel met hem eens.

1 Rasch, M. (2020). *Frictie. Ethiek in tijden van dataïsme.* De Bezige Bij.
2 Veldhuizen, A. van (2023). Begrijpen voor ingrijpen, op zoek naar een kennisgedreven politie. In: Hoorn, J. van, & Bavel, M. van, *Onze politie in een kwetsbare rechtsstaat.* Gompel&Svacina, p. 161-174.
3 Zwart, C. (2018). *Over hoop.* Anne Pastors.
4 Kromme, C. (2017). *Humanification.* The Choir Press.
5 Putters, K. (2022). *Het einde van de BV Nederland. Over de noodzaak van een verhaal voor onze samenleving.* Prometheus.

Jaco van Hoorn
Hoofdredacteur

HET TIJDSCHRIFT VOOR DE
Politie
NUMMER 2 • 2023

Foto: Pexels/Maxim Hopman

Foto: Pexels/ThisIsEngineering

Foto: Barbara Vreekamp Fotografie, Maarn

Coverfoto
Gorodenkoff / Shutterstock.com

Colofon

Nummer 2, jaargang 85

Verantwoordelijk uitgever
Mr. Stephan Svacina
Gompel&Svacina bv
Antwerpen / 's-Hertogenbosch
info@gompel-svacina.nl
www.gompel-svacina.eu

Hoofdredacteur
Drs. Jaco van Hoorn MPA

Redactie
Dr. Maud van Bavel; Marcel Bruinsma MBA; dr. mr. Barbara van Caem; Stan Duijf MSc; Philippe Estourgie MBA; mr. Sanne Groen; dr. Merlijn van Hulst; mr. dr. Wouter Jong; Evert Jan Kasteel EMSD; dr. Edwin Kruisbergen; dr. Wouter Landman; dr. Joery Matthys; dr. Marc Schuilenburg; dr. Annika Smit; dr. Ronald van Steden; prof. dr. Pieter Tops; mr. Hans de Vries

Eindredactie en redactieadres
Jan van Balkom MA
+31 (0)6 13470687
Achterstraat 95
5268 EB Helvoirt
jan.vanbalkom@gompel-svacina.nl

Boekenredactie en recensies
Dr. mr. Barbara van Caem
Alpen Rondweg 23
1186 CV Amstelveen

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

Internet vraagt een andere politie

Het internet is voor de politie niet 'iets erbij'. Het digitale domein kan niet los worden gezien van de fysieke samenleving waarin de politie werkt. Een prangend vraagstuk dat bij de politie voorligt, gaat dus niet sec over de rol en functie van de 'politie op het internet', maar meer over de 'politie in een digitaal transformerende samenleving'. Sociaal-maatschappelijke, technologische en politieke ontwikkelingen vragen nu al, maar zeker in de toekomst, niet meer maar iets anders van de politie. Het wordt tijd voor nieuwe concepten.

Over de auteurs
Drs. Martin van Wijngaarden en Rik Schiffelers MSc, B.A. zijn beiden strategie-adviseur bij het team Strategievorming & Duiding van de directie Strategie & Innovatie (Staf Korpsleiding).
Zij hebben deze bijdrage op persoonlijke titel geschreven.

Tekst: Martin van Wijngaarden & Rik Schiffelers • Afbeeldingen gemaakt o.b.v. artificiële intelligentie

Al enige tijd is de politie bezig om de brede vraag te beantwoorden wat haar rol en positie op 'het internet' moet zijn, nu en in de toekomst. Het internet is in feite een technisch fenomeen: een wereldwijd netwerk van computers, servers, routers, switches en andere hardwarecomponenten die met elkaar verbonden zijn via een reeks protocollen en standaarden. Dat internet heeft zich de afgelopen dertig jaar in een hoog tempo ontwikkeld, en heeft naast razendsnelle uitwisseling van gegevens een breed scala aan diensten en toepassingen mogelijk gemaakt. Daarbovenop is ook de platformeconomie ontstaan[1]. Alle nieuwe functionaliteiten daarvan hebben gezorgd voor een flinke toename van efficiëntie en gemak, maar ook voor grote veranderingen op de arbeidsmarkt, andere concurrentieverhoudingen, disruptie van traditionele bedrijfsmodellen en veranderende machtsverhoudingen.

Sociale impact

Het wereldwijde web werd bij het ontstaan gezien als "een medium waarmee nieuwe vormen van communicatie en kennisdeling worden gedemocratiseerd, met als doel om een rechtvaardige wereld te scheppen"[2]. Maar het heeft in de loop van de tijd helaas ook allerlei negatieve maatschappelijke effecten veroorzaakt, zoals het op grote schaal verspreiden van desinformatie, het ontstaan van digitale ongelijkheid, online intimidatie, nieuwe vormen van verslavingsproblematiek, nieuwe privacyvraagstukken en verminderde sociale interactie. Al in de jaren tachtig waren er discussies over anonimiteit op het internet, en over moderatie van en verantwoordelijkheid voor inhoud die daarop wordt aangeboden. Dat zijn dus geen vraagstukken die zich pas recent hebben ontwikkeld.

Sterk fluïde en moeilijk grijpbaar

Mede door het internet zijn ontwikkelingen in de samenleving sterk fluïde en moeilijk grijpbaar geworden. Er zijn diverse complexe maatschappelijke fenomenen ontstaan die voor de politie relevant zijn. We beschrijven er hier een aantal, samen met voorbeelden van vragen die ze opwerpen.
Socialemediaplatformen hebben een cruciale rol bij de ontwikkeling van onrust bij groepen in de samenleving, doordat zij protest- of anti-establishmentgroepen verenigen onder de paraplu van een narratief van onvrede, wantrouwen of onrecht[3]. Dat is van alle tijden, maar de eenvoud van gebruik, snelheid, massaliteit en internationaliteit van deze media zijn sterke katalysatoren gebleken. De nieuwe platformen hebben bovendien de diversiteit en omvang van media sterk doen toenemen[4]. Momenteel gebruikt meer dan de helft van de Nederlanders sociale media als primaire nieuwsbron. Daarbij ontbreekt de duiding en

> “Om in **verbinding** te zijn met je **omgeving**, zul je de **vorm** van die omgeving moeten **aannemen**”

context van gebeurtenissen vaak en worden filterbubbels en echokamers tot stand gebracht door toegepaste businessmodellen en algoritmen. Welke maatschappelijke dynamiek wordt hierdoor veroorzaakt en welke rol heeft de politie bij het beheersen daarvan?

Het technologienieuws wordt de laatste tijd gedomineerd door ‘generatieve kunstmatige intelligentie’. De technologische concepten achter kunstmatige intelligentie zijn al veertig tot vijftig jaar bekend, maar het wachten was op computers die voldoende krachtig zouden zijn om de theorie effectief in de praktijk te kunnen brengen. De enorme hoeveelheid gegevens die de afgelopen decennia via het internet zijn verzameld, is bovendien cruciaal geweest. Negentig procent van alle gegevens op de wereld is in de laatste paar jaren vastgelegd. Die toename zet door, maar een steeds groter deel zal de komende jaren kunstmatig gegenereerd (of ‘synthetisch’) zijn. Dit zal steeds vaker leiden tot vragen over de betrouwbaarheid, kwaliteit en authenticiteit van informatie. Welke rol heeft de politie bij het bewaken daarvan en hoe gaat de politie zelf om met deze vormen van onduidelijkheid?

Immorele of schadelijke uitingen en gedragingen op het internet[5] kunnen grote impact hebben op het leven van mensen. Het Rathenau Instituut heeft ze in kaart gebracht, samen met de kenmerken van de online omgeving waardoor ze worden bevorderd[6]. Denk dan aan informatiemanipulatie, haat, eigenrichting, pesterij, geweld, bedrog en zelfbeschadiging. Rathenau concludeert dat burgers op het internet onvoldoende zijn beschermd. Eerder concludeerde ook de Adviesraad Internationale Vraagstukken van de WRR dat de legitimiteit van de rechtsstaat onder druk staat, door de betrekkelijk geringe aanwezigheid van de overheid in het publieke online domein[7]. Wat doet de politie met uitwassen op het internet zolang de rol van de overheid niet scherp is?

Het internet speelt ook een faciliterende rol bij de evolutie van georganiseerde criminaliteit[8]. De toegankelijkheid van moderne techniek stelt criminele organisaties in staat om nieuwe markten aan te boren, waarbij polycriminele netwerken ontstaan. Ze zijn in staat om nieuwe, op platformen en andere op moderne technologie gebaseerde bedrijfsmodellen te ontwikkelen. En ze benutten meerdere technologieën om hun bereik, financiële winsten en ondermijnende invloed op de samenleving te vergroten. Technologie is daarbij niet alleen een facilitator, maar onder de noemer ‘crime-as-a-service’ ook een op zichzelf staand ‘verpakbaar’ en doorverkoopbaar product. Hoe volgt de politie welke nieuwe criminele dreigingen zich ontwikkelen? Hoe ontwikkelen we manieren om deze te bestrijden en welke internationale samenwerking is daarvoor nodig?

Tot slot constateren we dat de combinatie van sociale media, online gemeenschappen en de platformeconomie heeft geleid tot nieuwe vormen van macht en invloed. De afhankelijkheid van private tech-giganten en platformbedrijven is enorm[9]. Het grootste probleem van het huidige digitale tijdperk is niet dat die bedrijven lak hebben aan privacy. Onze democratieën worden bedreigd doordat de grote technologiebedrijven een enorme politieke factor zijn geworden, terwijl ze nauwelijks ter verantwoording te roepen zijn. Commerciële partijen beslissen grotendeels zelf welke informatie uitgelicht of weggelaten wordt. Dat is duidelijk een uitoefening van

1 Het economische systeem waarin bedrijven via digitale platforms vraag en aanbod bij elkaar brengen en transacties tussen verschillende partijen faciliteren. Lees ‘Platformrevolutie’, Martijn Arets (2020).
2 ‘Het internet is stuk, maar we kunnen het repareren’, Marleen Stikker (2019).
3 ‘Maatschappelijke Ontgoocheling van de Middenklasse. Optreden, Oorzaken en Gevolgen’ door Frank Bekkers, Eline de Jong, Laura Jasper en Ella MacLaughlin, HCSS (februari 2023).
4 ‘De staat van de rechtsstaat’ door Linde Arentze, Diederik Dekkers, Paul Sinning, Frank Bekkers en Tim Sweijs, HCSS in opdracht van de directie Strategie van de Nederlandse politie. Nog uit te brengen in april 2023.
5 Zie ook: ‘Evil online’, Jeroen van den Hoven en Dean Cocking (2018).
6 ‘Online Ontspoord’, Van Huijstee et al., Rathenau Instituut (2021).
7 Regulering van online content, naar een herijking van het Nederlandse internetbeleid. Adviesraad Internationale Vraagstukken (juni 2020).
8 Fourth Generation Organised Crime: Systemic change and the evolving character of modern transnational organized crime. HCSS in opdracht van de directie Strategie van de Nederlandse politie. Nog uit te brengen in april 2023.
9 ‘Digitale afhankelijkheid van platformbedrijven’, Rathenau Instituut (nog te publiceren).

Nieuwe concepten voor politiewerk onder het motto ‘niet meer, maar anders’

macht[10]. Op het gebied van kunstmatige intelligentie zijn vergelijkbare praktijken te verwachten. Europese wetgeving op het gebied van internetgedrag[11] richt zich op een betere positie voor internetgebruikers door extra regels, meer toezicht en meer verantwoordelijkheden voor de wereldwijd grootste online platforms en aanbieders van digitale diensten. Maar is dat voldoende? Wie moet de regels handhaven? Maar ook: op welke terreinen zou de politie juist met deze bedrijven moeten samenwerken?

Niet meer, maar anders

Het geweldsmonopolie en de bijzondere bevoegdheden staan altijd centraal als onvervreemdbare en unieke kenmerken van de politie. Over de evolutie van andere elementen van de politietaak en de daarbij behorende richtinggevende principes en operationele concepten wordt met enige regelmaat goed nagedacht. Twee belangrijke momenten in dat kader worden gemarkeerd door de rapporten ‘Politie in Verandering’[12] uit 1978 en ‘Politie in Ontwikkeling’[13] uit 2005. Ieder van deze visies heeft een periode van tien tot vijftien jaar ingeluid waarin behoorlijke veranderingen tot stand zijn gebracht in het politiebestel, de politieorganisatie en de aanpak van politiewerk. Denk aan centralisatie van de organisatie, meer gedeelde verantwoordelijkheid met lokale overheden voor veiligheid en openbare orde, en de ontwikkeling van concepten als GGP, IGP en nodale oriëntatie.

Op dit moment bepaalt de politie haar handelingsperspectief hoofdzakelijk aan de hand van wat ze waarneemt in de samenleving en de mogelijke risico’s voor de veiligheid en de openbare orde. Dat kan goed werken, zoals bij recente voorbeelden van het oprollen van illegale digitale marktplaatsen en cryptodiensten waar criminele organisaties op steunen. Maar die reactieve, risicogeoriënteerde aanpak blijkt ook steeds vaker niet volledig toereikend.

De digitale strategie van de Britse politie stelt heel treffend: “de snelheid van verandering is nog nooit zo snel geweest, maar het zal tegelijk ook nooit meer zo langzaam gaan”[14]. Anticiperen op mogelijke toekomstscenario’s wordt dan ook steeds belangrijker. Achttien jaar na ‘Politie in Ontwikkeling’ zijn diverse van de genoemde visie-elementen zoals GGP, IGP en nodale oriëntatie opnieuw aan actualisatie en aanvulling toe. En zelfs voor vaste waarden als het geweldsmonopolie en bijzondere bevoegdheden is het de vraag hoe die er in een digitaal transformerende samenleving uit komen te zien.

Het is duidelijk dat de rol en functie van de politie op het internet niet ‘bovenop het traditionele politiewerk’ komt. De fysieke en digitale samenleving vormen samen één versmolten ecosysteem. Omdat dit steeds meer en diepgaander wordt gevormd door digitale technologie, verschuift ook het zwaartepunt van politiewerk. De fysieke wijk is bijvoorbeeld al lang niet meer de enige plek waar de politie haar verbinding moet organiseren. Concerndirecteur Jan van Ginkel van de provincie Zuid-Holland formuleerde het onlangs treffend: “Om in verbinding te zijn met je omgeving, zul je de vorm van die omgeving moeten aannemen.” Een combinatie van onze activiteiten ‘in het digitale domein’ en in de fysieke samenleving zal nieuwe concepten voor politiewerk vragen, onder het motto ‘niet meer, maar anders’.

10 NRC interview Jamie Susskind 3 februari 2023. https://www.nrc.nl/nieuws/2023/02/03/techcriticus-jamie-susskind-we-moeten-anders-gaan-denken-over-technologie-politieker-a4156122
11 De Digital Services Act (DSA) en Digital Markets Act (DMA)
12 ‘Politie in verandering – Een voorlopig theoretisch model’, Projectgroep organisatiestructuren (1978).
13 ‘Politie in ontwikkeling – Visie op de politiefunctie’, projectgroep Visie op de politiefunctie en Raad van Hoofdcommissarissen (2005).
14 ‘National Policing Digital Strategy’, the National Police Chiefs’ Council (NPCC) (2020).

Tijd voor een andere blik

Gelukkig zijn er al initiatieven waarin elementen voor een nieuwe uitgangspositie voor de politie worden omschreven, zoals een uitvraag onder de strategische top van de politie over de gewenste rol en positie van de politie op het internet en een recent advies over de politie in de informatiesamenleving[15]. Deze laten een aantal gemeenschappelijke rode lijnen zien. Zo wordt vastgesteld dat er geen principieel onderscheid bestaat tussen het fysieke en het digitale domein als het gaat over de uitvoering van de politietaak. De politie is daar aanwezig waar burgers zijn en interacteren; dat is dus nadrukkelijk en in toenemende mate op het internet. Ook wordt onderkend dat het werkgebied in het fysieke domein al steeds minder gebiedsgrenzen kent en dat deze in het digitale domein nog veel minder gelden. Het voorkomen van misbruik van internet is in eerste instantie voornamelijk aan andere partijen. De politie moet wel nauw samenwerken met deze partijen en heeft daarin een belangrijk signalerende taak, omdat we door onze positie in de samenleving als een van de eersten worden geconfronteerd met nieuwe veiligheidsissues. Het belang van signaleren en adviseren neemt binnen deze context en in het samenspel met andere actoren sterk toe. Ten slotte kan de politie een symbolische rol hebben door incidenteel op te treden om voorbeelden te stellen en te agenderen.[16]

Dit zijn voornamelijk algemene uitgangspunten die nader moeten worden uitgewerkt. Om te voorkomen dat we na 'Politie in Verandering' en 'Politie in Ontwikkeling' terechtkomen in 'Politie in Verwarring' moeten we met een andere bril naar de samenleving leren kijken. Een die ons helpt om het moderne ecosysteem met alle fysieke en digitale elementen goed waar te nemen en te begrijpen. Daarvoor is het nodig om continu en kort-cyclisch kennis op te bouwen over maatschappelijke fenomenen en om met mensen vanuit diverse vakdisciplines binnen en buiten de politie na te denken over hoe deze zich zouden kunnen ontwikkelen in voorstelbare toekomstscenario's. Dan komen we ongetwijfeld tot de ontdekking dat de rollen en taken voor de politie wel enigszins gelijk zullen blijven, maar dat ze zich uitdrukkelijk anders moeten gaan manifesteren.

> Vormgeven aan **flexibele** samenwerkingsverbanden in de **netwerksamenleving**

Anders gezegd, het moment is hier om vernieuwende concepten te verkennen. We doen een aantal suggesties. Te denken valt aan het ontwikkelen van 'community policing 3.0', waarin we met nieuwe concepten naast de (digitale) wijkagent verbonden zijn en blijven met de haarvaten van de samenleving. In het verlengde van relatief recente ideeën over 'overheid als een platform', kunnen we met onze partners verkennen of en hoe veiligheidszorg in Nederland georganiseerd kan worden volgens platformprincipes. Zet moderne technieken in om de enorme hoeveelheid beschikbare gegevens op een zinvolle manier te verwerken voor verschillende werkvelden binnen de politie. Ontwikkel zo ook manieren om maatschappelijk sentiment te voorzien en op grond daarvan passende partijen tot actie te bewegen. Geef vorm aan flexibele samenwerkingsverbanden voor het uitvoeren van de politietaak in de netwerksamenleving, ook internationaal. Maak daarbij slim gebruik van de veranderende arbeidsmarkt waarin nieuwe functies en vakdisciplines ontstaan en pas de organisatie daarop aan.

In deze zoektocht naar 'anders politie zijn' staan we gelukkig niet alleen. Buitenlandse partnerorganisaties en politiediensten zijn op zoek naar antwoorden op dezelfde vragen. Binnen Europol- en INTERPOL-verband werken we al goed samen in het formuleren en delen van uitgangspunten en praktijkervaringen. Dat het vraagstuk alsnog uitdagingen en fundamentele keuzes met zich meebrengt is evident. We moeten dan ook niet overhaasten, behouden wat werkt, goed nadenken over onze opties en onderkennen dat dit een continu proces zal blijven. Onder het motto 'niet meer, maar anders' zullen we dan niet alleen antwoorden vinden op huidige uitdagingen, maar ook kansrijke mogelijkheden voor nieuw politiewerk. •

15 Onder informatiesamenleving verstaan we digitalisering en de sociaal-maatschappelijke gevolgen daarvan.

16 Lees voor meer achtergrond ook het themanummer 'Politie en rechtsstaat in de gedigitaliseerde samenleving' (2022) van *Cahier Politiestudies*.

ONLINE GEGEVENSGARING IN EEN WOELIGE SAMENLEVING

Spanningen bij politiewerk op het web

De politie maakt in haar werk in toenemende mate gebruik van gegevens op het wereldwijde web. Dit doet zij voor verschillende doeleinden. In hoofdlijnen is hierbij een onderscheid te maken tussen intelligence en bewijs.

Het online vergaren van gegevens ten behoeve van intelligence wordt OSINT genoemd: *open source intelligence*. Het online vergaren van gegevens ten behoeve van bewijs wordt internetrechercheren genoemd. OSINT heeft een niet-strafvorderlijk karakter en moet plaatsvinden op basis van de algemene taakstelling, die is opgenomen in artikel 3 van de Politiewet. Internetrechercheren heeft een strafvorderlijk karakter en vindt plaats binnen het kader van het Wetboek van Strafvordering. Dit artikel gaat over OSINT. De eerste paragrafen zijn inleidend en daarna volgen de vijf spanningen die centraal staan in dit artikel.

Intelligence is geanalyseerde informatie en kennis op grond waarvan beslissingen over de uitvoering van de politietaak worden genomen (Kop & Klerks,(2009). Korter gezegd: *information designed for action* (Duijn, 2011). In het intelligenceproces worden informatie- of intelligenceposities opgebouwd[1] over veiligheidsthema's. Voor het opbouwen van deze posities worden uiteenlopende gegevensbronnen benut. Een van die bronnen bestaat uit online gegevens. Het gaat daarnaast om bronnen waar de politie al langer gebruik van maakt, waaronder gegevens die worden verzameld in het straatwerk, in de opsporing en via het runnen van informanten. De bijdrage die online beschikbare gegevens leveren aan de intelligencepositie, is onder andere afhankelijk van de aard van het veiligheidsthema (Landman & Groothuis, 2022). In dit artikel zoom ik vooral in op het gebruik van OSINT voor het opbouwen van een intelligencepositie op het gebied van maatschappelijke onrust, omdat 1) dit een actueel thema is waarbij OSINT een belangrijke rol speelt, en 2) zich bij dit thema volop spanningen rond het gebruik van OSINT voordoen.

1 Onder opbouwen schaar ik ook het onderhouden van de intelligencepositie.

Over de auteur
Wouter Landman PhD begeleidt veranderprocessen en verricht onderzoek. Actuele thema's zijn: technologie & politiewerk, innovatie en ontwikkeling van politieteams. www.bureaulandman.nl

Tekst: Wouter Landman

Maatschappelijke onrust als veiligheidsthema

In de Veiligheidsagenda 2023-2026 is maatschappelijke onrust omschreven als "collectieve gedragingen in situaties die voortkomen uit een gevoel van angst, onzekerheid, onvrede of miskenning" (Ministerie van Veiligheid en Justitie, 2022). Er zijn verschillende vormen van maatschappelijke onrust, uiteenlopend van vreedzame en kleinschalige demonstraties tot radicale(re), stafbare en grootschalige acties. Er is tegenwoordig sprake van een breed scala aan maatschappelijke thema's die collectief ongenoegen in grote groepen in de samenleving veroorzaken (Bekkers et al., 2023). Hierdoor is de Nederlandse samenleving in 'woelig vaarwater' terechtgekomen (Eysink Smeets, 2022). Dit vaarwater wordt gekenmerkt door spanningen tussen bevolkingsgroepen en verzet tegen de overheid.

Het internet in het algemeen en socialemediaplatformen in het bijzonder spelen een belangrijke rol bij maatschappelijke onrust: het is het domein waar burgers zich onder andere uiten, verbinden en organiseren met gelijkgestemden en waar zij (des)informatie tot zich nemen die van invloed is op het ervaren ongenoegen (Bekkers et al., 2023; Beugelsdijk, 2021; Fukuyama, 2019). Deze rol van sociale media bij maatschappelijke onrust impliceert dat het voor de politie een belangrijk domein is voor het vergaren van gegevens over dit veiligheidsthema. Sinds de avondklokrellen in januari 2021 – toen de samenleving (opnieuw) te maken kreeg met grootschalige, online aangejaagde openbare ordeverstoringen – zijn de investeringen van de politie in OSINT dan ook toegenomen (Landman & Groothuis 2022).

Inzet van OSINT

Online verzamelde gegevens worden gebruikt voor het *monitoren* van trends & ontwikkelen en het *identificeren* van groepen en personen op het gebied van maatschappelijke onrust. OSINT-activiteiten worden vooral uitgevoerd door specialisten binnen de intelligenceorganisatie van de politie en in toenemende mate ook door digitaal-wijkagenten in de basisteams

> Het internet en socialemediaplatformen spelen een **belangrijke rol** bij maatschappelijke **onrust**

(Terpstra et al., 2021). Daarnaast zijn er binnen de specialistische opsporing *virtual agents*, die online onder dekmantel werken en ook worden ingezet ten behoeve van de intelligencepositie op het gebied van maatschappelijke onrust. Online gegevensvergaring vindt zowel handmatig als geautomatiseerd plaats. Voor de geautomatiseerde vergaring wordt uiteenlopende software gebruikt. De verzamelde gegevens worden in de regel gecombineerd met andere (politie)gegevens en geanalyseerd om te komen tot intelligenceproducten. Een voorbeeld van een intelligenceproduct is een rapport waarin boerenactiegroepen zijn beschreven die zich bezighouden met buitenwettelijke methoden van actievoeren.

Spanning I: offline en online

In de samenleving zijn offline en online werelden die voortdurend in elkaar overlopen (Lane, (2019). Dit geldt ook voor de gegevensverzameling voor de politie: de politie verzamelt zowel offline als online gegevens en combineert deze met elkaar. In berichtgeving over de online gegevensverzameling heeft de politie de neiging online gegevensverzameling op gelijke voet te stellen met offline gegevensverzameling. De politie-eenheid Den Haag gaf naar aanleiding van de berichtgeving over de virtual agent die – 'vermomd' als activiste – meekeek en meedeed in chatgroepen van Extinction Rebellion bijvoorbeeld aan dat dit te vergelijken is met het surveilleren door agenten in burgerkleding op straat.[2] Daarmee oogt de gegevensverzameling door de virtual agent licht en past het binnen de algemene taakstelling.

2 www.trouw.nl/binnenland/hoe-ver-mag-de-politie-gaan-bij-het-heimelijk-meekijken-in-chatgroepen

> **Digitale surveillance** is snel **diepgaander** dan **traditionele surveillance**

Het is echter de vraag of deze redenering voldoende hout snijdt. Digitale surveillance is namelijk (snel) diepgaander dan traditionele surveillance. Een politieagent die in burger in de wijk loopt en door de gordijnen kijkt of een 'interessante' burger thuis is, krijgt op dat moment een weinig diepgaand inzicht in het leven van die burger. Een politieagent die met een niet tot de politie herleidbaar account (functioneel account) een profiel van een burger op Facebook bekijkt, krijgt in veel gevallen een diepgaander inzicht, zoals inzicht in relaties en activiteiten.

Online gegevensverzameling is dus een ander type activiteit met andere effecten dan offline gegevensverzameling (Ferguson, 2022). Dit heeft onder andere als gevolg dat het juridisch kader voor regulering van offline gegevensverzameling niet of nauwelijks geschikt is voor regulering van online gegevensverzameling (Commissie Koops, 2018). In de praktijk moet niettemin van dit juridisch kader gebruik worden gemaakt, omdat er vooralsnog geen – op online gegevensverzameling toegesneden – juridisch kader is.

Spanning II: een niet meer dan geringe en meer dan geringe inbreuk

OSINT moet worden gebaseerd op de algemene taakstellende bevoegdheid van de politie, die wordt ontleend aan artikel 3 Politiewet. Deze bevoegdheid kan breed worden ingezet ten behoeve van het politiewerk (Zuurveen & Stol, 2020). De inzet wordt begrensd door het effect ervan op de grondrechten van burgers. Op basis van artikel 3 mogen opsporingsambtenaren van de politie uitsluitend een niet meer dan geringe inbreuk op deze grondrechten maken. Dit betreft onder andere het recht op eerbiediging van de persoonlijke levenssfeer. Dit recht wil eenvoudig geformuleerd zeggen dat iedere burger het recht heeft om (door de overheid) met rust te worden gelaten.

Online gegevensverzameling door de politie is – zoals gezegd – sneller diepgaander dan offline gegevensverzameling: er wordt relatief snel een min of meer volledig beeld van aspecten van iemands leven verkregen. Dit geldt in het bijzonder wanneer online verzamelde gegevens worden gecombineerd met andere gegevens. Ieder gegeven op zichzelf geeft dan wellicht nog niet zoveel inzicht, maar het resultaat van het combineren en analyseren doet dit wel (Fedorova et al., 2022). Als je sleutelpersonen binnen een protestgroep in kaart brengt, hun identiteit weet vast te stellen, online gegevens verzamelt, gegevens uit politiesystemen en de Basisregistratie Personen gebruikt, kun je een min of meer volledig beeld van aspecten van iemands leven krijgen.[3] Op dat moment kan er al sprake zijn van een meer dan geringe inbreuk in de persoonlijke levenssfeer.

Dit betekent dat de politie met OSINT moet stoppen zodra de drempel van de 'meer dan geringe inbreuk' in zicht komt (Commissie Koops, 2018). Dit roept een spanning op. Van de politie wordt verwacht dat zij zicht heeft op maatschappelijke ontwikkelingen, weet wat er bij bijvoorbeeld demonstraties kan worden verwacht en daarop anticipeert. Het voldoen aan deze verwachting wordt bemoeilijkt doordat de politie op het gebied van OSINT snel tegen grenzen aanloopt.

Spanning III: een publiek toegankelijke en afgeschermde bron

OSINT staat voor 'open source intelligence'. Open source wil zeggen dat het om publiek toegankelijke bronnen gaat. De grens tussen een publiek toegankelijke en afgeschermde online bron is echter niet duidelijk. In de Memorie van Toelichting op het gemoderniseerde Wetboek van Strafvordering is enige helderheid gegeven. Tot een publiek toegankelijke bron

3 Hierbij moet de politie overigens alert zijn op het gebruik van commerciële datasets die worden aangeboden door leveranciers van software, zoals (extra opties binnen) Maltego. Ik heb geen kennis over dit gebruik, maar wil er slechts op wijzen dat dit een risico is in het kader van inbreuk op de persoonlijke levenssfeer. Zie het rapport van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (2022) over automated OSINT in de context van de inlichtingen- en veiligheidsdiensten.

Literatuur

- Bantema, W., Twickler, S.M.A., Munneke, S.A.J., Duchateau, M. & Stol, W.Ph. (2018). *Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld.* Den Haag: Sdu.
- Bekkers, F., De Jong, E., Jasper, L., & MacLaughlin, E. (2023). *Maatschappelijke ontgoocheling van de middenklasse. Optreden, oorzaken en gevolgen.* The Hague Centre for Strategic Studies.
- Beugelsdijk, S. (2021). *De verdeelde Nederlanden. Hoe een perfecte storm een klein land dreigt te splijten (en wat we daaraan kunnen doen).* Amsterdam: Balans.
- Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Commissie Koops) (2018). *Regulering van opsporingsbevoegdheden in een digitale omgeving.* Den Haag.

kan toegang worden verkregen zonder een beveiliging te doorbreken of omzeilen, zonder het aanwenden van technische ingrepen, valse signalen of valse sleutels of het aannemen van een valse hoedanigheid.[4] Het gaat dus niet om de aard van de bron, maar om de wijze van toegang. Ik neem Facebook als voorbeeld. Er is sprake van een publiektoegankelijke bron als een politiefunctionaris met een functioneel account gegevens van een Facebookprofiel van een burger overneemt. Er is sprake van een afgeschermde bron als de politiefunctionaris vrienden wordt met de betreffende burger en vervolgens gegevens overneemt. Deze gegevens zijn namelijk niet voor iedereen toegankelijk, maar alleen voor vrienden en de betreffende burger geeft actief toegang door een vriendschapsverzoek te accepteren.

Het onderscheid tussen een publiek toegankelijke en afgeschermde bron is van belang, omdat – op basis van het gemoderniseerde Wetboek van Strafvordering – mag worden aangenomen dat het verzamelen van gegevens in afgeschermde bron om een 'zwaardere' bevoegdheid vraagt. Dit impliceert naar mijn idee dat het overnemen van gegevens uit afgeschermde bronnen op basis van artikel 3 niet mogelijk is of in ieder geval ter discussie staat. Dit zorgt voor een spanning, want de communicatie tussen burgers die voor de intelligencepositie van belang is, vindt tegenwoordig vooral plaats in allerlei online groepen. Het is in de praktijk niet altijd duidelijk in welke mate dergelijke groepen als afgeschermde bronnen moeten worden opgevat. In de praktijk blijken eenheden hier verschillend mee om te gaan: sommige eenheden zijn op grond van artikel 3 niet of nauwelijks aanwezig in online groepen, anderen zijn dat wel (Landman & Groothuis, 2022).

Spanning IV: (informatie)officier en burgemeester

In de Politiewet is het eenduidig geformuleerd: de politie treedt op onder het gezag van de burgemeester als het de openbare orde betreft en onder het gezag van de officier van justitie als het gaat om strafrechtelijke handhaving. Maar hoe zit dit bij online gegevensverzameling

> De politie is **op zoek** naar haar **gezag** in het kader van **online gegevensvergaring** op het gebied van **maatschappelijke onrust**

gericht in het kader van maatschappelijke onrust? De officier van justitie is het gezag bij strafrechtelijke handhaving, maar in veel gevallen gaat het om situaties waarin er (nog) geen specifieke verdenking is van enig strafbaar feit. De informatieofficier geeft richting aan en oefent gezag uit over de onderdelen van de politie die belast zijn met het informatieproces ter ondersteuning van de strafrechtelijke handhaving, maar het gaat hier om het informatieproces ter ondersteuning van (ook) de openbare orde. De burgemeester is het gezag bij het optreden in het kader van de openbare orde, maar het gaat hier om online gegevensverzameling in het kader van mogelijke openbare orde verstoringen. Dit is een andere vorm van 'optreden' dan waar het gezag van de burgemeester van oorsprong betrekking op heeft.

Het voorgaande heeft tot gevolg dat de politie op zoek is naar haar gezag in het kader van online gegevensvergaring op het gebied van maatschappelijke onrust. In de praktijk leidt dit tot verschillen (Landman & Groothuis, 2022). In een deel van de eenheden wordt er vanuit de intelligenceorganisatie – of vanuit de specialistische opsporing waar virtual agents werkzaam zijn – afgestemd met de informatieofficier. In sommige eenheden wordt er (af en toe) afgestemd met de burgemeester, omdat het om openbare orde aspecten gaat. In algemene zin geldt echter dat de burgemeester niet gewend is aan deze rol en het grenzeloze karakter van bijvoorbeeld online groepen zich moeizaam verhoudt tot het lokale karakter van het gezag (Bantema et al., 2018). In de praktijk zijn er met betrekking tot de beslissingsbevoegdheid dus

4 Zie p. 499 van de MvT, ambtelijke versie juli 2020.

Literatuur (vervolg)

- Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (2021). *Automated OSINT: tools en bronnen voor openbronnenonderzoek.* CTIVD
- Duijn, P. (2011). Intelligence en recherchestrategieën. In N. Kop, R. van der Wal & G. Snel (red.), *Opsporing belicht: over strategieën in de opsporingspraktijk* (pp. 63-94). Apeldoorn: Politieacademie.
- Eysink Smeets, M. (2022). *Onrust begrijpen begint bij anders kijken. Een veiligheidspsychologisch perspectief op maatschappelijke onrust.* Utrecht: Centrum voor Criminaliteitspreventie en Veiligheid.
- Fedorova, M.I., Te Molder, R.M., Dubelaar, M.J., Lestrade, S.M.A., & Walree, T.F. (2022). *Strafvorderlijke gegevensverwerking. Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden.* Nijmegen: Radboud University Press.
- Ferguson, A.G. (2022). Why digital policing is different. *Ohio State Law Journal*, 1-32.

> Het **risico** is dat er in toenemende mate een **politie ontstaat** die opereert op de **grens** van uitingen én gedragingen van **burgers**

Literatuur (vervolg)

- Fukuyama, F. (2019). *Identiteit. Waardigheid, ressentiment en identiteitspolitiek*. Amsterdam: Atlas Contact.
- Kop, N., & Klerks, P. (2009). *Doctrine intelligencegestuurd politiewerk*. Apeldoorn: Politieacademie.
- Landman, W. & Groothuis, S. (2022). *Politiewerk op het web. Een verkennend onderzoek naar online gegevensvergaring door de politie*. Den Haag: Sdu.
- Lane, J. (2019). *The digital street*. Oxford University Press.
- Ministerie van Justitie & Veiligheid (2022). *Veiligheidsagenda 2023-2026*. Ministerie van Justitie & Veiligheid.
- Schuilenburg, M.B. (2016). Predictive policing. De opkomst van een gedachtenpolitie? *Ars aequi, 65*(12), 931-936.
- Terpstra, J., Salet, R., Duijneveldt, I. van & Havinga, T. (2021). *Gebiedsgebonden politiewerk in ontwikkeling. Onderzoek naar basisteams in een digitale en superdiverse samenleving*. Den Haag: Sdu.
- Zuurveen, R. & Stol, W. (2020). *Benutten van digitale sporen*. Den Haag: Sdu.

onduidelijkheden, die binnen de politie zorgen voor een spanningsveld: het gezag is nodig als houvast in soms onduidelijke situaties, maar het gezag is zoekende naar diens eigen rol.

Spanning V: uiting en gedraging

De vijfde en laatste spanning heeft een iets ander karakter dan de vier voorgaande spanningen, maar verdient naar mijn idee wel aandacht. De online gegevensverzameling in het kader van maatschappelijk ongenoegen heeft onder andere het karakter van het (al dan niet geautomatiseerd) monitoren van allerlei uitingen die burgers doen. Burgers die uitingen doen die wijzen op mogelijke strafbare feiten, openbare orde verstoringen of anderszins zorgelijk zijn, worden in meer of mindere mate aan nadere gegevensverzameling en analyse onderworpen. Dit kan vervolgens leiden tot vormen van proactieve optreden. Gegeven de maatschappelijke ontwikkelingen is dit tot op zekere hoogte nodig en begrijpelijk. Het wordt ook van de politie verwacht, want voorkomen is beter dan genezen.

Deze praktijk gaat echter gepaard met de kans dat er in toenemende mate een politie ontstaat die opereert op de grens van uitingen én gedragingen van burgers (Schuilenburg, 2016). In februari 2023 was er een jongeman die naar aanleiding van de megawinst van Ahold Delhaize had getweet dat het moreel acceptabel was om te stelen bij Albert Heijn, omdat er over de rug van de basisbehoeften van burgers megawinsten werden gemaakt. Dit resulteerde in een wijkagent aan de deur die aangaf dat ze een signaal had gekregen van de 'digi-afdeling'. Ze waarschuwde de jongeman en gaf aan dat als het 'verder zou gaan met hem', de politie zou gaan kijken wat er kan worden gedaan met het account. Ook werd aangegeven dat hij online gevolgd zou worden. Dit voorbeeld illustreert mijns inziens hoe de politie op basis van (online) intelligence aan het schuiven is op de grens tussen uiting en gedraging. Het gevaar ontstaat dat het hebben en uiten van bepaalde gedachten steeds meer voorwerp van politiecontrole gaat worden (Schuilenburg, 2016). Dit roept een fundamentele spanning op tussen het belang van proactief politieoptreden enerzijds en het belang van de vrijheidssfeer van burgers anderzijds. Deze spanning leidt naar de vraag wat voor een politie wij in onze samenleving willen hebben.

Tot slot: legitiem politiewerk mogelijk maken

De politie staat voor de opgave om de beschreven spanningen te hanteren en waar mogelijk op te lossen. Om dit te goed te kunnen doen, is een passend juridisch kader nodig. De modernisering van het Wetboek van Strafvordering is een verbetering voor internetrechercheren – want er komt een (specifieke) wettelijke grondslag voor het stelselmatig overnemen van gegevens uit publiek toegankelijke bronnen – maar hier heeft OSINT weinig tot niets aan. Niet-strafvorderlijke normering is van belang. Niet om het politiewerk te begrenzen, maar om legitiem politiewerk mogelijk te maken. •

Jeroen van den Broek
Criminoloog en buitenpromovendus
en ondersteunt partijen binnen het jeugdveiligheidsdomein
op de thema's straatcultuur, social media en jeugdcriminaliteit

Klaar voor de virtuele straat van 2033?

Tien jaar geleden studeerde ik af op een onderzoek met de titel *Van de straathoek naar Facebook*, over hoe straatcultuur – paradoxaal genoeg – steeds meer vorm en invulling kreeg op social media. Jongeren gebruikten anno 2013 platforms als Twitter, YouTube en Instagram om zichzelf een reputatie van *jongen van de straat* aan te meten. Zo zinspeelden ze onder andere op het gevaar van hun buurt, hun bereidheid tot het gebruik van geweld of hun op straat verdiende vermogen. De digitalisering van straatcultuur heeft zodanig doorgezet dat we inmiddels – tien jaar later – kunnen spreken van een 'hybride straat': een context waarin de fysieke buitenruimte en het online domein dwars door elkaar heen lopen en in constante wisselwerking met elkaar verkeren. De digitale wereld maakt anno 2023 een integraal onderdeel uit van de levens van straatgeoriënteerde jongeren. Het biedt hun niet alleen een podium voor het construeren en communiceren van specifieke straatreputaties, maar voorziet ook nadrukkelijk in mogelijkheden voor het plegen van (deels) gedigitaliseerde straatdelicten. De centrale rol die het online domein inneemt in de leef- en belevingswereld van deze doelgroep, maakt deze context een onmisbaar onderdeel van het politiewerk.

De **hybride werkelijkheid** waarin jongeren zich bewegen écht **doorgronden**

In de afgelopen tien jaar ben ik binnen mijn werk talloze enthousiaste politiecollega's tegengekomen die deze noodzaak inzagen en die zich inspanden om beter aan te sluiten op deze nieuwe werkelijkheid. Keer op keer zag ik echter ook hoe deze collega's zich maar weinig aangemoedigd en gefaciliteerd voelden vanuit de hogere lagen van de organisatie. Eigenlijk lijkt er pas de afgelopen jaren momentum te zijn binnen de politie om wezenlijke veranderingen door te voeren op dit thema. Hoewel het inherent is aan de taak van de politie om – soms vrij letterlijk – achter de feiten aan te lopen, vind ik dat de digitaliseringsslag binnen de politie te lang op zich heeft laten wachten. Bovendien dienen er nog serieuze stappen te worden gezet om de hybride werkelijkheid waarin jongeren zich anno 2023 bewegen écht te doorgronden en hierop aan te sluiten.

De digitalisering van straatcultuur raast ondertussen in volle vaart door en lijkt voorlopig nog niet tot stilstand te komen. Sterker nog: het is niet ondenkbaar dat we in 2033, opnieuw tien jaar verder, onder invloed van de stormachtige ontwikkeling van technologieën als *artificial intelligence* en *virtual reality*, te maken krijgen met een straatwereld die in grote mate is *gevirtualiseerd*. Ik zou er persoonlijk in ieder geval niet van opkijken als de context van de straat tegen die tijd deels is verworden tot een virtuele wereld waarin de *avatars* van straatgeoriënteerde jongeren met elkaar rondhangen, ruzie zoeken, dader én slachtoffer worden van criminaliteit, onveiligheid veroorzaken en geweld plegen. Om te voorkomen dat we tegen die tijd opnieuw moeten concluderen dat we onvoldoende hebben ingespeeld op de veranderende werkelijkheid, zou het goed zijn ons nu alvast te buigen over de vraag hoe de politie de virtuele straat van 2033 het hoofd gaat bieden. En wat we daarbij kunnen leren van de afgelopen tien jaar.

“Kunstmatige intelligentie gaat onderdeel van ons werk worden”

Pim Takkenberg is algemeen directeur van Northwave BeNeLux. Northwave helpt middelgrote en grote organisaties in een ’safe digital journey’ bij het opzetten en onderhouden van een adequate beveiliging van hun informatie en business continuïteit. Hiervoor heeft Pim jarenlang teams geleid bij Team High Tech Crime van de Landelijke Eenheid en binnen de AIVD.

Floor Jansen combineert haar achtergrond in de sociale wetenschap, criminologie en computer science om High Tech Crime te bestrijden. Ze doet dit als teamleider van de Cyber Offender Prevention Squad (COPS); het daderpreventieteam van de Dienst Landelijke Recherche dat zij drie jaar geleden heeft opgezet. Daarnaast vervult zij de rol van plaatsvervangend teamchef van de afdeling Thematisch 1, waar THTC ook deel van uitmaakt.

Redactieleden Maud van Bavel en Stan Duijf gingen met hen in gesprek.

Tekst: Maud van Bavel & Stan Duijf • Fotós: Barbara Vreekamp Fotografie, Maarn

En de eerste vraag was wat de term 'Policing the Internet' bij hen oproept.

Floor: "Voor mij geeft het vooral het hiaat weer van waar we zouden willen staan en waar we nu staan. *Policing the Internet* is nu vooral opsporing, waar mogelijk aanhouden en anders verstoren, terwijl policing op straat veel breder is dan alleen opsporing. Op straat doen we als politie ook veel aan handhaving, aan preventie en surveilleren. Dat doen we online veel minder. Dat is precies een van de redenen waarom ik het daderpreventieteam ben gestart. Daarmee kijken we naar alle facetten van het politiewerk, waar preventie en verstoring ook onder vallen. Het Team High Tech Crime is een hele innovatieve omgeving waar veel nieuwe initiatieven ontstaan. Daar proberen we de hele organisatie in mee te krijgen, juist ook de blauwe diensten. We hebben natuurlijk digitale wijkagenten die op die manier bijdragen, maar ook zij zijn letterlijk gebonden aan een wijk; het internet is natuurlijk niet gebonden aan wijken of beperkt tot landgrenzen. Dus welk stukje van het internet valt dan onder zo'n wijkagent, wat zijn de bevoegdheden, wat is het hele juridisch kader waaruit je werkt? Dat zijn vragen waarop we het antwoord nog aan het formuleren zijn. Daarbij kijken we ook welke verantwoordelijkheid bij welk deel van onze organisatie ligt, en wat ligt er dan bijvoorbeeld bij de private sector, de gemeente?"

Pim: "*Policing the Internet* klinkt als een oplossing die klaarblijkelijk nodig is. Als je teruggaat naar de essentie, heeft het internet een dimensie gecreëerd in onze samenleving die we voor die tijd nog niet kenden. We kenden lucht, land, ruimte en water. Daar waren de regels vrij helder. Het internet werd het vijfde domein. Daarin is typisch dat tijd en afstand relatief zijn. Ze zijn er wel, maar hebben weinig waarde. Dat maakt ook dat IT-infrastructuren en digitalisering van data logisch zijn in het dagelijks gebruik; het betekent ook dat we hele andere vraagstukken voor ons krijgen. Vroeger had je iemand die jou afperste omdat ze iets gezien of gehoord hadden. Tegenwoordig hack je een bedrijf en pers je ze op die manier af. Het gaat om geld verdienen, maar de manier waarop zich dat openbaart is anders en daarin geeft het internet allerlei nieuwe kansen. Daar moet je op kunnen inspelen. Ik heb het idee dat de ontwikkelingen over het gebruik in de samenleving zo hard gaan, dat de manier waarop we daar de juiste kaders aan mee zouden willen geven om het ook een veilig deel van onze samenleving te laten zijn bemoeilijkt

> "Laten zien dat de politie ook **online aanwezig** is"

wordt. Het is een vraagstuk waar we nog lang niet over uit zijn. De wijkagent van nu heeft minder te maken met twee jongens die een meisje lastig vallen en een paar straten verderop wonen, maar des te meer met een foto die wordt gedeeld op Snapchat. Is de wijkagent die de melding krijgt dan zelf wel bij machte om passend op te treden?"

Floor: "Het is een heel geschaald probleem, iets wordt heel snel heel groot. Met een druk op een knopje heb je bij wijze van spreken duizend slachtoffers in plaats van één. Daar moet je als politie – en dus ook als overheid en bedrijfsleven – een schaalbaar antwoord op vinden. En dat is nog een zoektocht. Bovendien zijn we als politie niet schaalbaar ingericht, als het gaat om het digitale domein."

Pim: "Dat is binnen Nederland al ingewikkeld. Maar het is natuurlijk een internationaal vraagstuk; het stopt niet bij de grens. Soevereiniteitsbeginselen zijn nog steeds vrij dominant aanwezig en dat past niet meer goed bij hoe deze wereld werkt. We zullen met fundamenteel andere visies moeten komen om het ook op een andere manier te gaan bestrijden. Om terug te gaan naar het voorbeeld: een meisje wordt via Snapchat gevraagd om een filmpje te maken en op te sturen. Dat filmpje wordt vervolgens gedeeld met anderen, daar wordt melding van gemaakt. Het formele traject omvat heel veel stappen. Als buurtregisseur moet je dan gewoon snel kunnen schakelen met Snapchat, zodat dat account geblokkeerd kan worden. Die lijnen behoren net zo kort te zijn in het oplossen van het probleem als het ontstaan ervan. Daar ligt ook een hele interessante discussie over wie waar verantwoordelijkheid voor draagt."

Floor: "Dit voorbeeld gaat ook op voor meer High Tech Crime-varianten, zoals *ransomware*.

Over de auteurs
Maud van Bavel is onderzoeker bij Team Analyse & Onderzoek van de eenheid Amsterdam.
Stan Duijf is sectorhoofd Dienst Regionale Intelligenceorganisatie (DRIO) Oost-Brabant.

Op het moment dat een bedrijf wordt aangevallen en gijzel-software wordt geplaatst, ben je als opsporing eigenlijk al te laat. Eerst wordt Pim erbij geroepen, die gaat de brand blussen en onderhandelen, en wij proberen daarna uit te vinden wie het gedaan heeft. Vaak kom je bij een internationale infrastructuur uit en dat beperkt de mogelijkheden voor de opsporing. Daarom moet je veel breder kijken dan incident en opsporing: dat is natuurlijk een soort reflex vanuit de recherche. Uiteindelijk wil je op verschillende manieren een dader stoppen. Vervolging en opsporing zijn daar heel belangrijk in, anders wordt het een soort *Wild West*. Je moet bijten én blaffen: bijten is af en toe nodig, anders heeft het blaffen weinig zin. Zeker op het gebied van cyber moeten we als politie soms wat meer blaffen en meer aan die voorkant zitten. Daarmee maak je ook meer impact dan met zo nu en dan een aanhouding verrichten waar we drie jaar naartoe hebben gewerkt. *Policing the Internet* kan op heel veel manieren. Opsporing en vervolgen zijn het meest tijdsintensief, voorkomen is een essentiële en efficiënte toevoeging hieraan."

Pim: "Wat je breder wilt, is dat criminaliteit stopt. Hoe je daar komt, maakt niet zoveel uit. En dat werkt pas als je eerst heel goed snapt hoe criminaliteit zich openbaart: wie is de threat actor, wat is zijn intentie, zijn motivatie, zijn capabilities, zijn werkmethodiek? Als je dat goed begrijpt, kan je daarna bezien op welke onderdelen van het strafbare feit je in staat bent om iets te doen, en wie daar iets in kan betekenen. Dat kan best verrassend zijn: dat bedrijven in de eerste fase enkele maatregelen nemen om minder kwetsbaar te zijn bijvoorbeeld, of dat in de laatste fase de politie in het buitenland bepaalde dingen stuk kan maken. Daar zie je ook steeds meer initiatieven voor met crime-scripting, en daar moeten we in dit domein veel meer naartoe want hier heeft elke partij een stukje van de puzzel in handen."

Hoe is het team ooit tot stand gekomen?

Pim: "Het Team High Tech Crime is opgericht in 2006, in eerste aanleg als een team van 33 mensen. Voor die tijd is het een pilotproject geweest om te kijken of het zou kunnen werken. Toen ging het voornamelijk om een meer gespecialiseerd team dat bepaalde vormen van cybercrime zou kunnen opsporen. Er is vanaf dag één hard gevochten om er een team van te maken waarin klassieke recherchecapaciteit gecombineerd werd met technische capaciteit. Bij het opzetten van zo'n team begonnen de dilemma's bij het juridisch kader. Het werd daarnaast ondergebracht in een bestaande structuur terwijl er ook bijzondere elementen aan zitten: veel experts van buitenaf, die niet goed begrijpen hoe de klassieke politieorganisatie werkt. Dat bood ook kansen voor de mensen die vanuit een ander perspectief en andere achtergrond een wezenlijke bijdrage konden leveren aan het geheel."

Floor: “We trekken mensen aan die het werk mooi en spannend vinden. Daarnaast zien we dat de private sector concurrerend werkt voor wat betreft de salariëring. We missen ook doorgroeimogelijkheden: deze mensen zijn dan ‘executief-specifieke inzet’ (ESI), daar hebben we heel veel briljante mensen op aangenomen, waarvan sommige ook leidinggevende capaciteiten hebben. Het zou voor het team ook gezond zijn om vanuit die ESI-kolom leiding te laten geven. Ook de rest van de organisatie zou ik dat ontzettend gunnen, maar dat is niet mogelijk.
Er zijn ook nieuwe uitdagingen. Toen Pim begon, was het een nieuw team en moest je aan collega’s nog uitleggen wat cybercrime was. Nu is het bijna het tegenovergestelde. Alle criminaliteit digitaliseert, de maatschappij digitaliseert. Wij moeten dus blijven nadenken over de vraag waar wij het verschil kunnen maken.”

Wat zijn voor jullie sprekende voorbeelden van THTC-successen?

Pim: “We hebben in meerdere onderzoeken gezien dat Russische criminelen veelal westerse bedrijven aanvielen en in Nederland infrastructuur misbruikten. Ze communiceerden hiervoor via een chatprotocol genaamd ICQ. We hebben toen met zes à zeven landen samengewerkt en een tap kunnen plaatsen die al het verkeer filterde. Dat is een aanpak en methodiek die toen ongekend was, ook in de rest van de wereld. Een ander mooi voorbeeld was het onderzoek Bredolab. Daar werd een groot bot-net binnen Nederland gedraaid en dat hebben we kunnen overnemen. We hebben vijftigduizend machines op afstand een kleine update gegeven om de kwaadaardige software te deinstalleren en een berichtje op het scherm achtergelaten.”

Floor: “Een vergelijkbaar en recenter voorbeeld is Hansa Market, waar we een maand lang een darkwebmarkt hebben gerund. Heel vaak halen we dingen neer. Dat is op zich effectief maar niet heel duurzaam, want er komt steeds weer iets nieuws voor in de plaats. In dit onderzoek wilden we het vertrouwen van criminelen doorbreken. Dus als je het hebt over ‘Policing the Internet’, is

> “Een **zorgpunt** is dat **wetgeving** enorm **achterloopt**”

dit een mooi voorbeeld. Je laat hiermee zien dat de politie ook online aanwezig is. Je weet nooit waar ze zijn, je weet nooit met wie je praat. Hetzelfde geldt voor onze onderzoeken naar crypto-communicatie. Er is ontzettend veel informatie uitgehaald waarbij je als team ook ten onder kan gaan aan je eigen succes. Met het achterhalen van de data van crypto-communicatiediensten verkrijgen we informatie die voor wel twintig jaar aan recherchewerk oplevert. Het is bijna onmogelijk om al die informatie op te pakken dus met Artificial Intelligence (AI) proberen we daar ook slimmere keuzes in te maken."

Hoe zien jullie de samenwerking met private instanties?

Pim: "Zowel de publieke als de private sector houdt zich bezig met criminaliteitsbestrijding. Soms is het verstandig dat wanneer je effectief wil zijn over het geheel, er samenwerkingsverbanden worden opgezet. Dat kan waardevolle informatie opleveren of juist leiden tot effectieve uitkomsten. Het mag wel wat intenser. Nu ik aan de andere kant zit, probeer ik meer samenwerking op te zoeken. Het bedrijfsleven moet ook een steentje bijdragen om ervoor te zorgen dat het online wat veiliger wordt. De private sector heeft natuurlijk inzichten die de politie niet heeft, en andersom. We hebben direct contact met slachtoffers, maar praten ook met de criminelen, wat weer waardevolle informatie en inzichten oplevert."

Floor: "Het is vaak spannender voor de private kant. Er is terughoudendheid om aangifte te doen, waarbij vooral de vraag speelt: wat gaat die aangifte mij op dit moment opleveren? Er is brand en je wilt dat die geblust wordt, dus je belt de brandweer (Pim) en niet de politie. Maar wil je uiteindelijk uitzoeken wie die brand heeft aangestoken, dan zal de politie toch meegenomen moeten worden. En als wij dan niet als eerste ter plaatse worden geroepen, zien wij heel graag dat Pim – als brandweer – sporen veiligstelt. We moeten het wel weten, willen we die pyromaan uiteindelijk achterhalen. En het is voor een bedrijf nog steeds lastig om toe te geven dat ze zijn aangevallen, hoewel het eigenlijk een kwestie van *wanneer* is, en niet *óf* je bedrijf wordt aangevallen."

Pim: "Ik zie twee dingen vanuit de private sector. Ten eerste dat bedrijven niet zo goed weten wat ze aan de politie hebben. Dan heeft een aangifte minder prioriteit. Of dat ze bang zijn dat er bemoeienis komt en dat dat impact heeft op het tempo en de manier waarop ze als bedrijf kunnen herstellen. Ze zijn toch bang

dat een stuk van de regie wordt overgenomen. Daarin moeten beide partijen gewoon het gesprek aangaan."

Floor: "En het is ook niet alleen het opsporen. We hadden onlangs een groot *ransomware*-onderzoek waarbinnen aangifte is gedaan door een aantal mensen. Daardoor hebben we op een zeker moment de betalingen kunnen terugdraaien en zijn bestanden terug verkregen. Dan leidt een aangifte bij de politie daadwerkelijk tot schadeherstel, maar dat moet wel bekend zijn.
Het is mooi om te benoemen dat de private sector ook aan het einde van de keten weer instapt. Bijvoorbeeld het Hack Right-programma is een re-integratie project voor *first offenders* in cybercrime. Daarbinnen zijn koppels gemaakt van reclassering met mensen uit de private sector, die jongeren begeleiden zodat zij in de toekomst andere keuzes gaan maken."

Welke (technische) uitdagingen signaleren jullie voor de komende jaren?

Floor: "Het gebruik van AI is juridisch lastig. We hebben het idee dat alles wat politiemensen doen door een rechter goed gecheckt kan worden. Maar wat doet AI eigenlijk precies? Is het *self-learning* of voeden wij het model? Dat zijn juridisch en ethisch interessante vraagstukken. We kunnen in de toekomst niet zonder: dat gaat onderdeel van ons werk worden. En encryptie is een continue ratrace: zij doen het beter, wij doen het beter. Een zorgpunt is wel dat wetgeving enorm achterloopt."

Pim: "Op technisch vlak maak ik me niet zo'n zorgen. Dat is een kwestie van de juiste mensen aannemen. Wetgeving is een ander vraagstuk. De samenleving gaat sneller dan wat de politiek kan bijbenen. Dat zie je ook als je kijkt naar processen en structuren binnen organisaties zoals de politie en de wetgeving. Die moeten goed genoeg mee kunnen gaan, zodat wat er in de praktijk gebeurt binnen de juiste kaders geplaatst kan worden en dat de juiste toetsing kan plaatsvinden. Er moet ook veel meer nagedacht worden over Europese en wereldwijde frameworks. Dat kan zelfs betekenen dat een dienst als Europol uitvoerende bevoegdheden zal krijgen."

> "Als politie moet je **kijken** hoe de criminaliteit van **nu** en de **toekomst** eruitziet"

Wat betekent dat voor de politie en THTC in de toekomst?

Floor: "De toekomst vraagt in mijn optiek om andere keuzes. We zijn nu heel erg bezig met het digitaal vaardiger maken van het bestaande personeelsbestand. We moeten kritischer, eerlijker kijken naar hoe de toekomst van ons personeelsbestand eruitziet. Als politie willen we altijd meer mensen. Maar je moet soms ook mensen kiezen die niet alle politietesten halen door over dingen heen te springen, maar die wel digitaal vaardiger zijn. En ook door te kijken naar een nieuwe generatie die misschien een andere achtergrond heeft. Als politie moet je maatschappelijk meebewegen en kijken hoe de criminaliteit van nu en de toekomst eruitziet. En natuurlijk wat daarop ons antwoord is."

Nieuwe kennis en vaardigheden in het politiewerk

De samenleving digitaliseert en dus ook het politiewerk. Hierbij kan worden gedacht aan de opsporing van klassieke delicten en nieuwe vormen van criminaliteit die door digitalisering zijn ontstaan. Denk aan oplichting en illegale drugshandel die inmiddels ook via het internet plaatsvinden tot hacking en het verspreiden van computervirussen (Oerlemans & Van der Wagen, 2021). Maar in een gedigitaliseerde samenleving met het internet als infrastructuur verandert niet alleen een deel van de criminaliteit en de opsporing hiervan, ook andere aspecten van het politiewerk krijgen hierdoor een nieuwe invulling.

Over de auteurs
Melvin Soudijn is als operationeel expert D verbonden aan de Landelijke Eenheid, DLIO, van de Nationale Politie.
Marc Schuilenburg is werkzaam als bijzonder hoogleraar Digital Surveillance aan de Erasmus Universiteit Rotterdam en aan de Vrije Universiteit Amsterdam.

Inmiddels helpen op lokaal niveau digitale wijkagenten burgers bij aangiftes van cybercriminaliteit of marktplaatsfraude en zijn specifieke afdelingen als Team Rendement Operationele Informatie (TROI) opgericht om digitale tools te ontwikkelen waarmee bijvoorbeeld in beslag genomen data kunnen worden geanalyseerd met betrekking tot thema's zoals witwassen en drugshandel.

Op zoek naar nieuwe kennis en vaardigheden

Een gedigitaliseerde samenleving, en de politie die hierin meebeweegt, leidt tot de vraag welke nieuwe vormen van kennis en vaardigheden hiervoor nodig zijn. In antwoord hierop hebben wij tussen maart 2021 en maart 2023 periodiek alle vacatures op de wervingssite www.kombijdepolitie.nl doorgenomen met het oog op functieomschrijvingen die in verband kunnen worden gebracht met digitaal politiewerk. Zoektermen die hierbij zijn gebruikt, zijn onder meer 'cyber', 'internet', 'digitaal' en 'big data'. Dit leverde ruim honderdvijftig geschikte advertenties op. In dit artikel doen we verslag van de uitkomst van de analyse van deze vacatures. Voordat we de resultaten daarvan bespreken, geven we eerst een beknopt overzicht van veranderingen in de laatste decennia in de kennis en vaardigheden van politiewerk.

Veranderingen in kennis en vaardigheden

Voor een doeltreffend handelen van de politieprofessional zijn onder meer kennis, kunde en beheersing van het gebruikte instrumentarium noodzakelijk. Dat gaat gepaard met specifieke competenties en vaardigheden. In de literatuur wordt een onderscheid gemaakt tussen startbekwaamheid en vakbekwaamheid. Startbekwaam betekent dat iemand bevoegd en bekwaam is om te starten in een politiefunctie. Wil dezelfde persoon ook vakbekwaam zijn, dan zullen hiervoor in de praktijk de nodige uren ervaring moeten worden opgedaan. Op die manier wordt kennis direct

toegepast tijdens het werk waarbij er ruimte moet zijn om daarop te reflecteren. Belang van een goede opleiding is hiervoor een van de vereisten. Hoewel hierin steeds meer verandering komt, staat de politie van oudsher bekend als een praktische mbo-organisatie.

Het is lastig specifieke uitspraken te doen over de kennisbasis van het politiewerk. Daarvoor zijn de functies en bijbehorende competenties binnen de Nationale Politie te uiteenlopend. Met betrekking tot de maatschappelijke trend van digitalisering wordt in wetenschappelijk onderzoek wel gewezen op veranderingen die zich hierbij hebben voorgedaan in de uitoefening van de politietaak vanaf het einde van de jaren 1990, zowel op epistemologisch als op methodologisch niveau (Hannah-Moffat, 2019). Daarbij wordt gewezen op de aanvankelijk grote invloed van psychologische kennis in de strafrechtketen met betrekking tot de inzet van zogeheten actuariële instrumenten. Instrumenten waarmee risico's kunnen worden voorspeld op het gebied van criminaliteit en recidive. Deze actuariële risicotaxatie-instrumenten worden over het algemeen op een 'evidence-based' manier ontworpen en hebben duidelijke wortels in de klinische praktijk. Wetenschappelijke verklaringen voor het plegen van criminaliteit en recidive, zoals persoonskenmerken van daders en slachtoffers staan hierbij centraal.

De opkomst van het internet als nieuwe gelegenheidstructuur in het algemeen en het gebruik van big data en algoritmes in de opsporing in het bijzonder leidt tot een ander perspectief op politiewerk. Inmiddels is een technisch-economische benadering dominant geworden, waarbij wordt verondersteld dat digitale tools om de politietaak uit te voeren efficiënter en objectiever zijn dan door psychologische kennis geïnformeerde instrumenten. Deze digitale transformatie heeft ook consequenties op de werkvloer waarbij andere vormen van kennis, vaardigheden en bijbehorend gedrag van politiemensen noodzakelijk worden geacht. Dat maakt de vraag relevant welke competenties dit zijn en voor welke functies ze binnen de politieorganisatie worden gevraagd.

Resultaten onderzoek

Tot ongeveer 2014 was het beleid binnen de politie dat 'digitaal' géén specialisme is. Uitzondering daarop is het team High Tech Crime (HTC) dat op landelijk niveau opsporingsonderzoek doet naar digitale criminaliteit en nieuwe vormen van cybercrime, waaronder hacks en gijzelsoftware (Stol, 2018). Inmiddels is hierin flink verandering gekomen, zo blijkt uit de vacatures die we de afgelopen twee jaar hebben geanalyseerd. We zullen hiertoe de volgende aspecten behandelen die met veranderingen in politievaardigheden op digitaal vlak te maken hebben: functies, competenties, geografische spreiding en opleiding/schaal.

> De **opkomst** van het **internet** leidt tot een **ander perspectief** op **politiewerk**

Functies

Het eerste dat opvalt, is dat de vacatures een zeer grote variatie, een smörgåsbord, aan functieomschrijvingen laten zien. Er is simpelweg weinig uniformiteit in de functietitels te ontdekken. Alleen de functies van 'data engineer', 'netwerkontwerper' en 'test specialist' keren meerdere malen terug. Neem een term als 'digitaal'. Het blijkt dat er een 'digitale rechercheur netwerken en *the internet of things*' wordt gezocht, een 'digitaal rechercheur mobile & smart devices', een 'digitaal specialist automotive en embedded systems', en een 'landelijk digitaal coördinator'. Soms wordt er in de advertenties op een bepaald onderdeel van digitaal werk een accent gelegd, zoals de functietitels 'lead engineer cloud & big data', 'productlijnmanager cloud & big data', 'delivery manager cloud & big data' en een 'solution architect cloud & big data' laten zien.

Het lijkt wellicht vreemd dat er een grote verscheidenheid aan functietitels optreedt, maar dat is het niet wanneer ook naar de omschrijving van de functie wordt gekeken. Dan blijkt dat de invulling van de functie toch telkens anders is. Enerzijds omdat een bepaald politieonderdeel op zoek is naar

Literatuur

- Hannah-Moffat, K. (2019). 'Algorithmic Risk Governance: Big Data Analytics, Race and Information Activism in Criminal Justice Debates'. *Theoretical Criminology, 23*(4), 453-470.
- Oerlemans, J-J. & Van der Wagen, W. (2021). Types of cybercrime and their criminalisation., In: W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (eds.), *Essentials in cybercrime. A criminological overview for education and practice*, The Hague: Eleven International Publishing, pp. 53-97.
- Schuilenburg, M. & Soudijn, M. (2021). Big data in het veiligheidsdomein: Onderzoek naar big data-toepassingen bij de Nederlandse politie en de positieve effecten hiervan voor de politieorganisatie, *Tijdschrift voor Veiligheid, 20*(4), 44-62.
- Schuilenburg, M. & Wessels, M. (2022). Vier handvatten voor betrouwbare algoritmische toepassingen in het politiewerk. *Het tijdschrift voor de politie*, 3, 11-15.
- Stol, W. (2018). Politiewerk is … werken in een digitale samenleving, *Tijdschrift voor de Politie, 80*(5), 22-25.
- WRR (2021). *Politiefunctie in een veranderende omgeving*, Den Haag.

Digitale **expertise** komt ook terug in het **werk** op **straat**

specifieke eisen, anderzijds omdat het werk op uiteenlopende vakgebieden moet gaan plaatsvinden. Deze vakgebieden, zo blijkt uit de advertenties, zijn grosso modo onder te verdelen in varianten van procesmatige dan wel operationele intelligence, analyse, bedrijfsvoering of advies. Hierdoor blijft de digitale expertise niet beperkt tot de opsporing van online- en cybercriminaliteit, maar komt ze ook terug in intelligence en het werk op straat (Schuilenburg & Soudijn, 2021).

Competenties/vaardigheden

Op het gebied van competenties komen de vacatureteksten meer overeen. In de vacatures worden specifieke technische vaardigheden als het beheersen van bepaalde programmeer- of scripttalen zoals Python, Linux, HTML of Javascript gevraagd. In diverse functies wordt met big data gewerkt, waardoor ook kennis en ervaring met relevante (computer)programma's wordt gezocht. Het gaat dan om vaardigheden met betrekking tot ElasticSearch, Kubernetes, Hadoop of Graph databases. Een illustratie hiervan is de werving van een operator die verschillende hardware en software gaat gebruiken, waaronder Raspberry PI's, zelfgebouwde tools en C2-frameworks.
Kijken we over specifieke eisen als affiniteit met bepaalde programmeertalen of systemen heen, dan blijkt dat de boventoon in de vacatures wordt gevoerd door een vaardigheid om samen te werken. De vacatures geven aan dat kandidaten in specifieke teams zullen worden gestationeerd die gezamenlijk aan bepaalde producten of doelstellingen werken. Verder wordt verwacht dat kennis en ervaring met collega's wordt gedeeld of, waar nodig, wordt bijgesprongen. Hierbij komt een stuk communicatievaardigheid kijken. Er wordt gesproken over 'afstemmen', 'informeren' en 'terugkoppelen' met afnemers (personen in het werkveld) en opdrachtgevers. Net als in het leger is politiewerk een kwestie van teamwerk en kan een sterk gevoel van saamhorigheid kweken. In die zin kan bij de digitale vernieuwing nog steeds het oude *corps d'esprit* worden teruggevonden.

Er ontstaat een grote discretionaire **ruimte** voor software **developers** en **netwerkontwerpers**

Geografische variatie en opleiding/salarisschaal

De analyse van de vacatures toont dat in alle politieregio's naar digitale vaardigheden wordt gevraagd. De digitale vernieuwing binnen de politie blijft dus niet beperkt tot een centraal hoofdkantoor ergens op de achtergrond, maar vindt in alle geledingen in de organisatie en in alle regio's plaats. Dat neemt niet weg dat er bepaalde concentraties zijn te vinden, zoals in Driebergen of Utrecht. Dat is te verklaren omdat op deze plekken specialistische politieeenheden zitten die zich met de bestrijding van high-tech crime (HTC) bezighouden of een dienstencentrum (TROI) herbergen.
Door de digitalisering van de politiefunctie is er ook meer vraag naar hoogopgeleid personeel binnen de organisatie ontstaan. Het aantal hoger opgeleiden in de politie neemt hierdoor gestaag toe. Uit de vacatures spreekt duidelijk een voorkeur voor minimaal een hbo-opleiding, en in enkele gevallen is zelfs een wo-opleiding een vereiste. De salariëring is dan ook navenant ingeschaald, met gemiddeld een startbedrag op schaal 10 of 11 (ongeveer 3.000, resp. 3.700 euro bruto) tot senior experts in schaal 13. Ter vergelijking: een beginnende surveillant op straat wordt binnen de Nationale Politie ingedeeld in schaal 6 (2.245 euro).

Conclusie en discussie

De Wetenschappelijke Raad voor Regeringsbeleid (2021) schrijft dat het internet '*underpoliced*' is en dat digitaal politiewerk vraagt om andere kennis van politiemedewerkers. Op basis van de geanalyseerde vacatures kunnen we vier ontwikkelingen voor de politiepraktijk afleiden. Ten eerste behelst de digitalisering van het politiewerk veel meer dan alleen nieuwe

manieren van rechercheren, zoals de inzet van cyberspecialisten in de opsporing van online-criminaliteit. De digitalisering vindt juist over de gehele breedte van de politieorganisatie plaats, van de klassieke handhaving op straat en de opsporing tot intelligence en ondersteunende functies, die gericht zijn op optimalisatie van de interne bedrijfsvoering.
Ten tweede valt op dat de digitalisering zeer specialistische kennis vergt in bepaalde politiefuncties, waaronder beheersing van verschillende programmeertalen en skills om nieuwe digitale tools te ontwerpen, maar dat deze kennis doorgaans wordt ingebed in een breder kader en onderling een wisselwerking tussen developers, management en gebruikers op de werkvloer stimuleert. Dit lijkt op het eerste gezicht geen bijzondere constatering, maar hierbij moet wel het volgende worden gerealiseerd: dergelijke specialistische kennis maakt al te strakke sturing en managementmethoden lastig en zal in de praktijk leiden tot een grote discretionaire ruimte voor bepaalde politiefuncties, zoals in het geval van 'software developers' en 'netwerkontwerpers'. Dat maakt de vraag relevant hoe de leiding van de politie op hun werk kan sturen, bijvoorbeeld bij het ontwerp van nieuwe tools voor de opsporing van criminaliteit. Aan deze tools worden vanuit nationale en internationale regelgeving namelijk steeds meer eisen gesteld in relatie tot publieke waarden zoals non-discriminatie en algoritmische verantwoording (Schuilenburg & Wessels, 2022).
Een derde constatering is dat digitalisering niet op één plek binnen de organisatie plaatsvindt, maar in alle Nederlandse politieregio's wordt opgepakt. Dat is een positieve ontwikkeling, maar tegelijk roept de verscheidenheid aan functies de vraag op in hoeverre de leiding van de Nationale Politie erin slaagt inhoud te geven aan de vraag wat en op welke plek er precies nodig is om de digitalisering van de politiefunctie eigen te maken.
Ten vierde jaagt de digitale transitie van de politie de werving van hoger opgeleid personeel aan. Daarbij wordt het kennisniveau standaard gezocht op hbo- en zelfs op universitair niveau. Dit is in overeenstemming met de oude ambitie om het percentage hoger opgeleiden en specialisten binnen de politie fundamenteel te verhogen. De keerzijde hiervan is dat personeel met een mbo-opleiding hun promotiekansen zien verminderen. Hier zit dan ook een winstwaarschuwing die aan de digitalisering van de politieorganisatie moet worden meegegeven. Handhavers kunnen op straat nog zoveel digitaal worden ondersteund, uiteindelijk moeten er wel mensen zijn die 'met hun poten in de modder' durven te staan. •

> Politiewerk is een kwestie van **teamwerk** en kan een sterk gevoel van **saamhorigheid** kweken

VIJANDIGE STAAT OF NEDERLANDSE PUBER; DE SCHADE IS EVEN GROOT

De kracht van daderpreventie

De opkomst van het internet, handige apps en technologische snufjes heeft de manier waarop we leven, werken en communiceren volledig veranderd. Hoewel deze ontwikkelingen veel voordelen hebben opgeleverd, hebben ze ook voor nieuwe uitdagingen gezorgd.

Zo brak er in 2018 in Nederland grote paniek uit, omdat websites van de belastingdienst en Nederlandse banken niet meer bereikbaar waren door DDoS-aanvallen. Cybersecurityexperts en overheden wisten het zeker; het zijn de Russen! Maar niets bleek minder waar; het ging om de 18-jarige Jelle die op de computer op zijn zolderkamer deze netwerken platlegde voor de lol. Wanneer rechercheurs geconfronteerd worden met een delict met zoveel impact en motieven die zodanig uit verhouding zijn, komt al snel de vraag naar boven: hoe had dit voorkomen kunnen worden?

Het antwoord op deze vraag wordt gegeven door de Cyber Offender Prevention Squad: COPS. Dit multidisciplinaire team onder leiding van Floor Jansen[1] bestaat uit personen met verschillende specialismen zoals criminologie, psychologie, gedragswetenschappen en digitale expertise. Al drie jaar zijn zij bezig met het voorkomen en doorbreken van cybercriminele carrières. De COPS heeft als doel individuen die online grenzen opzoeken of zich schuldig maken aan cybercriminaliteit te weerhouden en te verwijzen naar positieve alternatieven. Bij bewuste daders tracht het team online reputaties en criminele markten te verzwakken en te verstoren. Zo wordt schade voorkomen en de rechtsketen ontlast, terwijl talent behouden blijft voor de samenleving.

Van dweilen naar de kraan repareren

De preventieve aanpak richting daders van cybercrime is van cruciaal belang om verschillende redenen:

- *Cybercrime stijgt*: met het ontstaan en de snelle ontwikkeling van het digitale tijdperk is cybercriminaliteit een grote bedreiging geworden voor zowel individuen als bedrijven. En de cijfers liegen niet: we zien dat traditionele criminaliteit daalt, terwijl cybercrime stijgt. Met de toenemende afhankelijkheid van technologie en het internet hebben criminelen nieuwe manieren gevonden om kwetsbaarheden in onlinesystemen uit te buiten om verschillende online misdrijven te plegen, van diefstal en fraude tot intimidatie en afpersing.[2]
- *Andere motieven*: de motieven van cybercriminelen blijken anders te zijn dan die van traditionele criminelen. Vaak zijn jonge hackers op zoek naar uitdaging en testen ze graag hun vaardigheden door de grenzen op te zoeken.[3] Dit vraagt om een andere aanpak dan bij het traditionele type dader. De interventies die gebruikt worden in de bestaande aanpak voor traditionele criminaliteit, sluiten niet goed aan bij de behoeften van cyberdaders.
- *De impact van cybercrime is groot*: in tegenstelling tot offline misdaden vergroot de schaalbaarheid van cybercriminaliteit de

Over de auteur
Nicole Mulder is interventiespecialist bij de Landelijke Eenheid. Ze maakt deel uit van het Team High Tech Crime en Cyber Offender Prevention Squad (COPS). Voor meer informatie: daderpreventie@politie.nl.

Tekst: Nicole Mulder

schade van elke aanval. Geavanceerde tools, ontwikkeld door technisch handige daders, zijn zo simpel in gebruik dat elke jongere hiermee enorme schade aan de samenleving kan toebrengen. Deze 'plug-and-play-tooltjes' worden online openlijk aangeboden, waardoor het plegen van cybercrime voor iedereen toegankelijk wordt.

- *Het wereldwijde web is net het Wilde Westen*: online regels zijn onduidelijk en er is nauwelijks toezicht. Dit laatste maakt dat jongeren zich anoniem wanen op het internet, met alle gevolgen van dien. De politie grijpt pas in bij grote incidenten, tijdige bijsturing van de criminele carrières ontbreekt.
- *Skills*: veel daders die cybercrime in enge zin plegen (denk aan malware, phishing etc.), hebben specifieke skills. En laten dit nou net de skills zijn waar ze in de publieke en private industrie enorm veel behoefte aan hebben. Daarom is het van belang dat deze personen hun skills niet voor de *dark side*, maar juist voor de *bright side* gaan inzetten en daarmee ons land (en de rest van de wereld) een stukje veiliger maken.

Deze argumenten resulteren in de vraag naar een nieuwe aanpak voor deze vorm van criminaliteit. Het voorkomen van cybercriminaliteit is kritiek voor wetshandhavingsinstanties, overheden en organisaties over de hele wereld. Want, zoals Loesje stelt: "Het is gewoon lekkerder dweilen als je weet dat ondertussen tenminste iemand probeert de kraan te repareren."

De aanpak

Het COPS-team heeft als doel om zo efficiënt en effectief in te grijpen in het ontwikkelingspad van cyberdaders. Met als motto: *hoe efficiënter en effectiever we ervoor zorgen dat de kraan gemaakt is, hoe minder men achteraf hoeft te dweilen.* Daarom hebben de COPS voor elke vorm van preventie interventies ontwikkeld. De COPS maken onderscheid tussen primaire, secundaire en tertiaire preventie.

> **Preventie** zonder opsporing is **machteloos**, maar **opsporing** zonder preventie is **eindeloos**

Primaire preventie omvat interventies die gericht zijn op de gehele populatie. Het gaat hierbij om iedereen die actief is online, van jong tot oud. Voorbeelden van primaire preventie van cybercriminaliteit zijn verschillende interventies om jongeren te wijzen op de gevaren van het internet, zoals de cybergame Framed. Framed speelt zich af op school. Om te testen hoe ver leerlingen gaan voor vriendschap, worden ze op de proef gesteld en krijgen ze een aantal keuzes voorgelegd. Door de keuzes die leerlingen maken, zoals het wel of niet doorsturen van een filmpje met inloggegevens of door cijfers te veranderen in het schoolsysteem, komen ze erachter dat hun online gedrag ernstige gevolgen kan hebben. En dat zij ook op een gewone schooldag slechts één klik verwijderd zijn van cybercrime. Daarnaast werkt het COPS-team ook aan het ontwikkelen van een educatietoolkit voor wijkagenten, docenten en ouders. Deze tool heeft als doel om hen te informeren over de verschillende mogelijkheden die er zijn voor jongeren met een interesse in cybersecurity en/of hacking, zodat ze weten waar ze jongeren naar kunnen doorverwijzen. Ouders, docenten en wijkagenten kunnen op persoonlijk vlak bij deze jongeren een groot verschil maken door een luisterend oor te bieden en hen te ondersteunen in de digitale wereld.

Secundaire preventie focust op personen die nog geen cybercrime hebben begaan, maar

1 Floor Jansen, teamleider bij het Team High Tech Crime (THTC) van de Nationale Politie, combineert haar expertise als criminoloog, sociaal wetenschapper en cybersecurity-expert om een integrale aanpak te hanteren bij het bestrijden van cybercrime. Haar multidisciplinaire achtergrond stelt haar in staat om problemen vanuit verschillende perspectieven te benaderen, wat resulteert in effectieve oplossingen voor complexe uitdagingen. Lees het interview met haar elders in deze editie van *Tijdschrift voor de Politie*.

2 https://www.nu.nl/tech/6247440/bijna-drie-keer-zoveel-gevallen-van-cybercrime-in-2022-als-voor-coronapandemie.html

3 Weulen Kranenbarg, M., Ruiter, S., Gelder, J. van & Bernasco, W. (2018). Cyber-Offending and Traditional Offending over the Life-Course: An Empirical Comparison. *Journal of developmental and life-course criminology, 4*(3), pp. 343-364.

Het **COPS-team** is onderdeel van Team High Tech Crime van de landelijke eenheid, maar heeft in de afgelopen jaren een nationaal en internationaal cybercrime daderpreventienetwerk opgebouwd met interne en externe partners vanuit de publieke en private sector. Het internationale en nationale netwerk heeft een gedeelde visie en verantwoordelijkheid. Als aanvoerder van zowel het nationale als het internationale netwerk zien de COPS dat er behoefte is aan het werk dat zij leveren en de resultaten die zij boeken. Het COPS-team is nu nog een projectteam, daarom wordt er hard gewerkt aan de borging van het gedachtegoed door dit team en om deze werkwijze een vaste plek te geven binnen de politieorganisatie.

De **motieven** van **cyber-criminelen** blijken **anders** te zijn dan die van **traditionele** criminelen

wel het risico vormen om dit in te toekomst te gaan doen. Het doel is om risicofactoren te verminderen en beschermende factoren te versterken. Het gaat hierbij om jongeren die bijvoorbeeld al online gamen en zich op hackerfora bevinden. Het COPS-team heeft twee secundaire interventies ontwikkeld. Zowel in de fysieke als in de online sfeer. Door gebruik te maken van Google Ads ontmoedigen de COPS startende cyberdaders door advertenties te laten verschijnen wanneer jongeren zoeken naar informatie over het plegen van cybercriminaliteit, zoals DDoS-aanvallen. Wie op de advertentie klikt, wordt doorgestuurd naar een landingspagina van de politie waar de gevolgen van deze delicten worden uitgelegd en positieve alternatieven worden aangeboden. Zo loopt er al een Google Ads-campagne sinds 2021, met inmiddels 227.300 impressies en 16.640 kliks. Verschillende wetenschappers doen onderzoek naar het effect van deze campagne.

De re_BooTCMP is een dag-event voor jongeren tussen twaalf en vijfentwintig jaar met interesse en skills op het gebied van IT. Tijdens deze dag geven experts uit de IT en Gaming-industrie presentaties en leren de jongeren over toekomstkansen in deze branches. De politie leert hen over de grenzen van de wet en de online sporen die zij achterlaten, terwijl ze ook een potje kunnen gamen met de politie. Aan het einde van de dag is er een *challenge* waar de jongeren worden uitgedaagd om hun skills te testen en waar de winnaar met een prijs naar huis gaat. Ouders en docenten zijn ook welkom en krijgen informatie en tips over hacken en hoe ze het gesprek kunnen aangaan met hun kind/student. Inmiddels hebben zeven re_BooTCMP's plaatsgevonden met zo'n tweehonderdtwintig jongeren en negentig ouders/docenten. Er zijn al meerdere succesverhalen, zoals één van de winnaars van de challenge die nu bij een van de cybersecuritybedrijven werkt en één andere winnaar die zich bij de club cyberspecials van de politie heeft gevoegd.

Tertiaire preventie richt zich op daders van cybercrime, met als doel het voorkomen van recidive en behoud van hun skills voor de samenleving. Voorbeelden hiervan zijn de interventies 'Cease & Desist' en 'Hack_Right'. Cease & Desist is een interventie die bestaat uit het voeren van stopgesprekken en het versturen van waarschuwingsberichten. Het doel van Cease & Desist is het tijdig waarschuwen van (potentiële) jonge daders op het gebied van cybercrime. Hack_Right is een interventie voor jonge first offenders (twaalf tot drieëntwintig jaar, met uitzonderingen tot dertig jaar) die voor een eerste cyberdelict worden vervolgd. Binnen Hack_Right werken Politie, het Openbaar Ministerie, Halt, de Raad voor de Kinderbescherming en de (jeugd)Reclassering samen met bedrijven vanuit de cybersecurity- en ICT-sector. Binnen het traject worden de jongeren enerzijds begeleid vanuit de publieke sector en anderzijds vanuit de private sector. Vooral dit laatste is van groot belang omdat juist de begeleiders uit de private sector deze jongeren op het gebied van hun skills het beste begrijpen en kunnen begeleiden. Het doel is om deze jongeren passende begeleiding te bieden om herhaling van daderschap te voorkomen en het inzetten van talent voor positieve alternatieven te stimuleren. Veel van de deelnemers hebben een studie in de IT-richting gekozen en een paar zijn gaan werken bij hun begeleidende bedrijf.

Investeren in preventie loont

Het is wel duidelijk; cybercrime is een groeiend probleem dat niet alleen door opsporing opgelost kan worden. De Cyber Offender Prevention Squad (COPS) ontwikkelt, implementeert en borgt interventies om potentiële daders te stoppen. Preventie is schaalbaar, efficiënt en betaalbaar. Door te investeren in preventie wordt opsporing het ultimum remedium, zoals bij offline criminaliteit. De COPS werken samen met onder meer het ministerie van justitie en veiligheid, gemeentes, cybersecuritybedrijven en het onderwijs, omdat daderpreventie een gedeelde verantwoordelijkheid is. Samen zetten zij zich in voor effectieve bestrijding door preventie en opsporing op elkaar af te stemmen. De politie draagt bij vanuit hun speciale informatiepositie en taakstelling, omdat daderpreventie nauw samenhangt met opsporing en verstoring. Blijf je zelf maar dweilen en wil je ook wel eens de kraan repareren? Wil je meer weten van preventie? Of zelf bijdragen aan de (borging) van daderpreventie binnen de politie organisatie? Neem dan contact met ons op.

Steven De Smet
(Ere)hoofdcommissaris Politie
auteur van 'Hooligans' (Davidsfonds 1996),
'De nieuwe politie' (LannooCampus 2012) en 'Quantumveilig' (LannooCampus 2022)

Overleeft 'de' politie het digitale tijdperk?

Nieuwe media, het nieuwe normaal, het nieuwe werken… Tien jaar geleden schreeuwden we al dat het allemaal 'nieuw' diende te zijn. Wat betekent 'nieuw' nog in deze razendsnel wijzigende wereld? Mijn hele, 43-jarige, loopbaan werd beheerst door twee grondslagen: vechten tegen onrechtvaardigheid en strijden voor open en eerlijke communicatie.
Laat het nu juist de technologische ontwikkelingen, met onder meer sociale media, zijn die op dit gebied een nieuwe dimensie geven aan ons werk.
Zoals de politie (B) nu echter te werk gaat, houdt ze (te) weinig rekening met de tendensen en ontwikkelingen in de digitale maatschappij. De politie deelt haar informatie (te) weinig. Ze houdt strenge controle op alle data in haar beheer en geheimhouding is quasi heilig. Ze volgt duidelijk afgebakende grenzen, waar iedereen binnen de lijntjes moet kleuren. Virtueel bestaat (nog) niet en wordt dus ook niet opgenomen in de politiewerking. De pen blijft het belangrijkste wapen. Kortom, de mentaliteit waarmee politiewerk gedaan wordt, is sinds de jaren zeventig van de vorige eeuw niet al te veel geëvolueerd.
Dit kan niet meer. Zowel in de reële als in de virtuele wereld dringen nieuwe spelregels zich op. Als ik eerlijk ben, moet ik toegeven dat ze ook mij af en toe afschrikken. Soms vraag ik me af of ik het allemaal nog wel snap en waarom alles toch zo verduiveld snel moet gaan. Maar dan draai ik mijn knop om en zie ik in elk vraagteken een spannende uitdaging.
Noodzaak aan een sterke mentaliteit, die we met de politie kunnen inzetten wanneer we zowel de traditionele als de nieuwe media bekijken. Een verbeterde politiecultuur die ons helpt om de interactie met partners te verhogen, die het praten met burgers makkelijker maakt en daardoor burgerparticipatie versterkt. Ondertussen moeten goede politiezorg en operationele werking topprioriteit blijven door nadruk te leggen op functionaliteiten binnen de organisatie, zodat de politie garant blijft staan voor een gevoel van vertrouwen en maatschappelijke veiligheid.

> De politie houdt (te) **weinig rekening** met de **tendensen** en ontwikkelingen in de **digitale** maatschappij

Een mens is een sociaal wezen. Alleen kan je niet overleven, het is enkel in relatie met anderen dat je een menswaardig bestaan opbouwt. De mens neemt daarvoor een identiteit aan die hem rechten en plichten verleent. In de digitale wereld is dat net zo en kun je ook een identiteit nemen of verwerven en dit geldt voor elke organisatie die het digitaal tijdperk wil overleven… ja, ook de politie! Digitalisering betekent dat de politie zich op een andere manier verhoudt tot de burger, kennis op een andere manier verkregen en/of gegeven wordt en dat er andere talenten nodig zijn.
Het directe contact met de burger zou het kenmerk moeten zijn van de dagelijkse verrichtingen.
Het is niet Über die de taxisector disrupteert, het is niet Airbnb die de hotelsector doet wankelen… Er werd een platform gecreëerd en doordat wij, als burger, er gebruik van maken verstoren we de oude industriële structuren.
Wat als men een platform maakt in 'safety & security'?
Voor mij is het niet de vraag of dit platform er komt, maar wanneer?
Laat ons, eindelijk, met de ervaringen van overmorgen werken aan de politie van vandaag.

Recensies over actuele publicaties

BOEK

De ongelijke strijd tegen de zware misdaad

H. Werdmölder (2023). *De ongelijke strijd tegen de zware misdaad. Opsporing, bestrijding en vervolging.* Walburg Pers: Zutphen, 200 pagina's, ISBN 9789464560480

Nederland is de **belangrijkste** "drugs**rotonde** ter **wereld**" geworden

De vraag die centraal staat in dit boek is: wat gaat er precies mis in de strafrechtketen? Het antwoord luidt: een heleboel.

Hoewel Nederland in de loop der jaren veiliger is geworden, geldt dit volgens criminoloog en cultureel antropoloog Hans Werdmölder niet voor de gevolgen van de georganiseerde en ondermijnende criminaliteit. In een beschouwing van de afgelopen dertig jaar beschrijft de auteur wat de strijd tegen de zware misdaad in Nederland 'ongelijk' maakt door in te zoomen op de pakkans, de vervolgingskans, de sanctiekans en de strafmaat, oftewel: opsporing, bestrijding en vervolging.

Het eerste deel van het boek richt zich op de slagkracht van de politie, en met name de recherche, waarbij Werdmölder zich grotendeels lijkt te baseren op het boek 'De gekooide recherche' van Michiel Princen. De capaciteit is gering, maar ook de kwaliteit schiet tekort in de aanpak van de georganiseerde misdaad, zo stelt hij. En terwijl het OM worstelt met een hoge werkdruk, verouderde registratiesystemen en een personeelstekort, signaleert de auteur een steeds groter wordende kloof tussen burgers en de rechterlijke macht. Er klinkt hierbij een terugkerend pleidooi voor het invoeren van minimumstraffen en het toepassen van snelrecht.

Oude bekenden zoals Holleeder passeren de revue, maar er is ook aandacht voor de nieuwe aanwas en verharding binnen de drugscriminaliteit. Kroongetuigen lijken inmiddels niet meer uit het strafproces weg te denken. Ook kijkt Werdmölder voorbij de landgrenzen, naar de effectiviteit van de misdaadbestrijding in Europese buurlanden. Hoewel er in Nederland aanmerkelijk strenger bestraft wordt dan voorheen, is de kans op vervolging en berechting door de lage pakkans en vele sepots gering, aldus de auteur. Wat betekent dat voor de geloofwaardigheid van de strafrechtspraak?

Al deze factoren – en meer – maken dat Nederland de belangrijkste "drugsrotonde ter wereld" is geworden; een paradijs voor buitenlandse criminelen. Drugszaken zijn de grootste werkverschaffer voor justitie. Er is aanvullende wetgeving nodig, meent de auteur, en harmonisatie van strafwetgeving op Europees niveau voor een probleem dat bij uitstek grensoverschrijdend is.

In slechts tweehonderd pagina's wordt veel materie behandeld. Met hoofdstukken getiteld 'Laag prestatieniveau van de recherche', 'De ondraaglijke lichtheid van het Nederlandse strafklimaat' en 'Soft beleid werkt niet tegen harde misdaad' steekt Werdmölder zijn mening niet onder stoelen of banken. Het boek leest op momenten dan ook als een – weliswaar stevig onderbouwde – reeks columns met een scherp randje: de toon is af en toe fel en de kritiek op de (falende) Nederlandse misdaadbestrijding groot.

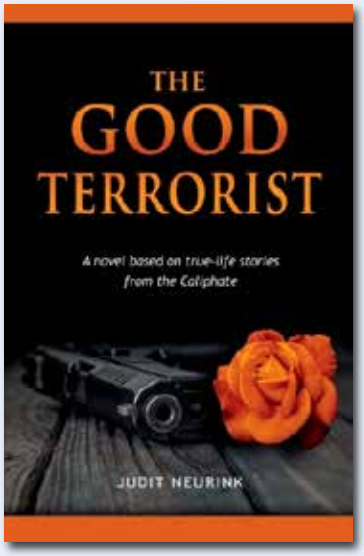
Recensent dr. **Maud van Bavel** is onderzoeker bij Politie Nederland.

BOEK

The Good Terrorist

J. Neurink (2022). *The Good Terrorist: A novel based on true-life stories from the Caliphate.* Onafhankelijke uitgave, 240 pagina's, ISBN 9798847506564

In de Engelstalige novel *The Good Terrorist* beschrijft Neurink vier verschillende verhaallijnen geïnspireerd door de waargebeurde verhalen van mensen verblijvend in en vluchtend van het Kalifaat. Als lezer word je onmiddellijk geboeid, omdat het boek als het ware midden in het verhaal begint. In deel I van het boek volgen we Rose, een jonge docente wonende in Amsterdam. Na haar scheiding leeft ze een rustig leven tot dit bruut verstoord wordt door een foto op Twitter van haar ex-man Ahmed als martelaar in Syrië. Samen met Ahmeds beste vriend Sam en zijn oudste zoon Mustafa probeert Rose er gaandeweg achter te komen wat er met haar ex-man gebeurd is en hoe hij bij IS terecht is gekomen. Al snel wordt de lezer meegenomen in de emoties van de verschillende personages. De wanhoop, maar vooral het onbegrip is voelbaar bij het karakter van Rose, waardoor je als lezer steeds nieuwsgieriger wordt naar wat er met Ahmed is gebeurd en wat zijn beweegredenen zijn geweest.



In deel II krijgt de lezer een inkijkje in Ahmeds kant van het verhaal door middel van een dagboek dat hij voor Rose heeft bijgehouden tijdens zijn verblijf in het Kalifaat. Hier komen we erachter dat Ahmed zijn jongste zoon Fuad achterna is gereisd om hem te bevrijden van IS. Waar Fuad in de eerste twee delen wordt neergezet als een harteloze extremist en terrorist, krijg je als lezer in deel III juist meer begrip voor dit karakter. Door ook een deel van het boek vanuit het oogpunt van Fuad te vertellen, toont Neurink de kant van het verhaal die in de media vaak onderbelicht blijft. De menselijke kant van terroristen vormgegeven in het karakter van Fuad brengt nuance aan in het verhaal en schept hierbij een beter beeld van de angsten en onzekerheden van jonge IS-strijders.

Een belangrijke rode draad in het boek is het netwerk dat Ahmed met zijn tot slaaf gemaakte Yazidi-vrouw Dua heeft opgezet. Samen bevrijden ze verschillende Yazidi-vrouwen, wat ook een zeker element van spanning aan het boek toevoegt. Ook laat deze verhaallijn weer een andere kant van de situatie in het Kalifaat zien en belicht het de helden die daar hebben geopereerd tussen de hardcore IS-strijders. Uiteindelijk komen alle verhaallijnen samen in deel IV, verteld door de ogen van de Yazidi-vrouw Amina. Hierdoor geeft Neurink een inkijkje in de wereld van mensenhandel, seksueel misbruik, vluchten en angst.

Ondanks de verschillende invalshoeken van het verhaal blijven de personages wat oppervlakkig en soms zelfs stereotyperend. De connectie tussen alle personages laat de verschillende verhaallijnen mooi bij elkaar komen, maar is her en der wel net te toevallig en onrealistisch. Desondanks verwerkt Neurink haar ervaring en expertise in een vermakelijk en makkelijk leesbaar boek, dat een goed inzicht geeft in het leven van mensen in het Kalifaat.

Het boek schept een beter **beeld** van de **angsten** en **onzekerheden** van jonge **IS**-strijders

Recensent **Maaike Beemsterboer** is tutor voor het bachelorprogramma Security Studies aan de Faculteit Governance and Global Affairs – Institute of Security and Global Affairs van de Universiteit Leiden.

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.

Bestorming van het Amerikaanse Capitool op 6 januari 2021

Online desinformatie als voorbode van geweld

EEN ROL VOOR DE POLITIE?

Desinformatie: op internet kom je het overal tegen. Vooral op sociale media worden de vreemdste onwaarheden gedeeld, vaak met verwijzing naar vage websites. In principe is dat geen zaak voor de politie; we kennen immers vrijheid van meningsuiting en we mogen tot op zekere hoogte roepen wat we willen. Maar wat als desinformatie tot criminele activiteiten leidt? Door het detecteren en monitoren van desinformatie kan de politie mogelijk vroegtijdige signalen verkrijgen over bijvoorbeeld te verwachten geweld.

Online **desinformatie** kan mensen verleiden zich in te laten met **mensenhandel**

Een bekend voorbeeld zijn de Capitool-rellen in de Verenigde Staten van januari 2021. Opgejut door desinformatie die toenmalig president Donald Trump en een groep mensen om hem heen via vooral sociale media verspreidden, bestormde een grote groep mensen het gebouw. Doel daarvan was een parlementaire bijeenkomst te verstoren waarin Joe Biden zou worden erkend als winnaar van de presidentsverkiezingen. Tijdens de bestorming vielen vijf doden, onder wie een politieagent, en vele gewonden, onder wie 138 politieagenten. Achteraf is het de vraag of de politie wel voldoende was voorbereid op de rellen (Woodruff Swan & Lippman, 2021).

Aanzetten tot criminaliteit

De Capitool-rellen zijn een uitzonderlijk voorbeeld, omdat de desinformatie werd verspreid door de president van de Verenigde Staten zelf. Hij beweerde dat de verkiezingen waren gemanipuleerd en suggereerde dat zijn volgelingen daarom moesten optrekken naar het Capitool. Meestal zijn de daders van opruiende desinformatie van een andere aard, zoals extremistische individuen of groeperingen. Regelmatig leidt online desinformatie tot geweld, bijvoorbeeld omdat het mensen aanzet tot rellen of zelfs terroristische aanslagen. Online desinformatie kan echter ook aanzetten tot andere criminele activiteiten, bijvoorbeeld door mensen te verleiden zich in te laten met mensenhandel.

Vervolging van mensen die desinformatie verspreiden, is heel lastig. Vaak verschuilen verspreiders van desinformatie zich achter anonieme websites en socialemedia-accounts. En als ze niet anoniem zijn, blijkt het ook lastig om ze aan te pakken. In Nederland werd bijvoorbeeld Willem Engel, voorman van actiegroep Viruswaarheid, in januari 2023 grotendeels vrijgesproken van opruiing door het verspreiden van desinformatie voorafgaand aan demonstraties tegen het coronabeleid (Reijmer, 2023).

Het recht op vrijheid van meningsuiting weegt, terecht, vaak zwaar. Maar dat betekent niet dat de verspreiding van desinformatie geen aandacht behoeft van de politie. Het detecteren en monitoren van online desinformatie zou goed kunnen helpen bij het voorspellen van crimineel gedrag, zoals gewelddadige rellen, extremistische aanslagen, grootschalig vandalisme of mensenhandel. Als de politie beter zou zijn voorbereid op de bestorming van het Capitool, om dat voorbeeld opnieuw te gebruiken, zouden de relschoppers wellicht veel minder kwaad hebben kunnen aanrichten.

Europees onderzoek

In veel Europese landen merken politiediensten dat er soms online desinformatiecampagnes voorafgaan aan ongeregeldheden.

Over de auteurs
Beatrice Cadet MSc is klinisch psycholoog en werkt als expert cyber en information bij TNO.
Kimberley Kruijver MSc is onderzoeker strategische veiligheidsvraagstukken bij TNO.
Sico van der Meer MA is verbonden aan de unit Defensie & Veiligheid van TNO.

> Politiediensten hebben meestal niet de **menskracht** om de enorme **vloed** aan online **informatie** op effectieve wijze **bij** te **houden**

Maar hoe precies die online desinformatie effectief kan worden gemonitord, blijft een lastige vraag. Met geld van de Europese Unie is daarom in 2023 een meerjarig internationaal onderzoeksproject gestart om te bekijken of er praktische mogelijkheden bestaan om online desinformatie te gebruiken als 'voorspeller' van ongeregeldheden. In het project 'VIGILANT' werken diverse Europese politiediensten, onder andere uit Estland, Griekenland en Spanje, samen met een aantal onderzoeksinstituten in Europa. Vanuit Nederland neemt onderzoekinstituut TNO aan het project deel (VIGILANT, 2023).

In het project wordt geprobeerd om een softwareapplicatie te ontwikkelen die het voor politiediensten mogelijk maakt om online desinformatie te detecteren en te monitoren. De applicatie moet daarbij aan enkele cruciale randvoorwaarden voldoen: het monitoren mag de politie niet te veel menskracht kosten, moet bruikbare en voor de politie relevante inzichten opleveren, en tegelijkertijd voldoen aan alle ethische en juridische eisen op het gebied van privacy en andere wetgeving. Dat zijn geen eenvoudige randvoorwaarden, want aan het detecteren en monitoren van online desinformatie door de politie zitten enkele serieuze haken en ogen.

Problemen

Een eerste lastige vraag is hoe de monitoring effectief kan plaatsvinden, gezien de enorme stortvloed aan sociale mediaberichten die dan moet worden geanalyseerd (en bij voorkeur zo snel mogelijk, om niets aan actualiteit te verliezen). Aan de ene kant lijkt detecteren en monitoren van online desinformatie nuttig om vroegtijdig te kunnen inspelen op daaruit voortvloeiende criminele activiteiten. Maar aan de andere kant hebben politiediensten meestal niet de menskracht om de enorme vloed aan online informatie op effectieve wijze bij te houden. Dit probleem is waarschijnlijk op te lossen door het inzetten van speciaal ontwikkelde software.

Een ander, nog groter probleem is dat het monitoren van online desinformatie door de politie kan leiden tot schending van privacywetgeving wanneer online uitingen van willekeurige burgers worden bijgehouden. Dit kan ook effect hebben op de publieke opinie over de politie, het zou bijvoorbeeld wantrouwen kunnen aanwakkeren en door sommige mensen kan de politie als 'Big Brother' worden gezien. Een vergelijkbare situatie deed zich voor toen de Koninklijke Landmacht tijdens de coronacrisis begon met een experiment om sociale media te monitoren om daarmee ongeregeldheden te kunnen voorspellen. Dit leidde tot ophef, het stilleggen van het experiment en zelfs een officiële onderzoekscommissie die onder meer concludeerde dat de landmacht met deze werkwijze privacywetgeving

Literatuur

- Onderzoekscommissie Land Information Manoeuvre Centre (LIMC) (2022). 'Grondslag Gezocht', https://www.rijksoverheid.nl/documenten/rapporten/2023/01/13/rapport-onderzoekscommissie-brouwer-naar-het-land-information-manoeuvre-centre-limc
- Reijmer, L. (2023). 'Rechter acht slechts 1 van de 6 uitspraken van Viruswaarheid-kopman Willem Engel strafbaar, vrijspraak voor de overige 5', *De Volkskrant*, 20 januari 2023, https://www.volkskrant.nl/nieuws-achtergrond/rechter-acht-slechts-1-van-de-6-uitspraken-van-viruswaarheid-kopman-willem-engel-strafbaar-vrijspraak-voor-de-overige-5~bdf925a0/
- VIGILANT (2023). https://www.vigilantproject.eu/
- Woodruff Swan, B., & Lippman, D. (2021). 'New Capitol Police document shows how unprepared they were for Jan. 6 riots', *Politico*, 29 October, https://www.politico.com/news/2021/10/29/capitol-police-documents-unprepared-jan-6-riots-517478

had geschonden (Onderzoekscommissie Land Information Manoeuvre Centre, 2022).
Tot op zekere hoogte zou men kunnen volhouden dat het monitoren van uitingen van burgers op het internet in Nederland uitsluitend een taak kan zijn van de inlichtingendiensten AIVD en MIVD. Die diensten staan onder voortdurend toezicht van de Toetsingscommissie Inzet Bevoegdheden (TIB) met betrekking tot burgerrechten en proportionaliteit van het onderzoek. Dat zou betekenen dat er geen rol voor de politie is weggelegd bij het detecteren en monitoren van desinformatie.
Toch lijkt het wel degelijk nuttig om na te denken over ethische en juridische kaders waarbinnen de politie aan detectie en monitoring van online desinformatie kan doen zonder dat dit tot de schending van privacy leidt. Zo wordt nu onderzocht of er wellicht minder problemen aan dergelijke monitoring vastzitten als online informatie niet wordt bekeken op het niveau van individuele internetgebruikers, maar uitsluitend op geaggregeerd niveau (dat wil zeggen de grote lijnen van de uitingen bij elkaar). Denk bijvoorbeeld aan het monitoren van agressieve, haatzaaiende en/of opruiende berichten op het niveau van groepsfora, in plaats van op het niveau van individuele leden van die fora. Zorgvuldigheid is hierbij uiteraard een absolute noodzaak.

Conclusie

Het detecteren en monitoren van online desinformatie kan politiediensten helpen om beter voorbereid te zijn op criminele activiteiten zoals rellen en geweld. Maar aan dat detecteren en monitoren zitten wel wat haken en ogen. Naast de enorme stortvloed aan socialemediaberichten die moet worden geanalyseerd, zijn er vooral ook juridische en ethische dilemma's aan verbonden. Mogelijk kunnen deze problemen worden omzeild door de ontwikkeling van een softwareapplicatie die online informatie niet op individueel niveau maar op groepsniveau monitort en op basis daarvan voorspellingen kan doen over mogelijke aankomende ongeregeldheden. Dit kan een stukje van de oplossing zijn voor het probleem waar politiediensten in vele democratische landen mee worstelen: hoe bereik je een gezond evenwicht tussen veiligheid enerzijds en vrijheid van meningsuiting anderzijds?

Dr. Peter Klerks
Docent aan de Politieacademie en Raadsadviseur Parket-Generaal, Openbaar Ministerie

Onmisbare jeugd

Vroeger had je jeugdcriminaliteit en serieuze criminaliteit. Dat was overzichtelijk; bij jeugdige verdachten ging het vooral om straatdelicten en de jeugdagent of -officier probeerde dan crimineel afglijden te voorkomen. 'Echte boeven' waren volwassen, want moordenaars, drugshandelaren en fraudeurs kwamen vaak pas op latere leeftijd strafrechtelijk in beeld.

Anno 2023 plaatsen 'street soldiers' van veertien jaar springladingen bij doelwitten in drugsconflicten. Amper meerderjarige jongens werken als huurmoordenaar voor drugsnetwerken of verdienen goudgeld in de cokehandel. Van de aangehouden cybercriminelen is de helft jonger dan 22. Ze proberen als 'F-Gamer' met cyberfraude snel veel geld te verdienen voor een *bling-bling* lifestyle. Terwijl het aantal jeugdige verdachten sinds jaren daalt, neemt de ernst van de delicten verontrustende vormen aan.

Moeten die *kids* het tegen **killers** en **drugsmiljonairs** opnemen?

Gelukkig staan tegenover die uitdagingen ook ambitieuze jongeren. Ik heb het geluk kennis en ervaring te mogen overdragen op jonge collega's. Zo verzorg ik enkele keren per jaar samen met hippe specialisten de zelf ontwikkelde les 'Verrassend rechercheren'. Het gaat dan over psychologische misleiding en nieuwe technieken zoals ChatGPT. We praten de aankomende recherchekundigen bij over handige politie-apps en onvoorspelbaar opsporen. Het enthousiasme in deze lessen is aanstekelijk.

Ook operationeel is er veel jeugdige dynamiek, zoals bij een klapdag van het Team High Tech Crime afgelopen februari. Het lukte hen opnieuw om maandenlang live mee te kijken bij een internationale cryptocommunicatiedienst. Ditmaal ging het om Exclu, waarvan duizenden criminelen gebruik maakten. Bij doorzoekingen op tientallen locaties waren zes Europese landen betrokken. Computers werden draaiend in beslag genomen en per koerier naar de locatie gebracht waar ze worden uitgelezen. Daarnaast werden drugs, vuurwapens en miljoenen aan cash in beslag genomen. Dan is het natuurlijk hard werken; 5 x 9 met ook nog een dozijn overuren is niet ongewoon. Het salaris van jonge rechercheurs houdt nog altijd niet over, maar je werkt wel aan topzaken met de grootste criminelen en over de hele wereld. Die kick maakt veel goed, en zulke zaken zijn er steeds vaker. De Nederlandse politie scoorde in april opnieuw met operatie *Cookie Monster*. Samen met onder meer de FBI werd de cybermarktplaats Genesis aangepakt, die zich vermoedelijk in Rusland bevindt. Deze actie was vooral gericht op het belemmeren van handel in gestolen *passwords*. Volgens Europol zou Genesis anderhalf miljoen computers middels virussen hebben gehackt.

Eerlijk gezegd verbaas ik me soms over de studenten die ik voor me krijg. Er hangt een beertje aan hun rugzak, ze zijn druk bezig met mode, sociale media en gamen. Velen zijn veganist en drinken vooral thee. Moeten die *kids* het tegen killers en drugsmiljonairs opnemen? Maar vergis je niet: ze zijn slim, nieuwsgierig en wereldwijs. We mogen blij met ze zijn, want ze zijn keihard nodig om de nieuwe criminaliteitsfenomenen te kunnen aanpakken. Deze mensen denken interdisciplinair en samenwerking is vanzelfsprekend. Ze brengen het opsporingsvak echt verder. Ze zijn bijvoorbeeld geïnteresseerd in de afloop van 'hun' strafzaken en gaan met een officier van justitie in discussie over tactiek en jurisprudentie. Een welgemeend hoera dus voor 'onze' jeugd!

→ Reageren? p.p.h.m.klerks@om.nl

Burgemeester, sheriff van het internet?

Het internet staat vol ongewenste berichten. Deze berichten kunnen uitmonden in opruiing of wanordelijkheden en hebben invloed op de openbare orde. Eenenveertig burgemeesters hebben via *NRC* en de *Volkskrant* aangegeven meer bevoegdheden te willen om ook online (preventief) rellen te kunnen voorkomen. Dat online ingrijpen wordt ook wel aangeduid als internetverbod of online/digitaal gebiedsverbod.[1]

Sommige juristen zien mogelijkheden om het online gebiedsverbod te baseren op de huidige Gemeentewet.[2] De gemeente Amsterdam heeft aangegeven de grenzen daarvan te willen verkennen. Anderen geven aan dat de genoemde artikelen in de Gemeentewet te algemeen en te ruim gedefinieerd zijn. Ook de Algemene Plaatselijke Verordening (APV) als grondslag kent beperkingen.[3] De vraag of een online gebiedsverbod binnen het territoriaal grondgebied van de gemeente valt, wordt weinig problematisch geacht.[4] De burgemeester van de gemeente waar de ordeverstoring zich voordoet of dreigt te gaan voordoen, wordt als bevoegd gezag gezien om daartegen op te treden.

De gemeentepraktijk heeft de onderzoeken niet afgewacht. Zo heeft de raad van de gemeente Almelo eind 2022 als eerste gemeente in Nederland een verbod in haar APV opgenomen om tegen online ordeverstoringen te kunnen optreden.[5] Onlangs floot de Rechtbank Midden-Nederland de burgemeester van Utrecht terug bij het opleggen van de last onder dwangsom, die inhield dat een persoon zich dient te onthouden van online uitlatingen op social media.[6] De burgemeester heeft in maart 2023 laten weten in hoger beroep te gaan tegen de uitspraak.[7]

Uitvoerbaarheid online gebiedsverbod

In deze bijdrage focussen we ons niet op de houdbaarheid van de juridische grondslag om een online gebiedsverbod op te baseren. Als eenmaal via rechtspraak of wetswijziging een juridische basis is gevonden voor het opleggen van een online gebiedsverbod, dan wordt het bij de uitvoering namelijk pas echt spannend. Zolang regels niet uitvoerbaar en handhaafbaar zijn, hebben ze amper nut. Willem Bantema en Mariëtta Buitenhuis publiceerden hier een artikel over in de Gemeentestem.[8] Zij stippen in deze bijdrage de belangrijkste conclusies aan voor wat betreft de onderbelichte perikelen op het gebied van de bekendmaking, de handhaafbaarheid en de randvoorwaarden voor gegevensverwerking. Ook komt aan bod hoe al geplaatste ongewenste content kan worden verwijderd.

Bekendmaking online gebiedsverbod

Eén van de uitdagingen die zich vanuit de bestuursrechtpraktijk bij een online

1 In deze bijdrage hanteren we de term 'online gebiedsverbod'.
2 Artikel 175 Gemeentewet.en Artikel 172, lid 3, Gemeentewet, zie: M. Buitenhuis, 'De burgemeester: burgervader, handhaver van de openbare orde en sheriff van het internet? (deel 1), Kunnen burgemeesters met een internetverbod optreden tegen een verstoring van de openbare orde met aanleiding in het online domein?', *Gst.* 2022/44.
3 Thorbecke Academie NHL Stenden, 'Juridische grenzen en kansen bij openbare orde handhaving – Een onderzoek naar mogelijkheden van de APV voor de aanpak van online aangejaagde ordeverstoringen', 27 oktober 2022.

Over de auteurs
Dr. **Willem Bantema** is lector aan de Thorbecke Academie van NHL Stenden Hogeschool.
Mr. **Mariëtta Buitenhuis** is advocaat bij AKD.

Tekst: Willem Bantema & Mariëtta Buitenhuis • Foto's: Pexels/Tracy LeBlanc/Talha Güney

> Zolang **regels niet uitvoerbaar** en handhaafbaar zijn, kunnen we stellen dat ze **amper nut** hebben

gebiedsverbod voordoen, uit zich bij de bekendmaking. Een probleem hierbij is dat men niet in alle gevallen weet wie er achter het opruiende bericht schuilgaat. Veel mensen die zich op het internet begeven, doen dat anoniem of onder een alias. Het bekendmaken van een online gebiedsverbod zonder te weten wie erachter zit, is uitermate lastig. Daarvoor zal beschikking over naam, adres en woonplaats (hierna: 'NAW-gegevens') een IP-adres moeten worden verkregen. Nu het duidelijk is dat dit persoonsgegevens betreffen, dient voor het delen van deze gegevens een wettelijke grondslag te bestaan. Die kan bijvoorbeeld worden gevonden in een onrechtmatige daad[9] of zal in een separate wettelijke grondslag moeten worden voorzien. Burgemeesters zullen dus niet zomaar beschikking krijgen over de IP-adressen van personen waarvan wordt aangenomen dat zij met hun berichten de openbare orde verstoren.

Wij zijn bekend met de praktijk waarin de politie IP-adressen doorgeeft aan burgemeesters. De vraag is of artikel 11 van de Politiewet hiervoor concreet genoeg is. Hieruit volgt dat indien de politie in een gemeente ter handhaving van de openbare orde en ter uitvoering van de hulpverleningstaak optreedt onder gezag van de burgemeester staat. De burgemeester kan de betrokken ambtenaren van politie daarbij de nodige aanwijzingen geven. Dit geldt ook voor artikel 16, eerste lid onder b, van de Wet politiegegevens. Deze bepaling maakt het voor de politie als verwerkingsverantwoordelijke mogelijk om politiegegevens aan de burgemeester te verstrekken, maar enkel indien de burgemeesters deze behoeven in verband met hun gezag en zeggenschap over de politie, of in het kader van de handhaving van de openbare orde. In ieder geval doet zich hierbij het probleem voor dat wanneer er meerdere personen op één adres wonen, zij doorgaans van hetzelfde IP-adres gebruik zullen maken. Het verkrijgen van het IP-adres zal in dat geval niet voldoende zijn om de overtreder te vinden. Daarvoor zal ook toegang moeten worden verschaft tot de (fysieke) router.

Handhaving online gebiedsverbod

Gemeenten hebben zorgen geuit over de regels rond de handhaafbaarheid van online ordeverstoringen. Een van de routes voor de handhaving van het verbod is de strafrechtelijke, bij de overtreding van een op grond van de APV of de Gemeentewet gebaseerde maatregel.[10] Een andere route is de bestuursrechtelijke handhaving. Daarvoor zal niet kunnen worden ontkomen aan online monitoring. Onlangs bleek uit onderzoek van Bantema dat 95% van de gemeenten aan enige vorm van online monitoring doet, waarbij 60% van de gemeenten dit toepast binnen het openbare orde domein.[11] De ministeries van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en Justitie en Veiligheid

4 Thorbecke Academie NHL Stenden, 'Juridische grenzen en kansen bij openbare orde handhaving – Een onderzoek naar mogelijkheden van de APV voor de aanpak van online aangejaagde ordeverstoringen', 27 oktober 2022.
5 Artikel 2:1b, lid 1, Algemene Plaatselijke Verordening gemeente Almelo; zie Gemeente Almelo, Raad – 29 november 2022, https://ibabsonline.eu/Agenda.aspx?site=Almelo&agendaid=f24ed39d-da52-4af7-a4dd-d031812d595e&FoundIDs=.
6 Rechtbank Midden-Nederland 3 februari 2023, ECLI:NL:RBMNE:2023:375.
7 https://www.ad.nl/utrecht/burgemeester-dijksma-in-hoger-beroep-tegen-besluit-rechter-over-online-gebiedsverbod-17-jarige-jongen~ab701608/
8 M. Buitenhuis & W. Bantema, 'De burgemeester: burgervader, handhaver van de openbare orde en sheriff van het internet? (deel 2), Kunnen burgemeesters met een internetverbod optreden tegen een verstoring van de openbare orde met aanleiding in het online domein?', Gst. 2023/8.
9 Artikel 6:162 BW, zie Gerechtshof Arnhem-Leeuwarden 5 november 2019, ECLI:NL:GHARL:2019:9352; bekrachtigd door de Hoge Raad in HR 25 juni 2022, ECLI:NL:HR:2021:985.

(J&V) publiceren binnenkort een handreiking om het juridisch kader voor online monitoring te verhelderen.[12]
Naast de juridische mogelijkheden en beperkingen rondom online monitoring, spelen er ook organisatorische belemmeringen. Zo blijkt uit onderzoek dat gemeenten zich zorgen maken over de organisatorische capaciteit en specifieke kennis die online monitoring vraagt. Te denken valt aan juridische kennis, maar ook aan de vereiste kennis om online signalen goed te kunnen duiden. Een complicerende factor voor de gemeente is dat soms moeilijk is vast te stellen wie bij online gedrag waar verantwoordelijk voor is. Dat geldt zeker bij online groepsdynamiek.

Randvoorwaarden AVG

Voor het opleggen van een online gebiedsverbod is het noodzakelijk om persoonsgegevens te raadplegen en daarmee verwerken. De politie kent voor de verwerking van persoonsgegevens een eigen regime in de Wet politiegegevens. Bij de verwerking van persoonsgegevens door een burgemeester zal echter aan de Algemene Verordening Gegevensbescherming (hierna: de 'AVG') moeten worden voldaan. Uit de AVG volgt dat de gegevensverwerking noodzakelijk en transparant moet zijn, moet voldoen aan de beginselen van proportionaliteit en subsidiariteit en er documentatievereisten gelden.[13] Verder moet de verwerking voldoen aan de beginselen van doelbinding en moet er een grondslag voor de gegevensverwerking bestaan.
Met name de verwerkingsgrondslag vraagt voor het kunnen opleggen van een online gebiedsverbod aandacht. Voor de verwerking zal moeten worden teruggevallen op de grondslag dat de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.[14] De AVG vereist in dat geval dat deze grondslag moet worden vastgesteld in een wet in formele zin.[15] Wanneer er een enkele keer een online gebiedsverbod wordt opgelegd, kan daarvoor mogelijk een basis worden gevonden in deze al bestaande wettelijke grondslag. Voor het vaker kunnen opleggen daarvan zal een meer specifieke wettelijke grondslag in het leven moeten worden geroepen.

Offline halen ongewenste content

Met het opleggen van een online gebiedsverbod is de reeds geplaatste ongewenste content nog niet van het internet verdwenen.

10 Artikel 184 Wetboek van Strafrecht.
11 W. Bantema e.a., 'Black Box van gemeentelijke online monitoring', 2021.
12 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Monitoring sociale media en naleving AVG door overheden, 29 april 2022. https://www.rijksoverheid.nl/documenten/kamerstukken/2022/04/29/kamerbrief-over-monitoring-sociale-media-en-naleving-avg-door-overheden
13 Artikel 5 AVG.
14 Artikel 6, lid 1 onder e, AVG.
15 Artikel 6, lid 3, AVG.

Daarvoor kan een burgemeester een 'Notice and Take Down' (hierna: 'NTD')-verzoek indienen. Voor het offline halen van de content dient behoorlijk wat aan de hand te zijn. Bij strafbare of onmiskenbaar in strijd met de wet zijnde gedragingen dient het internetplatform binnen maximaal tien dagen op de klacht te reageren. Indien het bericht ernstige schade berokkent, moeten de gegevens soms al binnen 24 uur ontoegankelijk worden gemaakt. De vraag is of dat op tijd genoeg is om op een online aangejaagde ordeverstoring te reageren of om deze te voorkomen. Een ander bekend probleem van de NTD-procedure is dat bepaalde socialemediaplatforms – Telegram is daar een bekend voorbeeld van – zich weinig aantrekken van NTD-verzoeken. De gemeente Bodegraven-Reeuwijk probeerde daarom een platform in een civiele procedure in kort geding te dwingen om onrechtmatige content toch offline te halen. De vordering werd afgewezen, omdat het platform zich volgens de voorzieningenrechter voldoende had ingespannen om de content van het account in kwestie offline te halen.[16] Op dit moment wordt gewerkt aan een register waarin gemeenten ongewenste content kunnen melden, waarna de verzoeken tot offline halen gebundeld kunnen worden ingediend.[17]

> Het bekendmaken van een **online gebiedsverbod** zonder te weten wie achter de gedraging of uitlating **schuilgaat**, zal uitermate **lastig** zijn

Indien er geen gehoor wordt gegeven aan een NTD-verzoek, kan de burgemeester een verzoek indienen bij de Officier van Justitie (hierna: de 'OvJ') om informatie offline te laten halen.[18] De OvJ kan dan met tussenkomst van een rechter-commissaris een communicatiedienst bevelen om bepaalde informatie tijdelijk ontoegankelijk te maken. Een dergelijk verzoek kan enkel worden gericht aan een aanbieder van een communicatiedienst, waar een socialemediaplatform zoals Facebook in beginsel ook onder kan vallen. Platforms kunnen strafrechtelijk vervolgd worden indien zij het bevel niet opvolgen.[19]

Conclusie

De burgemeester zou met de huidige regels of eventueel met aangepaste wetgeving een online sheriff kunnen zijn. Toch blijven er duizend-en-een vragen en obstakels bestaan voor wat betreft de uitvoerbaarheid en handhaving van dergelijke online gebiedsverboden. Zo vereist de AVG bij het herhaaldelijk opleggen van een online gebiedsverbod een specifieke grondslag in een wet in formele zin. Daarnaast bevat het bestuursrecht onvoldoende handvatten om een online gebiedsverbod adequaat bekend te maken aan anonieme personen of personen die zich onder een alias op het internet bevinden. Ook ontbreekt er nog een wettelijke regeling om het online gebiedsverbod te handhaven. De discussie richt zich hier nog onvoldoende op, terwijl die regels en uitvoeringsaspecten juist aandacht zouden moeten hebben bij de eventuele aanpassing van wetgeving.

16 Rechtbank Den Haag 4 oktober 2022, ECLI:NL:RBDHA:2022:10082
17 AG connect, 'Gemeenten hopen op bevoegdheid om online-opruiing aan te pakken', 15 september 2022. https://www.agconnect.nl/artikel/gemeenten-hopen-op-bevoegdheid-om-online-opruiing-aan-te-pakken
18 Artikel 125p Wetboek van Strafvordering.
19 Artikel 54a Wetboek van Strafvordering.

Politieacademie
Police Academy of the Netherlands

GESLAAGD

Aan de Politieacademie studeren jaarlijks vele politiefunctionarissen af. Voor deze rubriek selecteren de opleiders van de Politieacademie enkele boeiende en goed beoordeelde verslagen van afstudeeronderzoeken. De meeste scripties kunnen bij de Mediatheek van de Politieacademie (www.politieacademie.nl/mediatheek) geraadpleegd worden. Publicatie aldaar is afhankelijk van de rubricering van de mate van vertrouwelijkheid. De scripties van onderstaande studenten kunt u rechtstreeks aanvragen via het vermelde e-mailadres.

Nazorg in de basispolitiezorg

Jamie Friesen
jamie.friesen@politie.nl
Bachelor Politiekunde, Politieacademie

Een onderzoek naar de behoeften op het gebied van nazorg na het meemaken van schokkende gebeurtenissen door politiemensen werkzaam in de basispolitiezorg (BPZ). Effectieve nazorg kan psychisch letsel voorkomen of beperken. Het in kaart brengen van de behoeften is belangrijk omdat het aanknopingspunten kan bieden voor het verhogen van de effectiviteit van de geleverde nazorg.

Uit het onderzoek is gebleken dat er vooral behoeften bestaan op emotioneel gebied, maar ook op het gebied van het krijgen van informatie. De emotionele behoeften komen vooral tot uiting in *behoeften aan persoonlijke aandacht, een veilige werkomgeving, erkenning, je verhaal kwijt kunnen en sociale steun.* Op het gebied van informatie hebben de respondenten behoefte aan het *kunnen herkennen van signalen* dat het niet goed met hen of collega's gaat en aan het aanleren van *manieren van zelfbescherming.* Naar aanleiding van de resultaten zijn verschillende aanbevelingen gedaan. Ook bieden de resultaten input voor drs. Bartelds, die in de hoedanigheid van cultureel antropoloog onderzoek gaat doen naar posttraumatische stressstoornis binnen de Eenheid Limburg.

Recherchepsycholoog op de plaats delict

Stella Lemmens
stella.lemmens@politie.nl
Master Criminal Investigation, Politieacademie

Draagt deze functionaris kennis over gedrag bij aan het forensisch onderzoek op de plaats delict? Daar zocht Stella Lemmens een antwoord op voor haar scriptie van de Master of Criminal Investigation.

In vijf eenheden sloten recherchepsychologen aan bij het forensisch onderzoek naar overlijdensonderzoeken. Recherchepsychologen bleken meer contextinformatie te kunnen verschaffen aan de forensisch onderzoekers. Dit draagt bij aan het denken in hypothesen en scenario's en geeft bijvoorbeeld informatie over wie het slachtoffer was. Dit kan van meerwaarde zijn bij onderzoeken waarbij geen eenduidig sporenbeeld is of wanneer forensisch onderzoekers twijfel hebben over de toedracht van het misdrijf of overlijden. Ook bij de uitgebreide forensische onderzoeken (maatwerk+-PD's) zou een recherchepsycholoog waardevolle input kunnen geven. Naar aanleiding van deze resultaten pleit Stella ervoor om de recherchepsychologen en forensisch onderzoekers aan elkaar te verbinden.

Tekst: Politieacademie & Jan van Balkom

Jaco van Hoorn & Maud van Bavel (red.)

Onze politie in een kwetsbare rechtsstaat

Wat leert de eerste tien jaar van de Nationale Politie ons over de komende tien jaar?
Een decennium na de vorming van de Nationale Politie is het tijd om de balans op te maken. Wetenschappers, journalisten en politiemedewerkers blikken in dit boek kritisch terug op de eerste fase van deze nieuwe structuur en bieden een vooruitblik op de toekomst.
De bijdragen geven inzicht in de uitdagingen waarvoor de politie zich gesteld ziet. Een rechtsstaat die in toenemende mate kwetsbaar is, een sluimerende vertrouwenscrisis onder burgers. Maar ook de strijd tegen de georganiseerde misdaad en de digitale stroomversnelling die zowel de boven- als onderwereld raakt.
Hierbij worden verschillende kansen gesignaleerd: in het streven naar meer diversiteit, het groeiende belang van de gebiedsgebonden politiezorg, andere sturing en de rol die kennis zou moeten spelen. Welke keuzes dienen zich aan voor de toekomst? Wat betekent dit voor het leiderschap, ook op strategisch niveau?
De bijdragen in '*Onze* politie in een kwetsbare rechtsstaat' geven richting aan collega's, partners en beleidsmakers die de politie in staat stellen om te kunnen blijven doen waar zij voor staat: waakzaam en dienstbaar zijn aan de waarden van de rechtsstaat.

Thom Snaphaan, Manon Kostense & Teun van Ruitenburg

Financial Crime Scripting

Inzicht in winstgedreven criminaliteit

Financial crime scripting is een nieuwe methode waarmee inzicht wordt verschaft in criminele geldstromen gerelateerd aan winstgedreven vormen van criminaliteit. Voortbouwend op de bestaande methode van crime scripting, die al in de jaren negentig van de vorige eeuw werd geïntroduceerd in de criminologie, is het met deze nieuwe methode mogelijk om kennis over financiële aspecten van specifieke vormen van criminaliteit te ontwikkelen, organiseren en systematiseren. Financial crime scripting vormt op deze manier een vliegwiel voor een intelligence-gestuurde aanpak van criminaliteit.

In dit boek worden de fundamenten en basisprincipes van de methode uiteengezet, worden handvatten en een stappenplan geboden om er concreet mee aan de slag te gaan, en worden tot slot (mogelijke) praktijktoepassingen ervan toegelicht.

Kwalitatief hoogwaardig functionele schoenen voor WERK & VRIJE TIJD!

Verkrijgbaar bij uw vakman of in de HAIX® Webshop

haix.nl