Editoriaal

Politie en cybercrime

Cahiers Politiestudies
Jaargang 2020-3, nr. 56
p. 7-12

ISBN 978-94-6371-226-2

Christianne de Poot[1], Eva Lievens, Wouter Stol en Lies De Kimpe (gasteditoren)

Cybercrime is een relatief nieuw onderwerp dat tal van vragen oproept. Welke delicten vallen onder de verzamelterm 'cybercrime'? Wie zijn de nieuwe daders? Wie zijn de slachtoffers? Voor welke uitdagingen staan de politie, private partners en lokale overheden bij de aanpak van dit fenomeen? In dit Cahier gaan we op zoek naar resultaten van recent (internationaal) onderzoek om antwoord te vinden op deze vragen. Er wordt aandacht besteed aan de wijze waarop de politie kennis ontwikkelt over nieuwe vormen van cybercrime en aan de bewijsvergaring in een digitale omgeving, er wordt ingezoomd op de slachtoffers van cybercrime, op hun aangiftegedrag en hun behoefte aan steun. Ook wordt ingegaan op werkwijzen van cyberdaders, criminele bedrijfsprocessen, het internationale karakter van cybercrime en het criminele verdienmodel. Daarnaast wordt ingegaan op specifieke fenomenen, zoals sexting en hacking, op veelvoorkomende delicten zoals oplichting en helpdeskfraude, en op technisch geavanceerde en lastig te bestrijden misdrijven, zoals complexe phishing en malware verspreiding, DDoS-aanvallen en gebruikmaking van botnets. Het Cahier besteedt aandacht aan de daders van deze vormen van criminaliteit, aan de slachtoffers en aan de mogelijkheden hiertegen op te treden. Daarbij wordt ingezoomd op de rol en de bevoegdheden van de politie, op de mogelijkheden van privaat-publieke samenwerking en op de rol van de burgemeester en van lokale risicocommunicatie bij de aanpak van complexe digitale veiligheidsvraagstukken. Zo biedt dit Cahier een waaier aan interessante kennis rond dit fenomeen.

Een eerste bijdrage, 'Digitalisering en criminaliteit: een beknopte inleiding op cybercrime' van **Wouter Stol**[2], verkent de reden waarom digitalisering doorwerkt in criminaliteit. Het begrippenkader van cybercrime wordt uitgewerkt en verder de betekenis van digitalisering voor criminaliteit. Hoe faciliteert digitalisering nieuwe vormen van criminaliteit, de zogenaamde cybercrime? Digitalisering bemoeilijkt identificatie, maakt de samenleving complexer in termen van zowel sociale als technische netwerken en leidt tot verdergaande vervlechting van technologie en menselijk lichaam. Deze drie gevolgen van digitalisering worden in deze bijdrage verder in detail uitgewerkt.

[1] Hoogleraar Criminalistiek, Vrije Universiteit Amsterdam; Lector Forensisch Onderzoek, Politieacademie en Hogeschool van Amsterdam; waarnemend hoofd en senior onderzoeker afdeling Criminaliteit, Rechtshandhaving en Sancties, WODC.

[2] Lector Cybersafety Politieacademie en NHL Stenden Hogeschool, hoogleraar Politiestudies aan de Open Universiteit Nederland.

In de tweede bijdrage, 'Bewijsverzameling in digitale omgeving door politieambtenaren' van de hand van **Sofie Royer**[3] en **Ward Yperman**[4], gaan de auteurs in op de mogelijkheid van politieambtenaren om in een digitale context bewijsmateriaal te verzamelen. Het wetgevend kader staat hierbij centraal. Ze focussen daarbij op de autonome bevoegdheden van politieambtenaren en vermelden voor welke onderzoeksdaden de tussenkomst van de procureur des Konings of de onderzoeksrechter verplicht is. Meer bepaald gaan ze in op de openlijke en heimelijke informaticazoeking, de netwerkzoeking, de online infiltratie, de inkijkoperatie in een informaticasysteem, het databeslag en enkele medewerkingsplichten.

De derde bijdrage, 'Het cybercrimebeeld van de Nederlandse politie: van algemeen beeld naar verdiepende analyse en aanpak' van **Jildau Borwell**[5], **Kristiaan Schuppers**[6], **Joke Rooyakkers**[7] en **Albert Harteveld**[8], belicht het aspect opsporing van cybercrime. Met de digitalisering van de samenleving zijn voor de politie nieuwe uitdagingen op het vlak van criminaliteit en veiligheid ontstaan, waaronder cybercrime. Om de aanpak van cybercrime te versterken werd geïnvesteerd in een informatie- en intelligencepositie. Onderdeel hiervan is een nationaal cybercrimebeeld. In deze bijdrage wordt beschreven hoe dit beeld tot stand kwam, wat de resultaten hiervan zijn en wat voor aanknopingspunten dit biedt voor de aanpak. Zo zijn de belangrijkste verschijningsvormen van cybercrime in kaart gebracht. Eén van de verschijningsvormen ('helpdeskfraude') en de aanpak hiervan wordt in deze bijdrage uitgelicht. Met behulp van publieke en private partners zijn aard, omvang, schade, ontwikkelingen, het criminele bedrijfsproces en kenmerken van verdachten en slachtoffers beschreven, wat belangrijke aanknopingspunten biedt voor een probleemgerichte aanpak. De belangrijkste bron voor het nationaal cybercrimebeeld zijn politiegegevens. Deze kennen enkele voordelen ten opzichte van andere bronnen, die in deze bijdrage aan bod komen. Ook de nadelen hiervan worden beschreven, evenals oplossingen waarmee deze (deels) kunnen worden opgevangen.

In de bijdrage 'De kracht van privaat-publieke allianties' van **Peter Hagenaars**[9] en **Jacqueline Bonnes**[10] analyseren de auteurs de privaat-publieke samenwerking (PPS). Dit

3 Senior researcher, CiTiP, KU Leuven.

4 Doctoraatsassistent, Instituut voor Strafrecht, KU Leuven.

5 Senior cybercrime analist, Analyse & Onderzoek, Dienst Regionale Informatieorganisatie, Eenheid Noord-Nederland, Nationale Politie.

6 Onderzoeker, Analyse & Onderzoek, Dienst Regionale Informatieorganisatie, Eenheid Den Haag, Nationale Politie.

7 Senior cybercrime analist, Analyse & Onderzoek, Dienst Regionale Informatieorganisatie, Eenheid Limburg, Nationale Politie.

8 Onderzoeker, Analyse & Onderzoek, Dienst Landelijke Informatieorganisatie, Landelijke Eenheid, Nationale Politie.

9 Bedrijfskundige en directeur van Top Management Consult. Als organisatiemaker heeft hij zich de afgelopen tien jaar gespecialiseerd in het ontwerpen en realiseren van privaat-publieke samenwerkingsverbanden in het digitale veiligheidsdomein zoals het landelijk skimmingpoint en het digitaal bedrijvenloket. Hij tekende voor ontwerp en realisatie van het Digital Intrusion Team, een geheel nieuw team van politie, KMar en FIOD dat invulling geeft aan de hackbevoegdheid. Momenteel is hij als projectleider belast met de borging en vernieuwing van het Landelijk Meldpunt Internet Oplichting (LMIO), een PPS van politie, bankensector, OM, Marktplaats en de ACM.

10 Officier van Justitie cybercrime en digitaal bewijs. In 1994 promoveerde ze op het proefschrift 'Uitvoering van EG-verordeningen in Nederland'. Dat zij 25 jaar later de AVG (een EU-verordening inzake gegevensbescherming) mag toepassen, vindt ze een mooi toeval. Na een wetgevingscarrière bij onder meer ministeries, waarin zij ook ervaring opdeed met het formuleren van convenanten, geeft ze nu al bijna tien jaar als Officier van Justitie leiding aan de opsporing en vervolging van cybercrime. Ze is als projectleider belast met de

lijkt steeds meer het toverwoord voor complexe veiligheidsvraagstukken in het digitale domein, maar hoe breng je een goede PPS tot stand en hoe smeed je effectieve allianties? De auteurs brengen de succesfactoren van PPS aan de hand van praktijkcases en internationaal onderzoek in beeld. Naast tastbare factoren, zoals heldere doelen, resultaten waar alle partijen beter van worden en voldoende middelen, blijken ook ontastbare factoren als vertrouwen, begrip en respect belangrijk voor succes. De auteurs gaan ook in op de juridische aspecten van privaat-publieke samenwerking. De belangrijkste lessen voor de praktijk worden in enkele aanbevelingen samengevat.

Zoals aangekondigd vinden ook enkele specifieke vormen van cybercrime een plaats in dit Cahier. De bijdrage 'Het fenomeen sexting: een grootschalige studie bij Vlaamse scholieren uit het middelbare onderwijs' van **Joris Van Ouytsel**[11], **Michel Walrave**[12], **Lieven De Marez**[13], **Bart Vanhaelewyn**[14] en **Koen Ponnet**[15] schetst de resultaten van een grootschalig empirisch onderzoek over dit fenomeen. Sexting, het verzenden van zelfgemaakte seksueel getinte foto's, kan een normaal onderdeel zijn van hoe jongeren hun seksualiteit beleven. Sexting is vooral problematisch wanneer het gebeurt onder druk of wanneer de beelden zonder toestemming verder worden verspreid. Eerder kwantitatief onderzoek naar sexting is vaak louter gericht op het beschrijven van de prevalentie van het verzenden van sextingfoto's zonder vragen te stellen over de bredere context waarin het gedrag plaatsvindt of zonder te focussen op problematische vormen van sexting. Deze bijdrage geeft een dieper inzicht in de bredere context waarin sexting bij jongeren plaatsvindt, door middel van een elektronische enquête die werd afgenomen bij een gewogen steekproef van 1309 Vlaamse scholieren uit het middelbaar onderwijs. De resultaten leiden tot enkele belangrijke aanbevelingen voor de praktijk en ze nuanceren enkele vaak gehoorde aannames over sexting, zoals de assumptie over genderverschillen bij het verzenden en doorsturen van sextingfoto's.

Ook de bijdrage 'Sexting tussen minderjarigen – strafbaar of niet?' van **Argyro Chatzinikolaou**[16] en **Eva Lievens**[17] en behandelt dit fenomeen. Volgens auteurs speelt digitale technologie een belangrijke rol in de ontwikkeling van de seksuele identiteit van minderjarigen. Het verzenden van zelfgemaakte seksueel getinte foto's via het internet en mobiele apps komt steeds vaker voor. Deze bijdrage onderzoekt in hoeverre het vervaardigen, in bezit hebben en/of verspreiden van seksuele beelden van minderjarigen door minderjarigen strafbaar gedrag vormt binnen de rechtsorde van een aantal Europese landen. Daarnaast wordt nagegaan welke overwegingen een rol kunnen spelen in beslissingen omtrent het al dan niet strafbaar stellen van sexting tussen minderjarigen.

---

bestrijding van Tech Support Scams. TSS is een PPS van financiële, software en telecomsector, en van de overheid.

11 Postdoctoraal onderzoeker, Fonds Wetenschappelijke Onderzoek – Vlaanderen, Departement Communicatiewetenschappen, Onderzoeksgroep MIOS, Universiteit Antwerpen, Sint-Jacobsstraat 2, 2000 Antwerpen, België.

12 Departement Communicatiewetenschappen, Onderzoeksgroep MIOS, Universiteit Antwerpen, Sint-Jacobsstraat 2, 2000 Antwerpen, België.

13 Departement Communicatiewetenschappen, IMEC-MICT-Ghent University, Gent, België.

14 Departement Communicatiewetenschappen, IMEC-MICT-Ghent University, Gent, België.

15 Departement Communicatiewetenschappen, IMEC-MICT-Ghent University, Gent, België.

16 Doctoraatsstudent, Onderzoeksgroep Recht & Technologie, lid van het Human Rights Centre, ANSER & PIXLES, Universiteit Gent.

17 Docent Recht & Technologie, Onderzoeksgroep Recht & Technologie, lid van het Human Rights Centre, CCCP, ANSER & PIXLES, Universiteit Gent.

Een volgende bijdrage wordt gewijd aan een ander fenomeen en draagt de titel 'Van 'cybercop' naar 'cyborg cop'? Implicaties van het 'cyborg crime-perspectief' voor de politiepraktijk', van de hand van **Wytske van der Wagen**[18] en **Frank Bernaards**[19]. In het digitale tijdperk zijn vormen van criminaliteit ontstaan waarbij de machine niet slechts een bijrol, maar vaak ook een hoofdrol speelt. Denk bijvoorbeeld aan botnets, DDoS-aanvallen en zelfreplicerende malware. De analyse van deze geautomatiseerde vormen van cybercrime vraagt om een meer hybride benadering die de relatie tussen mens en machine meer op de voorgrond plaatst. In deze bijdrage wordt stilgestaan bij de implicaties van een dergelijke benadering voor de politiepraktijk. Gekeken wordt of de drie principes van het 'cyborg crime-perspectief' – 'follow the network', 'follow the hybrid' en 'follow the tool' – ook bruikbare, haalbare en effectieve opsporings- of interventiestrategieën kunnen betekenen voor de bestrijding van cybercrime en wat dit impliceert in termen van automatisering voor de politie. Geconcludeerd wordt dat de transformatie van cybercop naar cyborg cop onvermijdelijk is in de strijd tegen cybercrime. Dit impliceert zowel een meer hybride oriëntatie en interventiestrategie als een goede samenwerking tussen mens en machine.

Ook de slachtoffers van cybercrime krijgen in dit Cahier een plaats. De bijdrage 'Zwijgen is zilver, spreken is goud? Het zoeken van formele en informele steun door slachtoffers van cybercriminaliteit' van **Lies De Kimpe**[20], **Thom Snaphaan**[21], **Wim Hardyns**[22], **Michel Walrave**[23], **Lieven Pauwels**[24] en **Koen Ponnet**[25] analyseert – aan de hand van een empirisch onderzoek – de zoektocht van het slachtoffer naar formele steun (i.e. aangiftegedrag) en informele steun (i.e. hulp en advies vragen) na een cyberincident. Vier factoren worden hierbij in rekening genomen: 1) socio-demografische en -economische kenmerken, 2) sociaal kapitaal, 3) interne reacties op het incident (i.e. zelfverwijt en ontkenning), en 4) gepercipieerde ernst en controle. De analyses zijn gebaseerd op data van een representatieve steekproef (n = 1601) in 50 Gentse buurten. De resultaten tonen aan dat slechts 26,6% van de participanten een incident formeel meldt, dat 46,4% familie en vrienden om hulp vraagt, en dat opleidingsniveau, interne reacties en gepercipieerde ernst van en controle over het incident samenhangen met het zoeken van informele steun. Deze resultaten impliceren dat slachtoffers verder aangemoedigd moeten worden om te praten over een incident, zowel formeel als informeel.

Een laatste reeks bijdragen wordt gewijd aan organisatorische aspecten. Een eerste in deze rij is de bijdrage over de daders, de hackers. Onder de titel 'Hacked it! What's next? Een kwalitatief onderzoek naar de afwegingen van jonge hackers omtrent het melden van kwetsbaarheden in websites van organisaties in het kader van Coordinated Vulnerability

18 Assistant Professor, Erasmus School of Law, Criminology.
19 Case Agent bij National High Tech Crime Unit.
20 Doctoraatsonderzoeker, onderzoeksgroep MIOS, departement Communicatiewetenschappen, Universiteit Antwerpen en onderzoeksgroep IMEC-MICT, Vakgroep Communicatiewetenschappen, Universiteit Gent.
21 Doctoraatsonderzoeker en assistent, Institute for International Research on Criminal Policy (IRCP), Vakgroep Criminologie, Strafrecht en Sociaal recht, Faculteit Recht en Criminologie, Universiteit Gent.
22 Professor, Institute for International Research on Criminal Policy (IRCP), Vakgroep Criminologie, Strafrecht en Sociaal recht, Faculteit Recht en Criminologie, Universiteit Gent.
23 Professor, Voorzitter onderzoeksgroep MIOS, Departement Communicatiewetenschappen, Universiteit Antwerpen.
24 Professor, directeur Institute for International Research on Criminal Policy (IRCP), Vakgroep Criminologie, Strafrecht en Sociaal recht, Faculteit Recht en Criminologie, Universiteit Gent.
25 Professor, Onderzoeksgroep IMEC-MICT, Vakgroep Communicatiewetenschappen, Universiteit Gent.

Disclosure' van **Freya Spronk**[26] en **Marleen Weulen Kranenbarg**[27] wordt het Coordinated Vulnerability Disclosure (CVD) systeem besproken dat hackers de mogelijkheid biedt om melding te maken van kwetsbaarheden in systemen. Deze bijdrage bespreekt de resultaten van een empirisch onderzoek waarbij via twaalf diepte-interviews bij jonge hackers inzicht verkregen werd in hun meningen en ervaringen omtrent dit beleid en de mate waarin zij gemotiveerd zijn om een melding te maken. Alle respondenten bleken bekend te zijn met CVD en vooral meldingen te maken om bij te dragen aan een veilig internet. Gebleken is dat de bereidheid van jongeren om kwetsbaarheden te melden afhankelijk is van (1) de aanwezigheid, vormgeving en grenzen van CVD, (2) de ernst van de kwetsbaarheid, (3) de afhandeling van meldingen door organisaties, en (4) de waardering en status voor het doen van meldingen. Op basis van de resultaten biedt deze bijdrage aanbevelingen voor de verdere ontwikkeling van CVD en toekomstig onderzoek.

En hoe moet cybercrime, dat vaak een nationaal en zelfs een internationaal fenomeen wordt genoemd, op lokaal vlak worden benaderd? Daarover gaat de bijdrage 'De lokale aanpak van cybercrime: risicocommunicatie als antwoord op een grenzeloos vraagstuk' van **Rutger Leukfeldt**[28]**, Remco Spithoven**[29] en **Ellen Misana-ter Huurne**[30]**.** Onder lokale overheden leeft doorgaans het beeld dat cybercrime zich buiten hun invloed afspeelt: Daders zitten aan de ene kant van de wereld en de slachtoffers aan de andere kant. Wat kunnen lokale overheden hiertegen doen? In deze bijdrage wordt beschreven hoe lokale overheden kunnen bijdragen aan het beschermen van burgers en bedrijven tegen cyberaanvallen. Welke rol kunnen lokale overheden spelen bij het frustreren van de activiteiten van (inter)nationale cybercriminele netwerken? Dadergroepen blijken veelal lokaal te opereren of in ieder geval een sterke lokale inbedding te hebben. Daarnaast bestaan er vaak al lokale contacten tussen overheden en (potentiële) slachtoffergroepen, waarbinnen doeltreffende risicocommunicatie kan plaatsvinden. Vanuit de situationele criminaliteitspreventie wordt beargumenteerd dat lokale overheden wel degelijk een sleutelpositie hebben in de aanpak van cybercrime. Lokale risicocommunicatie vormt namelijk een passend antwoord op dit schijnbaar grenzeloze vraagstuk.

We sluiten dit Cahier af met een laatste organisatorisch aspect, namelijk de rol van de burgemeester. Met de titel 'Hoe burgemeesters kunnen bijdragen aan een digitaal veilige samenleving' van **Willem Bantema**[31] en **Wouter Stol** wordt op dit thema ingezoomd. Waar aanvankelijk vooral aandacht was voor preventie, gaan steeds meer Nederlandse burgemeesters en gemeenten zich melden aan het digitale front om onveiligheid, waar cybercrime deel van uitmaakt, actief te bestrijden. Nederlandse burgemeesters hebben immers diverse bevoegdheden die ingezet kunnen worden om de openbare orde en veiligheid te handhaven. Het doel van deze bijdrage is om op basis van beschikbaar onderzoek naar online ordehandhaving door burgemeesters aanknopingspunten te bieden voor de bestuurlijke aanpak van cybercrime. Uit de bijdrage blijkt dat burgemeesters, om verschillende redenen, hun bevoegdheden online niet kunnen inzetten tegen ordeverstoringen die daar ontstaan, maar dat ze zich wel verantwoordelijk voelen om

[26] Master Opsporingscriminologie, Vrije Universiteit Amsterdam.
[27] Assistant Professor, Vrije Universiteit Amsterdam, Faculty of Law, Criminology.
[28] Directeur Centre of Expertise Cybersecurity bij de Haagse Hogeschool en senior onderzoeker bij het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR).
[29] Lector Maatschappelijke Veiligheid bij Hogeschool Saxion.
[30] Senior onderzoeker en docent bij Hogeschool Saxion.
[31] Senior onderzoeker onderzoeksgroep Cybersafety, Thorbecke Academie/NHL Stenden Hogeschool.

dergelijke verstoringen te voorkomen. Ze geven die verantwoordelijkheid vorm met tal van niet-juridische interventies waarbij in veel gevallen het gezag van de burgemeester en communicatie centraal staan. Dergelijke interventies en ervaringen kunnen mogelijk ook bijdragen aan de bestrijding van cybercrime.

In de rubriek 'Boekbespreking', ten slotte, bespreekt **Lodewijk Gunther Moor**[32] in zijn bijdrage het werk *De veilige stad als collectief doel* van Jan Willem Sap en Emile Kolthoff.

[32] Algemeen redacteur van de *Cahiers Politiestudies* en gewezen directeur van de Stichting Maatschappij, Veiligheid en Politie (SMVP).