Universiteit Leiden
The Netherlands

Meer dan alleen een goed idee: naar een empirisch onderbouwde aanpak van cybercrime

Leukfeldt, E.R.

Citation
Leukfeldt, E. R. (2024). *Meer dan alleen een goed idee: naar een empirisch onderbouwde aanpak van cybercrime*. Leiden. Retrieved from https://hdl.handle.net/1887/4108035

Version:	Publisher's Version
License:	Leiden University Non-exclusive license
Downloaded from:	https://hdl.handle.net/1887/4108035

Note: To cite this publication please use the final published version (if applicable).

Prof.dr. E.R. Leukfeldt

Meer dan alleen een goed idee
Naar een empirisch onderbouwde aanpak van cybercrime

Universiteit Leiden

Bij ons leer je de wereld kennen

Meer dan alleen een goed idee
Naar een empirisch onderbouwde aanpak van cybercrime

Oratie uitgesproken door

Prof.dr. E.R. Leukfeldt

bij de aanvaarding van het ambt van bijzonder hoogleraar

Governing Cybercrime

aan de Universiteit Leiden

op maandag 25 november 2024

Universiteit Leiden

Mevrouw de Rector Magnificus, zeer gewaardeerde toehoorders,

1. Inleiding

> '"Orange en green gezocht!", "Wie wil snel geld maken?" Jongeren in Nederland worden op deze manier op straat of via sociale media gevraagd of ze bankpassen en bijbehorende pincodes van banken uit Nederland hebben of kunnen aanleveren. De kleuren oranje en groen staan voor de kleuren van de bankpassen van twee grootbanken. De passen en codes worden door criminele groepen gebruikt om geld dat afkomstig is van slachtoffers van phishing weg te sluizen. Bij phishing proberen criminelen op slinkse (digitale) wijze inloggegevens van internetbankieren te ontfutselen. Als dat lukt dan worden grote bedragen overgeschreven van de rekeningen van slachtoffers.'

Deze quote komt uit een van de eerste artikelen van mijn proefschrift (Leukfeldt, 2014). Phishing en banking malware (waarbij via kwaadaardige software toegang wordt verkregen tot de online bankieromgeving van klanten van banken) was op dat moment een groot probleem in Europa. Ik zou nog tientallen van dit soort casussen analyseren voor mijn proefschrift. De reden dat ik over deze enkele casus een wetenschappelijk artikel schreef, was dat wat ik zag zo anders was dan wat ik las in de wetenschappelijke en grijze literatuur, dat ik dacht een unieke casus te pakken te hebben. Een die ik daarna wellicht niet meer zou treffen. Dat bleek gaandeweg het proefschrift wel anders te zijn: dankzij empirische bestudering van cybercriminele netwerken kwam ik erachter dat het beeld dat er was van deze netwerken sterk genuanceerd moest worden. Hoe dan precies? Daar zal ik tijdens deze oratie nog uitgebreid op ingaan.

Laten we de twee delicten die zojuist zijn beschreven eerst in een wat breder perspectief plaatsen. Feitelijk hebben we het natuurlijk helemaal niet over een nieuw type delict. Immers: geld stelen van anderen bestond ook al voor de komst van internet. We hebben het over delicten waarbij technologie een belangrijke rol speelt bij de uitvoering ervan. En dat is dan weer niet zo gek, want we leven immers in een sterk gedigitaliseerde samenleving. Vandaag heeft u waarschijnlijk al bewust of onbewust allerlei ICT-toepassingen gebruikt: even een e-mail sturen vanuit de trein, een online betaling gedaan, via Zoom of Teams een vergadering gehad en wellicht bent u *as we speak* nog snel even dat belangrijke bericht via WhatsApp of Signal aan het versturen. Uit cijfers van het Centraal Bureau voor de Statistiek blijkt dat in 2022 zo'n 90% van de Nederlanders van 12 jaar en ouder dagelijks online was (CBS, 2023). Als we kijken naar alle technologische innovaties die op ons afkomen, durf ik wel te stellen dat de digitalisering een steeds grotere rol gaat spelen in onze levens.

Vandaag wil ik het vooral hebben over de personen die digitalisering misbruiken en over de personen die zich bezighouden met de bestrijding van deze vorm van criminaliteit.

Criminelen zou je *early adoptors* van deze digitalisering kunnen noemen: zodra er een nieuwe technologische toepassing is, maken ze volop misbruik van deze nieuwe mogelijkheden.[1] Ze vallen die technologie zelf aan of zetten technologie in om hun aanvallen beter uit te voeren. Bij het aanvallen van de technologie zelf kun je denken aan een ransomware-aanval waarbij digitale bestanden of systemen niet meer toegankelijk zijn. Bij de inzet van technologie voor crimineel gedrag gaat het bijvoorbeeld over een hack van een database met gegevens, om phishing-e-mails om toegang te krijgen tot online bankrekeningen of om stalkers die hun slachtoffers ook in hun eigen huis lastigvallen door hun e-mail, socialmedia-accounts of webcam te hacken. Voor dit soort delicten hanteer ik vanaf nu de term 'cybercrime'. Een uitgebreidere analyse van dit soort delicten en terminologie volgt in deel 2 van deze oratie.

1 Vrij naar Rogers (1962, herdruk in 2003), die verschillende stadia van adoptie van innovatie beschrijft: *innovators*, *early adopters*, *early majority*, *late majority* en *laggards*.

De laatste jaren zien we een belangrijke trend die ervoor zorgt dat beide typen criminaliteit die ik zojuist beschreef nog makkelijker te plegen zijn: de opkomst van cybercrime-as-a-service (CaaS). Dat zijn tools die zijn ontwikkeld door anderen (laten we die dan in lijn met de gehanteerde typologie van Rogers de *innovators* noemen) en op allerlei online criminele markten worden aangeboden. Zowel criminele netwerken als eenlingen maken volop gebruik van dergelijke markten om de benodigde technische hulpmiddelen te verkrijgen om cyberaanvallen uit te voeren. CaaS heeft cybercrime daarmee echt voor iedereen toegankelijk gemaakt. Ofwel: door CaaS kunnen ook – in lijn met de stadia beschreven door Rogers – de *early majority* en zelfs de *late majority* cyberaanvallen uitvoeren. CaaS blijft floreren en wordt door Europol gezien als een van de belangrijkste transversale misdrijven en uitdagingen (Europol, 2021). Op deze manier verkort CaaS ook de *pathway* naar cybercrime, omdat cybercriminelen niet het leerproces van het bouwen van hun eigen cybercriminele tools hoeven te doorlopen, maar deze simpelweg kunnen kopen of huren. Niet verrassend is dan misschien ook wel dat in de meest recente monitor jeugddelinquentie te zien is dat jongeren relatief veel cybercrimes plegen. Bij zowel 12-minners, 12- tot 18-jarigen als jongvolwassenen staan cyberdelicten inmiddels in de top drie van de meest gepleegde delicten (Tollenaar et al., 2024).

Slachtofferschap van allerlei vormen van cybercrime is inmiddels dan ook veelvoorkomend te noemen. We kennen allemaal de krantenkoppen van grote bedrijven die gehackt zijn of platliggen door een ransomware-aanval. Maar empirisch onderzoek laat zien dat cybercrimes alle lagen van onze maatschappij raken: van burgers en zzp'ers tot mkb'ers, overheden en grote organisaties. Al in 2012 lieten we zien dat een delict als hacken vaker voorkomt dan het meest traditionele Nederlandse delict – fietsendiefstal (Domenie et al., 2012). Sinds 2012 meet het CBS regelmatig de aard en omvang van slachtoffers middels een grootschalig zelfrapportageonderzoek. Helaas wordt daar nog steeds maar een beperkt aantal cybercrimes in meegenomen, maar duidelijk is te zien dat de slachtofferpercentages van die delicten hoog zijn en blijven: in 2023 werd bijvoorbeeld 9% van de Nederlanders slachtoffer van een vorm van online oplichting en fraude (9%), gevolgd door hacken (6%) en online bedreiging en intimidatie (3%). Hetzelfde beeld is te zien binnen het bedrijfsleven: recent internationaal vergelijkend onderzoek naar slachtofferschap van cybercriminaliteit onder 12.863 Europese mkb'ers laat zien dat 37% van de Nederlandse mkb'ers slachtoffer werd van cybercriminaliteit in 2021. Daarmee scoorde Nederland aanzienlijk hoger dan de andere Europese landen, waarbij het gemiddelde 28% is. Het vaakst was er sprake van malware en phishing (respectievelijk 17% en 21%).

Dan de aanpak van cybercrimes. Zijn politie en justitie dan de *laggards* – vrij naar weer Rogers (2003, oorspr. 1962) diegenen die achterblijven bij het gebruik van nieuwe technologie? Nee, dat lijkt me een te makkelijk antwoord. Zoals later in deze oratie zal blijken, moet er nog veel gebeuren, maar gelukkig zitten politie en justitie ook niet stil. De aanpak van cybercrime is de afgelopen decennia flink verbeterd. Hadden we in 2007 bijvoorbeeld pas voor het eerst een Nationaal Team High Tech Crime, anno 2024 is er naast een flink uitgebreid nationaal team ook bijvoorbeeld de publiek-private samenwerking ECTF (Electronic Crimes Taks Force), waarbinnen de grootbanken en politie samenwerken om cybercrimes gericht op de financiële sector te bestrijden. Daarnaast heeft iedere politieeenheid een cybercrimeteam, is er een landelijk programma rondom veelvoorkomende vormen van cybercrime (met name gedigitaliseerde criminaliteit, zie deel 2) en zijn er tal van alternatieve interventies ontwikkeld: van Hack_Right gericht op *first offenders* en re_B00TCMP waarbij jongeren met IT-talent positieve alternatieven worden aangeboden tot het gebruik van GoogleAds door de politie om potentiële in cybercrime geïnteresseerde jongeren te informeren en af te schrikken (en zoveel meer, zie bijvoorbeeld Schiks et al. (2021) voor een overzicht van lokale initiatieven en Bluhm et al. (2024) voor een analyse van twintig cybercrimeprojecten).

We moeten echter constateren dat de strafrechtketen nog steeds hapert. Alle ontwikkelingen ten spijt zien we veel van de problemen die er grofweg tien jaar geleden waren vandaag de dag nog steeds (zie deel 4 van deze oratie). Dit is ook niet zo gek: op basis van de cijfers over slachtofferschap en de toename van het aantal criminelen die cyberaanvallen kunnen uitvoeren dankzij CaaS durf ik wel te stellen dat het aannemelijk is dat er alleen maar meer cyberaanvallen komen en het werkaanbod van politie, justitie en cybersecuritybedrijven alleen maar zal toenemen.

Daarom is het des te belangrijker dat we stoppen met het zomaar beginnen van het zoveelste goedbedoelde project om het cybercriminelen moeilijker te maken of burgers en bedrijven cyberweerbaarder te maken. Niet dat er iets mis is met deze goede bedoelingen, maar er is inmiddels flink wat discussie over of veel van de gebruikte interventies wel een meetbaar effect hebben of wellicht zelfs een onbedoeld effect kunnen hebben (bijvoorbeeld Kruisbergen, 2023; Hendriks & Stams, 2024). Het adagium in cyberland is momenteel: maar we moeten *nu* iets doen, anders verliezen we de race. Ik ben het daar niet mee eens. Ja, we moeten nu iets doen, maar doe het dan goed en (1) zorg voor een goede onderbouwing van het beleid / de interventie / het project, (2) zorg ervoor dat resultaten meetbaar zijn en (3) meet de effectiviteit ook daadwerkelijk. U wilt niet weten hoeveel projectleiders ik de afgelopen jaren heb gesproken die stellen dat hun project zonder meer een succes is, omdat 'iedereen die betrokken is dit zo'n goed idee vindt en nog steeds enthousiast is', of omdat 'we wel tientallen bedrijven bereikt hebben'. We moeten ons echter realiseren dat 'de race' sowieso niet voorbij is na een paar jaar. Immers: door de steeds verdergaande digitalisering zal cybercrime alleen maar toenemen. Een ander argument om maar niet al te veel empirisch onderzoek te doen is: maar cybercrime verandert toch zo snel dat het geen zin heeft om onderzoek te doen. De achterliggende gedachte is dan dat de technologische ontwikkelingen zo snel gaan, dat de werkwijze van vandaag morgen alweer achterhaald is. We hebben de afgelopen vijftien jaar denk ik heel duidelijk laten zien dat dit een mythe is. Ja, de technologie verandert snel, maar de motieven, manieren van samenwerken, opbouwen van vertrouwen binnen criminele samenwerkingen en grote bottlenecks binnen de modus operandi – zoals het cashen en witwassen van illegaal verkregen geld of het aantrekken van betrouwbare kundige mededaders – blijven min of meer hetzelfde. Sterker nog, in een aantal studies zien we dat cybercriminelen door de verbeterde aanpak ervan steeds *minder* technologie gebruiken binnen hun aanvallen en steeds sterker leunen op *social engineering* (bijvoorbeeld Loggen & Leukfeldt, 2022).

Mijn bijdrage aan een betere aanpak van cybercrime is dan ook tweeledig. Aan de ene kant kan de wetenschap zorgen voor empirisch onderzoek naar daders en slachtoffers van cybercrime, waardoor een gedegen kennisbasis ontstaat om beleid op te maken en nieuwe interventies op te ontwikkelen. Dit is uiteraard langetermijnwerk en vergt samenwerking tussen onderzoekers uit verschillende disciplines en landen. Daarom ben ik ook voorstander van een bijdrage van de wetenschap op een tweede manier: het stimuleren van de praktijk om interventies te ontwikkelen die meetbaar zijn en als onafhankelijke partij die interventies te evalueren. Op die manier kan de wetenschap ook op een veel kortere termijn effect hebben. Recent hebben we op deze manier bijvoorbeeld de alternatieve interventies Hack_Right en GoogleAds geëvalueerd. De onderzoeken laten zien dat de interventies veelbelovend zijn, maar dat er ook nog flink wat moet gebeuren. Mooi om te zien is dat de praktijk – in ieder geval in deze twee voorbeelden – vervolgens daadwerkelijk aan de slag gaat met de uitkomsten en aanpassingen doorvoert. Beter kan je het niet krijgen wat mij betreft: relevante wetenschappelijke studies en een directe impact in de praktijk.

De rest van deze oratie zal gaan langs de twee lijnen die ik zojuist heb geschetst. Ik zal uitgebreid ingaan op de resultaten van enkele empirische onderzoeken naar cybercrime die mijns inziens van belang zijn voor de aanpak van cybercrime

en ik zal het belang laten zien van empirisch onderzoek naar een ongrijpbaar fenomeen als cybercrime. Daarbij ga ik in op twee van mijn wetenschappelijke liefdes: samenwerkende cybercriminelen en ontwikkelpaden van jonge cybercriminelen. Vervolgens volgt een beschouwing op de knelpunten binnen de strafrechtketen, waarna ik twee casussen behandel waarbij we alternatieve interventies hebben geëvalueerd: de alternatieve interventie Hack_Right en het gebruik van GoogleAds door de politie. Ik zal deze oratie afsluiten met een blik op de toekomst: welke onderzoekslijnen staan de komende jaren centraal en wat doen we daarbinnen nu al?

2. Waar hebben we het eigenlijk over? Cybercriminaliteit, gedigitaliseerde criminaliteit en meer

Voordat ik overga tot het bespreken van de lessen die ikzelf heb geleerd over cybercrime, wil ik wat dieper ingaan op het concept cybercrime. Ik zal er niet te lang bij stilstaan, maar het is toch wel van belang dat we weten waarover we het precies hebben. Al zal ik vast verklappen: dat is best lastig. Dit deel van de oratie is een bewerking van een nog niet gepubliceerd hoofdstuk dat ik samen met anderen schreef (Leukfeldt et al., 2025) voor het *Handboek digitale veiligheid*, dat volgend jaar uitkomt onder redactie van Leidse collega's. Geïnteresseerden kunnen dus binnenkort een uitgebreidere versie lezen in dat hoofdstuk.

De vraag wat cybercriminaliteit nou precies is en welke delicten onder deze term vallen, speelt al decennia binnen de criminologie. Met name vanaf de jaren negentig van de vorige eeuw krijgt dit onderwerp veel aandacht van wetenschappers en worden er theoretische verhandelingen over geschreven. Het voert te ver om die op deze plaats in detail te herhalen. In de kern komt het in verschillende variaties neer op twee kernvragen: is het delict gericht op ICT en/of is het delict gepleegd met behulp van ICT? Vervolgens worden delicten in twee of drie categorieën onderverdeeld.

In het huidige criminologische onderzoek naar cybercriminaliteit worden tegenwoordig in de regel twee categorieën gebruikt. De gangbare Engelse terminologie van deze categorieën is *cyber dependent crime* en *cyber enabled crime*.[2] In het Nederlands kan dat vertaald worden als 'cybercriminaliteit' en 'gedigitaliseerde criminaliteit'. Beide categorieën vallen dan onder het paraplubegrip 'online criminaliteit' (in het Engels dan weer *cybercrime* genoemd).

Delicten die vallen onder de noemer 'cybercriminaliteit' kunnen gezien worden als 'nieuwe' vormen van criminaliteit. ICT is in dit geval niet alleen het middel om het delict te plegen, maar ook het doelwit. Dergelijke delicten waren in het predigitale tijdperk simpelweg niet mogelijk, omdat er geen ICT-infrastructuur was om aan te vallen. Voorbeelden zijn hacken (het zonder toestemming binnendringen in een geautomatiseerd werk), het gebruik van malware (kwaadaardige software zoals een virus of spyware), ransomware (het versleutelen van digitale informatie of systemen en daar losgeld voor vragen), DDoS-aanvallen (het platleggen van een digitaal systeem door er heel veel informatievragen op af te vuren) en *defacen* (het zonder toestemming aanpassen van websites).

Delicten die vallen onder de noemer 'gedigitaliseerde criminaliteit' zijn feitelijk delicten die er in het predigitale tijdperk ook al waren, maar waarbij ICT nu van wezenlijk belang is voor de uitvoering van dat delict. Een voorbeeld is het uitvoeren van een phishingcampagne waarbij criminelen via een valse e-mail mensen inloggegevens proberen te ontfutselen om zo controle te krijgen over hun online bankieromgeving. Vervolgens is het doel om geld van de rekening van een slachtoffer via zogenaamde geldezels (*money mules*) door te sluizen naar de rekeningen van de criminelen. Hier gaat het om een vrij klassiek motief, namelijk financieel gewin, samen met een nieuwe vorm van een heel oud delict, namelijk oplichting of diefstal.

2 In de regel wordt hierbij verwezen naar het werk van McGuire en Dowling (2013a, 2013b), en in Nederland naar Beerthuizen et al., 2020.

Onder gedigitaliseerde criminaliteit kan een veelheid aan delicten vallen. Grofweg is te zien in de criminologische literatuur dat er drie subcategorieën kunnen worden onderscheiden: financieel-economische delicten, interpersoonlijke delicten en zedendelicten. Bij financiële cyberdelicten is het doel van de daders financieel gewin. Voorbeelden zijn phishing, identiteitsfraude, WhatsAppfraude, koop- en verkoopfraude, virtuele diefstal, voorschotfraude, heling, CEO-fraude en *romance scams*. Interpersoonlijke cyberdelicten zijn digitale vormen van strafbare gedragsdelicten waarbij de persoonlijke levenssfeer wordt aangetast. De meest voorkomende vormen zijn laster en chantage, gevolgd door cyberstalking en cyberbedreiging met geweld. Sinds de opkomst van internet vinden ook zedendelicten online plaats. Voorbeelden zijn grooming en de verspreiding van kinderpornografisch materiaal. Daarnaast zijn er de zogenaamde IBSA-delicten (*Image Based Sexual Abuse*), zoals het zonder toestemming verspreiden van naaktfoto's en -filmpjes (ook wel *shame sexting* genoemd) of het dreigen hiermee (*sextortion*).

Binnen de categorie gedigitaliseerde criminaliteit is er duidelijk sprake van een hellend vlak. Het is immers de vraag wanneer ICT van *wezenlijk* belang is voor de uitvoering van een delict en wanneer een dader dan wel gebruik heeft gemaakt van ICT voor het plegen van dat delict, maar waarbij ICT eigenlijk geen substantieel onderdeel uitmaakt van de werkwijze. In het voorbeeld van phishing is het duidelijk dat ICT een belangrijke rol speelt bij de uitvoering, maar hoe zit dat bij drugshandel via socialmedia-platformen zoals Telegram of bij het gebruik van GoogleMaps om een woninginbraak voor te bereiden? Verder zullen door de steeds verdergaande digitalisering steeds meer delicten onder deze noemer vallen, omdat ICT steeds meer verweven is met ons dagelijks leven. Samen met Roks schreef ik hier enkele artikelen over, waarin we ingaan op deze *hybridisering* van criminaliteit (Leukfeldt & Roks, 2020; Roks et al., 2020). Het is momenteel niet duidelijk welke categorieën nog net wel en net niet in deze categorie vallen. Het kan zelfs zo zijn, dat op een gegeven moment alle criminaliteit zo gedigitaliseerd is, dat het niet meer nodig is om een aparte categorie te hebben voor gedigitaliseerde criminaliteit.

Ik ga nu niet nog dieper in op de discussie welke delicten onder welke categorie vallen. In de praktijk blijkt het namelijk lastig om tot een verdeling te komen waarbij delicten echt altijd maar in één categorie vallen (denk aan bank-helpdeskfraude wat een duidelijk financieel-economisch delict is, terwijl daders ook de computer van slachtoffers overnemen, ofwel 'hacken', om zo geld over te schrijven). Vanuit criminologisch oogpunt is het onderscheid tussen delictscategorieën echter wel belangrijk, omdat daar wordt ingegaan op fundamentele vraagstukken. Er spelen namelijk hele andere fundamentele vraagstukken (zie bijvoorbeeld de onderzoeksagenda die we hier in 2017 al over uitbrachten – Leukfeldt (2017)). Zo is het bij de nieuwe verschijningsvormen – cybercriminaliteit zoals hacken en het plegen van DDoS-aanvallen – de vraag of we te maken hebben met een nieuw type dader met andere motieven, achtergrondkenmerken en risicofactoren dan daders van traditionele delicten. Onderzoek hiernaar staat nog in de kinderschoenen en we weten daarom momenteel het antwoord op deze vraag niet, terwijl het wel van belang is om effectieve interventies in te zetten gericht op deze doelgroep (zie ook Schiks et al., 2023; Loggen et al., 2023, 2024). Van daders van allerlei delicten die vallen onder de noemer gedigitaliseerde criminaliteit is er steeds meer bewijs dat het deels om daders gaat die eerder al traditionele delicten pleegden en nu hun werkterrein deels hebben verplaatst naar het online domein (Leukfeldt et al., 2017a; Lusthaus et al., 2023). Binnen deze categorie is het veel meer de vraag wat de betekenis is van de digitale component binnen de ontstaans- en groeiprocessen en de modus operandi – de werkwijze – van cybercriminele netwerken. Internet biedt bijvoorbeeld allerlei digitale ontmoetingsplaatsen waar nieuwe criminele contacten kunnen worden opgedaan, waardoor er nieuwe mogelijkheden ontstaan voor losjes georganiseerde gelegenheidsnetwerken. Verder kan de rol van ICT binnen de werkwijze van criminelen bijvoorbeeld van grote invloed zijn op de criminele mogelijkheden die een

netwerk heeft en daarmee op de wijze waarop delicten worden gepleegd en bijvoorbeeld of op die manier niet alleen meer, maar ook *andere* slachtoffers worden bereikt.

3. Het belang van empirisch onderzoek: enkele lessen over cybercriminele netwerken en criminele hackers

Het beeld dat veel mensen hebben van cybercriminelen is dat van internationaal opererende specialisten met een hoge mate van technische kennis. Specialisten die elkaar ook nog eens weten te vinden via criminele markten op het *dark web* – het niet-geïndexeerde en dus via bijvoorbeeld Google niet te vinden deel van internet – of worden aangestuurd door statelijke actoren, het liefst uit Rusland, China of Noord-Korea. En dat klopt, die netwerken zijn er (zie bijvoorbeeld de crime script-analyse van ransomware-groepen van Matthijsse et al., 2023). Maar het verhaal is veel complexer – of misschien is 'eenvoudiger' hier een beter woord.

Dé cybercrimineel bestaat niet, net zomin als dé traditionele crimineel. In dat laatste geval weet iedereen dat eigenlijk wel: er zijn vandalen die bushokjes slopen, verslaafden die af en toe een fiets stelen, groepen jongeren die overlast veroorzaken in bepaalde straten en allerlei criminele activiteiten plegen en zware en georganiseerde criminaliteit (en alles wat daartussen zit). In het geval van cybercrime lijken al die verschillende typen daders met hun verschillende soorten motieven op één hoop te worden gegooid. Of erger wat mij betreft: er is met name aandacht voor alles wat van ver komt: we vechten tegen in duister gehulde individuen uit verre landen met haast magische skills die bijna onmogelijk tegen te houden zijn. Nogmaals: die zijn er vast en zeker. Gelukkig zijn cybercriminelen ook gewoon mensen en dus waarschijnlijk van net zo'n diverse pluimage als daders van traditionele criminaliteit. Ook bij cybercrime is er feitelijk sprake van vandalisme, zijn er gelegenheidsplegers, maar ook netwerken die lijken op criminele jeugdnetwerken en meer georganiseerdere samenwerkingsverbanden. En meer en meer zien we dat de wereld van cybercrime eigenlijk heel veel overlap heeft met de traditionele criminele wereld. In mijn proefschrift en later met onder andere Kleemans, Roks en nog later Holt en Lusthaus liet ik zien dat plegers van traditionele delicten helemaal niet denken in 'wel of niet cybercrime' plegen. Nee, wat we eerder zagen, was dat 'er een nieuwe mogelijkheid bij is gekomen om geld te verdienen en dat gaan we proberen' (bijvoorbeeld Leukfeldt et al., 2017a, 2017b; Leukfeldt & Holt, 2020; Leukfeldt & Roks, 2020; Roks et al., 2020; Loggen & Leukfeldt, 2022; Lusthaus et al., 2023). Opvallend was verder dat er inderdaad internationale cybercriminele netwerken zijn, maar dat die vaak ook een lokale inbedding kennen en dat er bovendien net zo goed veel Nederlandse netwerken actief zijn.

Het is daarom van groot belang om empirisch onderzoek te doen naar cybercriminelen en de samenwerkingsverbanden waarbinnen zij werken. Anders blijven we jagen op een haast mysterieus wezen dat niet bestaat. Ik zie veel overeenkomsten met de beeldvorming rondom georganiseerde criminaliteit begin jaren negentig van de vorige eeuw. Door een gebrek aan gedegen empirisch onderzoek was er in de maatschappij en bij politie en justitie een beeld ontstaan van georganiseerde criminaliteit die – naar afschrikwekkend Italiaans voorbeeld – werd gepleegd door grootschalige, piramidale organisaties met een baas aan de top, hiërarchische relaties, een vaste taakverdeling en een intern sanctiesysteem. Om die te bestrijden was het wel nodig om steeds verder 'door te rechercheren' naar de top met als gevolg dat de politie zelf een grote speler werd in de internationale drugshandel en grote hoeveelheden drugs ongecontroleerd de Nederlandse markt op liet gaan. Ze kwamen immers steeds maar niet bij die ene *master mind* uit en daarom werd steeds meer ruimte gegeven aan criminele burgerinfiltranten en andere ingrijpende opsporingsmethoden. Dit mondde uiteindelijk uit in de zogenaamde IRT-affaire[3] en de commissie-Van Traa, en heel kort door de bocht daarmee ook de start van de Monitor Georganiseerde Criminaliteit. Binnen deze monitor worden sinds 1996 grootschalige opsporingson-

3 Meer hierover is te vinden op www.parlement.com: Parlementaire enquête opsporingsmethoden, IRT (1994-1996).

derzoeken geanalyseerd om beter zicht te krijgen op de aard van de georganiseerde criminaliteit in Nederland (zie Kleemans et al., 1998, 2002; Van de Bunt & Kleemans, 2007; Kruisbergen et al., 2012, 2018, 2018). Daaruit blijkt: het veelkoppige monster bestond niet en in Nederland was er met name sprake van criminele netwerken en zogenaamde transitcriminaliteit, waarbij de kern illegale handel is en waarbij gebruik wordt gemaakt van dezelfde gelegenheidsstructuren die ook de legale economische activiteiten faciliteren. Georganiseerde criminaliteit is daarmee niet minder erg, maar vergt wel een totaal andere aanpak.

Ik pleit ervoor om ook op het gebied van cybercrime een dergelijk instrument te ontwikkelen, waarbij er systematisch data worden verzameld over cybercriminaliteit in al haar verschijningsvormen. Ik zal hierna twee voorbeelden geven van onderzoek waar ik bij betrokken was dat heeft laten zien dat gedegen empirisch onderzoek de bestaande denkbeelden kan nuanceren of zelfs veranderen en beleidsmakers zo kan voorzien van de informatie die ze nodig hebben om goed beleid te ontwikkelen.

Cybercriminele netwerken

Ik zal beginnen met mijn eerste wetenschappelijke liefde: cybercriminele netwerken. Mijn proefschrift ging over deze netwerken en in de jaren na mijn proefschrift heb ik aan verschillende onderzoeken meegewerkt met diverse auteurs in binnen- en buitenland om dit onderwerp verder uit te diepen. Uiteindelijk hebben we data van dergelijke netwerken verzameld in de periode 2012-2024 in Nederland, Duitsland, het Verenigd Koninkrijk (VK) en de Verenigde Staten (VS) (bijvoorbeeld Leukfeldt et al., 2017a, 2017b; Leukfeldt & Holt, 2020; Leukfeldt & Roks, 2020; Roks et al., 2020; Loggen & Leukfeldt, 2022; Lusthaus et al., 2023; Romagna & Leukfeldt, 2024a, 2024b).

De reden dat ik aan mijn proefschrift begon, heeft te maken met alle verhalen die ik als junioronderzoeker hoorde over deze netwerken. Ik werkte tussen 2007 en 2011 als junioronderzoeker en was betrokken bij veel opdrachtonderzoek naar cybercrime voor politie en justitie. Ambities om een proefschrift te schrijven had ik toen nog niet. Ik wilde gewoon relevant onderzoek doen. Dat veranderde langzaamaan door de vele anekdotes die ik hoorde over cybercriminelen. Ik begon te zoeken naar publicaties over deze netwerken. Vanuit de sociale wetenschappen was er nagenoeg geen empirisch onderzoek gedaan naar cybercriminele netwerken. Wel waren er diverse publicaties vanuit de *computer science*-gemeenschap te vinden die vooral inzoomden op de online ontmoetingsplaatsen waar deze daders elkaar ontmoeten. Ook waren er ontelbaar veel trendrapportages van cybersecuritybedrijven die – uiteraard zonder methodische verantwoording – het ene na het de andere verontrustende beeld schetsten.

Het beeld dat ik had op dat moment door alle anekdotes uit de praktijk, de *computer science*-publicaties en de trendrapportages was er een van internationaal samenwerkende actoren die elkaar alleen maar kennen bij hun online *nickname*, elkaar leren kennen op *hacking fora* en het *dark web*, zeer gespecialiseerd zijn en samenwerkingen aangaan op basis van hun reputatie, waarbij de traditionele zaken rondom het opbouwen van vertrouwen geen rol meer spelen. Immers: de digitale ontmoetingsplaatsen en vooral de plekken op het *dark web* hebben net als eBay en Marktplaats review- en ratingsystemen, waardoor je heel simpel de betrouwbare en kundige criminelen van de onbetrouwbare en onkundige criminelen kunt onderscheiden. Als dit klopte, dan zou dit de criminologie en alles wat we weten over de ontstaans- en groeiprocessen, maar ook van de criminele mogelijkheden van netwerken op zijn kop zetten. Immers: de manier waarop een belangrijk element binnen de ontstaans- en groeiprocessen tot stand komt – namelijk vertrouwen – is dan heel anders. Een mooi onderwerp voor een proefschrift was geboren. Omdat er in die periode een grote toename was van aanvallen op het digitale betalingsverkeer middels phishing- en banking malware-aanvallen, waarbij criminelen de controle over de online bankieromgevingen van

slachtoffers probeerden te krijgen, richtte mijn proefschrift zich op die netwerken.

Maar hoe krijg je nou zicht op die cybercriminele netwerken? Ik besloot om te beginnen met een methode die ook gewerkt had voor een andere criminaliteitsvorm die moeilijk in kaart te brengen is: georganiseerde criminaliteit. Daarom hanteerde ik hetzelfde analysekader en dezelfde methode als in de Monitor Georganiseerde Criminaliteit – de analyse van grootschalige opsporingsonderzoeken. Over de voor- en nadelen hiervan kan ik lang spreken. De liefhebber verwijs ik naar het hoofdstuk dat Kleemans en ik hierover schreven in 2021 (Leukfeldt & Kleemans, 2021). Kortgezegd: ik denk dat het analyseren van grootschalige opsporingsonderzoeken een heel waardevolle methode is om zicht te krijgen op nog relatief onbekende fenomenen.

De allereerste zaak die ik analyseerde, bleek zo anders te zijn dan alles wat ik daarvoor had gehoord en gelezen, dat ik er meteen een wetenschappelijk artikel over schreef: *The case of phishing in Amsterdam* (Leukfeldt, 2014). Deze zaak speelde zich – zoals de titel al verklapt – voornamelijk af in Amsterdam, alhoewel dit netwerk door heel Nederland slachtoffers maakte via phishing-e-mails en -websites, waardoor de leden van het netwerk toegang verkregen tot de online bankieromgevingen van klanten van Nederlandse banken.

Dat criminele netwerk bestond uit acht kernleden, negen leden met een faciliterende rol en tientallen *money mules*. Ik heb deze casus al vaak gebruikt in presentaties en beschrijf dit netwerk dan als 'het op dat moment meest succesvolle cybercriminele netwerk in Nederland die gedurende het opsporingsonderzoek verantwoordelijk was voor een groot deel van het slachtofferschap van phishing in Nederland'. Ik wil er vooral mee aangeven dat het dus niet gaat om een klein onbelangrijk netwerkje, maar om een netwerk dat een grote impact had in Nederland. Opvallend was dat dit netwerk eigenlijk helemaal geen internationale component had. In tegenstelling tot de literatuur over phishing-netwerken op dat moment was er ook helemaal geen sprake van het gebruik van online ontmoetingsplaatsen om nieuwe plannen te maken en geschikte mededaders te rekruteren. In tegendeel, in de Amsterdamse casus blijkt dat de ontmoetingsplaatsen de straten van de Bijlmer zijn. Kernleden kennen elkaar via via, bijvoorbeeld door het rondhangen op straat, doordat ze op dezelfde school of sportvereniging hebben gezeten of via familie. Ze hebben allemaal al een behoorlijke lijst met criminele antecedenten en hebben eerder in verschillende samenstellingen samengewerkt aan andere delicten. Dat doen ze overigens nog steeds, want er zijn ook drugslijnen die kernleden samen hebben opgezet en de kernleden zijn actieve bedrijfsinbrekers waarbij ze steevast voor de kluis met waardepapieren en pinpassen gaan. Leden met een faciliterende rol, zoals bankmedewerkers en postmedewerkers, worden gericht geronseld: ze worden op straat aangesproken door (oude) bekenden. In het geval van de bankmedewerkers werd er vervolgens druk op ze uitgeoefend om mee te werken. De rekrutering van de *money mules* (die hun rekening laten gebruiken om het geld weg te sluizen van rekeningen van slachtoffers) gaat ook via via. Potentiële *money mules* worden op straat, op school of op de sportvereniging aangesproken. En via chatfuncties op mobiele telefoons worden berichten verstuurd met de vraag wie snel geld wil verdienen (in die tijd nog vooral BlackBerry Ping). In verhoren verklaren *money mules* dat het heel gewoon was dat er om pasjes werd gevraagd: 'Iedereen in Nederland doet dit toch.' Ook is er sprake van een aanzuigeffect: mensen die snel geld nodig hebben, vragen zelf of ze hun pinpas kunnen afgeven om zo een percentage te krijgen.

Ik dacht een unieke casus te pakken te hebben, maar dat bleek behoorlijk mee te vallen. Ik analyseerde daarna met diverse (intern)nationale onderzoekers nog tientallen opsporingsonderzoeken naar phishing in Nederland, Duitsland, het VK en de VS en deed dit later ook voor cybercriminele netwerken die andere delicten plegen. Steevast kwamen we tot de conclusie dat cybercriminelen inderdaad gebruik maken van de voordelen van digitalisering: ze weten slim gebruik te maken

van criminele ontmoetingsplaatsen op het *dark web*, hacking fora en tegenwoordig ook socialmedia-platformen als Instagram, Snapchat en Telegram. Daardoor kunnen ze een grote range aan specialisten inhuren en zo snel de criminele mogelijkheden van hun netwerk uitbreiden. En ja, met name ransomware-netwerken zijn heel internationaal en er is sprake van een heel ecosysteem waarbij er een paar grote ontwikkelaars zijn en tal van 'onderaannemers' die (onderdelen van) de aanval uitvoeren (zie bijvoorbeeld de crime script-analyse van Matthijsse et al., 2023). Maar betekent dit dan ook per definitie dat alle cybercriminele netwerken dat doen? Nee. Ook leden van cybercriminele netwerken zijn net mensen en de traditionele processen rondom vertrouwen lijken ook binnen dit soort netwerken nog steeds van groot belang. Met name offline sociale banden blijken nog steeds van groot belang te zijn binnen dit soort netwerken. Zeker voor de kernleden, maar ook voor het inzetten van belangrijke facilitators. Dit is nogal van belang voor het opsporingsbeleid in Nederland. Immers: het is maar de vraag of dergelijke criminele netwerken nog wel vallen binnen de scope van het landelijke cybercrimeteam. En zeker in de tijd dat ik mijn proefschrift schreef, was dit hét team dat verantwoordelijk was voor de aanpak van cybercriminele netwerken. In deel 4 van deze oratie zal ik laten zien dat er gelukkig wel het een en ander veranderd is binnen de politie en dat nu ook teams op lokaal niveau belast zijn met het opsporen en verstoren van cybercriminele netwerken.

Pathways into cybercrime

Een tweede voorbeeld. Dat gaat over mijn tweede wetenschappelijke liefde: *pathways into cybercrime*. Dit voorbeeld zal een stuk korter zijn, omdat deze onderzoekslijn nog pas net is opgezet en ik hier met verschillende collega's de komende jaren nog hard aan zal werken.

Eerst een situatieschets: Ik zit in een kraakpand in een niet al te best deel van een middelgrote stad in het westen van Nederland al een paar uur te praten met een criminele hacker (in tegenstelling dus tot de 'ethisch hacker' die dezelfde skills inzet voor het verbeteren van cybersecurity). Ik leerde hem kennen via de hacker met wie ik een paar weken daar voor sprak. In de kamer waar we zitten, hangen lakens voor het raam als gordijnen. Het gesprek duurt meer dan vier uur en deze respondent vertelt in detail over al zijn legale en illegale 'avonturen' als het gaat om het 'creatief' gebruiken van ICT om toegang te krijgen tot alles wat hij maar wil. Toen ik hem vroeg hoe en waar hij al zijn vaardigheden had geleerd, antwoordde hij simpelweg: 'Het staat allemaal op Google en YouTube.'

Ik realiseerde me tijdens dit gesprek dat dit de zoveelste geïnterviewde was die precies hetzelfde antwoord gaf. Dat nu toch wel opvallende antwoord heb ik daarna gehoord van alle respondenten die ik sprak: zonder uitzondering noemen ze deze en andere voor iedereen toegankelijke en veelgebruikte online platformen als dé manier om de wereld van hacken en oplichten binnen te komen. Zonder het te beseffen, kwamen ze op jonge leeftijd en heel gemakkelijk terecht in een wereldwijde subcultuur waar 'iedereen hackt en iedereen [criminele] kennis deelt'. In deze subcultuur zijn er geen tekenen dat ethische grenzen worden overschreden en wetten worden overtreden. Voor degenen die geïnspireerd zijn door de mogelijkheden die deze subcultuur biedt, is het gemakkelijk om links te vinden naar openbare online hack- en oplichtingsfora. En via die plekken kan je dan weer terechtkomen op de hack- en oplichtingsfora die alleen 'op uitnodiging' zijn. Op dergelijke online ontmoetingsplaatsen vinden ze uiteindelijk gelijkgestemden en worden ze gerekruteerd door actieve cybercriminele netwerken.

De belangrijkste les in dit verhaal is dat ik op een stukje van een ontwikkelpad naar cybercriminaliteit stuitte dat tot nu toe over het hoofd was gezien: Google en YouTube. Deze mainstream platformen, die door bijna iedereen ter wereld worden gebruikt, spelen blijkbaar ook een rol binnen de ontwikkelpaden van jonge plegers van cybercrimes en – belangrijker – kunnen worden gezien als de plek waar geïnteresseerde personen hun eerste stappen zetten in de wereld van cybercri-

minaliteit. Het is van groot belang om te onderzoeken hoe deze stap twee bekende en belangrijke factoren bij de betrokkenheid van criminele netwerken – het belang van online en offline sociale banden en online en offline ontmoetingsplaatsen – beinvloedt.

Deze ontdekking van een nieuwe en belangrijke stap binnen de ontwikkelpaden van jonge criminele hackers is afkomstig uit mijn veldnotities van een project waar ik enkele jaren aan gewerkt heb en dat mij door heel Nederland heeft gebracht, meestal in het weekend of 's avonds. Het laat ook duidelijk het belang zien van kwalitatief onderzoek naar nieuwe fenomenen zoals cybercriminaliteit: zonder interviews zouden deze basismechanismen nooit zijn geïdentificeerd, omdat ze zo anders zijn dan traditionele betrokkenheidsmechanismen.

Dit is precies de reden waarom ik deze bevinding centraal heb gemaakt in een – gelukkig gehonoreerde – ERC-aanvraag voor een vijfjarig onderzoeksprogramma: het is van ontzettend groot belang om meer zicht te krijgen op de paden in en uit de cybercriminaliteit. Het CybercrimePathways-programma gaat daarom fundamentele kennis opdoen over deze ontwikkelpaden. Bovendien wil ik bestaande theorieën die zijn ontwikkeld in het predigitale tijdperk toekomstbestendig maken door ze empirisch te toetsen. Er kunnen verschillende theorieën gebruikt worden om de *pathways into* en *pathways out of* (cyber)criminaliteit te bestuderen. Voorbeelden zijn de sociale leertheorie van Aker, de neutralisatietheorie van Matza en Sykes en de *general theory of crime* van Hirschi en Gottfredson. Mijns inziens is met name de levensloopcriminologie hier van belang. Levensloopcriminologie richt zich op individuele ontwikkelingen in criminaliteit over tijd, en in het bijzonder op de factoren die het ontwikkelpad van een individuele pleger beinvloeden (Farrington, 2003; Blokland & Nieuwbeerta, 2010). Verder heb ik al in tal van eerdere studies gebruik gemaakt van het concept van sociale gelegenheidsstructuren – of in het geval van cybercriminelen 'online gelegenheidsstructuren'. Kleemans en Van de Bunt (1999) benadrukten het belang van sociale relaties en leggen uit waarom criminaliteit en daders binnen een sociale en maatschappelijke context moeten worden bekeken, waarbij de belangrijkste aspecten zijn: de plegers zelf, de illegale partnerschappen waarin ze opereren en de interactie met hun sociale omgeving. Kleemans en De Poot (2008) hanteren het concept 'social opportunity structure' en de belangrijke rol die dergelijke structuren spelen in criminele netwerken. Dit is van groot belang, aangezien de meeste criminelen niet alleen werken. Het feit dat de meeste criminelen met anderen samenwerken, is al lang erkend in de criminologie (Shaw & McKay, 1931; Sutherland, 1937; Reiss, 1988; Reiss & Farrington, 1991). Hetzelfde geldt voor cybercriminelen. Hoewel sommige hackers misschien alleen kunnen werken, hebben onderzoeken aangetoond dat er over het algemeen meerdere personen met verschillende vaardigheden nodig zijn om financieel gemotiveerde cyberaanvallen uit te voeren, zoals phishing-, malware- en ransomware-aanvallen (Grabosky, 2007; Broadhurst et al., 2014; Hutchings, 2014, Lusthaus, 2016; Leukfeldt & Holt, 2020). Het is daarom belangrijk om te begrijpen hoe iemand betrokken raakt bij criminaliteit en of deze theorieën nog wel te gebruiken zijn in een gedigitaliseerde samenleving.

We zijn daarom begonnen met een systematische review van de literatuur (Loggen et al., 2023, 2024) en zullen de komende tijd interviews met experts afnemen om een duidelijk beeld te formuleren van de bestaande kennis over paden naar en uit cybercriminaliteit. Vervolgens nemen we interviews af met cybercriminelen en ethische hackers, analyseren we opsporingsonderzoeken, maken we gebruik van data van de reclassering en voeren we een vragenlijstonderzoek uit onder Nederlandse jongeren om een zo volledig mogelijk beeld te krijgen van de ontwikkelpaden van jonge cybercriminelen. Dit is allemaal input voor het opzetten van een reeks online veldexperimenten in het laatste deel van het onderzoeksprogramma. Op de online plekken waar potentiële jonge cybercriminelen daadwerkelijk rondhangen, zullen we experimenteel onderzoeken hoe we de *pathways* naar cybercrime kunnen verstoren en

pathways weg uit de cybercrime kunnen versterken. Hiermee levert het programma niet alleen een bijdrage aan onze empirische kennis van deze specifieke dadergroep, maar kunnen er *evidence based* interventies worden getest die meteen gebruikt kunnen worden door de praktijk. Pilotstudies op Instagram – waarbij we meer leerden over hoe jongeren precies worden geronseld (Bekkers & Leukfeldt, 2022; Bekkers et al., 2023) – en op Google (Moneva et al., 2023; Moneva & Leukfeldt, 2023) en YouTube (Moneva et al., 2024) – waarbij we keken hoe personen die actief op zoek zijn naar informatie over hacken of tools die gebruikt kunnen worden om cyberaanvallen uit te voeren – laten zien dat dergelijke platformen van grote waarde kunnen zijn voor criminologisch onderzoek en dat de doelgroep daadwerkelijk bereikt kan worden.

4. Meten is weten: de strafrechtketen door de jaren heen

Cyberaanvallen zijn dus veelvoorkomend, slachtofferaantallen zijn hoog en er is een grote variatie aan plegers. Een belangrijke vraag is dan ook hoe het zit met de aanpak van cybercrime. Laat ik beginnen met duidelijk maken dat die aanpak zowel uit de publieke als private hoek moet komen. Zoals Boes en ik in 2015 al schreven, zijn er diverse lagen bij het beschermen tegen cyberaanvallen. Zo is er de eerste laag, waarin burgers en bedrijven zelf een rol hebben door bijvoorbeeld adequate beveiligingsmaatregelen te nemen en zich online niet onveilig te gedragen (empirisch onderzoek laat dan weer zien dat dit heel moeilijk is voor eindgebruikers – zie Van 't Hoff-de Goede et al., 2023; Van der Kleij et al., 2023; Bekkers et al., 2023). Dan is er de tweede laag van organisaties die wellicht niet primair bezig zijn met cybersecurity, maar wel degelijk een rol hebben bij het veilig houden van internet. Voorbeelden zijn Internet Service Providers, hostingbedrijven en online platformen zoals Facebook en Telegram. En zoals ik met collega Spithoven heb laten zien, is er ook een belangrijke rol weggelegd voor allerlei traditionele partijen die zich bezighouden met veiligheid, zoals gemeenten en het PVO (platform veilig ondernemen) (bijvoorbeeld Leukfeldt et al., 2020). Daarna komt de derde en laatste laag van bescherming: politie en justitie en cybersecuritybedrijven. Ik sta nu alleen stil bij de meest traditionele speler in het geheel: de politie.

Problemen in de strafrechtketen: hoge instroom, hoge uitstroom?[4]

In 2021 kwam het Wetenschappelijk Onderzoek- en Data Centrum (WODC) van het ministerie van Justitie en Veiligheid met een interessante onderzoeksvraag. Kortgezegd komt die neer op: waarom zien we aan het eind van de strafrechtketen zo weinig veroordeelde cybercriminelen, terwijl we weten dat de slachtofferaantallen hoog zijn? Deze vraag is niet alleen interessant omdat het inderdaad goed is om te weten waar het verschil vandaan komt (naast het gegeven dat enkele daders veel verschillende slachtoffers kunnen maken en dat daders ook vanuit het buitenland kunnen opereren), maar ook omdat diezelfde vraag ruim tien jaar eerder al aanleiding voor mij was om onderzoek te doen op dit gebied (Leukfeldt et al., 2013a, 2013b). Toen was de vraag afkomstig van de net ingestelde cybercrime officieren van justitie die hun werkaanbod nog wat gering vonden. Ik was vooral benieuwd of we ruim tien jaar later grote verschillen zouden zien in de afhandeling van cybercrimes en de problemen binnen de strafrechtketen.

Uit het onderzoek dat we in 2013 publiceerden (Leukfeldt et al., 2013a) bleek dat er grofweg drie oorzaken ten grondslag lagen aan het grote verschil in het aantal slachtoffers en het aantal veroordelingen: een lage aangiftebereidheid, de organisatie van politie en justitie die nog onvoldoende is ingericht om dergelijke zaken effectief op te pakken, en de complexiteit van zaken.[5] De lage aangiftebereidheid en de organisatie van de politie op het gebied van de aanpak van online criminaliteit kunnen ervoor zorgen dat een deel van de zaken nooit de straf-

4 Dit deel van de oratie is grotendeels gebaseerd op de onderzoeksrapportage van Ruiter et al. (2023) en een bijdrage van Leukfeldt et al. (n.n.g.).

5 Deze zaken zien we overigens ook terug bij offline vormen van criminaliteit en zijn dus niet uniek voor cybercrimes, maar studies – en in feite alle respondenten die ik sprak in onze verschillende onderzoeken hiernaar – wijzen erop dat de problematiek bij cybercrimes erger kan zijn dan bij de traditionele delicten vanwege de onbekendheid met deze delicten.

rechtketen instroomt. Daarnaast zorgt de organisatie van de politie al dan niet in combinatie met de complexiteit van zaken mogelijk voor een beperkte doorstroom van zaken binnen de politieorganisatie zelf en tussen de politie en het Openbaar Ministerie. Ten slotte kan de complexiteit van zaken er niet alleen voor zorgen dat het lang duurt voordat de politie een zaak overdraagt aan het OM, maar zorgt de schaalbaarheid in dergelijke zaken mogelijk voor een schijnbare tegenstelling tussen de hoge aantallen slachtoffers in enquêtes en het geringe aantal verdachten in de strafrechtketen: enkele daders kunnen grote aantallen slachtoffers maken. De schaalbaarheid van online delicten is immers anders dan bij traditionele offline delicten.

Ruim tien jaar later onderzochten we dit dus nogmaals (Ruiter et al., 2023). Er zijn de laatste tien jaar in Nederland diverse ontwikkelingen geweest met betrekking tot de aanpak van cybercrimes. Zo is het nationale Team High Tech Crime flink uitgebreid, zijn er gespecialiseerde cybercrimeteams op eenheidsniveau bijgekomen, wordt ingezet op cyberdadergerichte interventies zoals Hack_Right en zijn er allerlei lokale initiatieven om de aangiftebereidheid te verhogen en de aanpak te verbeteren (Schiks et al., 2021, 2022).

Opvallend is dat veel van de knelpunten die tien jaar geleden geconstateerd zijn en al vaak zijn beschreven in de literatuur nog steeds door respondenten benoemd worden (Cross et al., 2016; Button et al., 2020). Nog steeds is er volgens respondenten bijvoorbeeld sprake van een lage kwaliteit van aangifte, doordat intakemedewerkers te weinig kennis hebben om zaken goed op te nemen. Dit is – na een lage aangiftebereidheid waardoor cybercrimes überhaupt niet de strafrechtketen instromen – een belangrijke bottleneck in de aanpak van cybercrime. Een slechte kwaliteit van de intake zorgt er immers voor dat de kans op een succesvolle tweede cruciale stap in dit proces nog lager wordt: de *case screeners* maken gebruik van de informatie van de intakemedewerkers om te beoordelen of een aangifte voldoende opsporingsindicatie heeft om door te zetten naar een opsporingsteam. Een nog niet eerder genoemd punt is daarbij dat de kwaliteit van de aangifte ook afhankelijk is van (de kennis van) de aangever. En burgers weten zelf ook lang niet altijd precies wat er is gebeurd. Des te belangrijker is het voor intakemedewerkers om de juiste vragen te stellen.

Een tweede onveranderd knelpunt is de *case screening*. Nog steeds is de conclusie van experts uit de praktijk dat zaken onnodig afvallen bij de case screening (Leukfeldt er al., 2013). Niet alleen omdat de kwaliteit van de aangifte onnodig laag is, maar ook omdat internet volgens respondenten veel afschermmogelijkheden biedt, waardoor het moeilijker is om een verdachte in beeld te krijgen en het überhaupt lastiger is om op voorhand in te schatten of een zaak voldoende opsporingsindicatie bevat doordat ook case screeners lang niet altijd sporen op waarde weten te schatten. Nieuw bij deze stap is dat respondenten aangeven dat de hoogte van de financiële schade een belangrijke reden is dat veel zaken afvallen bij de case screening. Daarbij bestaan er verschillen tussen door respondenten genoemde bedragen.

Ten slotte zagen we ook een aantal oude bekende knelpunten terug binnen de opsporing. Ook nu worden gebrek aan prioriteit, capaciteit, gebrek aan kennis en de complexiteit van zaken als belangrijke knelpunten genoemd (zie Hadlington et al., 2018; Harkin et al., 2018; Boekhoorn, 2019; Graham et al., 2020). Op de prioritering ga ik hier dieper in. Het is namelijk opvallend dat gebrek aan prioriteit nog steeds genoemd wordt als belangrijk knelpunt. Cybercrimes zijn immers gegaan van prioriteit 3 (in feite de categorie 'niets mee doen') naar prioriteit 1 ('in principe altijd oppakken'). Respondenten geven echter aan dat traditionele delicten in de praktijk nog steeds voorrang krijgen. Niet alleen de 'bloed = spoed'-zaken gaan voor, maar in algemene zin lijken traditionele delicten die ook in de categorie 'prioriteit 1' vallen voor te gaan. Opgemerkt moet worden dat respondenten aangeven dat politieteams in de praktijk lang niet altijd zelf kunnen kiezen of ze een traditioneel delict of een online delict oppakken. In het geval van een aanhouding (bijvoorbeeld bij een winkeldiefstal), moet die verdachte simpelweg 'afgehandeld' worden.

Een nieuwe bevinding bij knelpunten binnen de opsporing is een gebrek aan eigenaarschap (ofwel: welk team moet de zaak oppakken?). Het is bij online criminaliteit op voorhand niet altijd duidelijk waar het delict heeft plaatsgevonden, aangezien vaak nog onduidelijk is vanuit waar de dader opereert en de dader bij online delicten ook op meerdere plaatsen tegelijk in Nederland slachtoffers kan maken. In het geval van online criminaliteit komen aangiften daarom binnen in de woonplaats van de aangever(s), hetgeen niet noodzakelijkerwijs de plaats is vanuit waar de dader opereert. Het knelpunt dat door respondenten wordt genoemd, speelt een rol wanneer een zaak wordt overgedragen aan een andere eenheid, bijvoorbeeld omdat duidelijk is dat de verdachte niet in dezelfde eenheid als het slachtoffer woont of wanneer sprake is van meerdere slachtoffers en/of verdachten in verschillende eenheden.

Alles overziend is het dus de vraag hoe het komt dat ondanks belangrijke veranderingen in de organisatie van de bestrijding van cybercrime binnen de politie veel van de geconstateerde knelpunten van tien jaar geleden min of meer dezelfde zijn als die van vandaag de dag. Komt dat doordat de veranderingen niet ingrijpend genoeg waren (moet er *meer* gebeuren?), waren de veranderingen niet effectief, of komt het simpelweg doordat het werkaanbod van cybercrimes de afgelopen tien jaar ook enorm gestegen is? Vragen waar wat mij betreft nog geen antwoord op is en waarom empirisch onderzoek van belang is, waarbij we bestuderen wat werkt en waarom het werkt.

Alternatieve interventies

Er zijn dus nog genoeg problemen binnen de strafrechtketen. Naast de opschaling van politieteams is er een andere belangrijke trend te zien binnen de strafrechtketen: de inzet van zogenaamde alternatieve interventies. Ik zie veel innovatieve projecten voorbijkomen die zijn opgezet met de beste bedoelingen. Maar zoals ik eerder al aangaf, hoeft dit niet per se te betekenen dat die projecten daadwerkelijk het effect hebben zoals ooit beoogd. Nu is er een behoorlijk verschil tussen de projecten. Zie voor een overzicht bijvoorbeeld onze rapporten over de parels in de lokale aanpak van cybercrime (Schiks et al., 2022) en de evaluaties die we deden voor het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) (Bluhm et al., 2024). Rijp en (vooral veel) groen door elkaar. Op al die kleinere projecten ga ik hier niet in. Ik neem twee wat grotere voorbeelden, namelijk Hack_Right en het gebruik van GoogleAds door de politie.

Eerst Hack_Right. Uit ons onderzoek blijkt dat de aanleiding voor Hack_Right als volgt is: een toename in het aantal verdachten van computercriminaliteit, het verschil in profiel tussen daders van computercriminaliteit en daders van traditionele delicten en het gebrek aan werkzame interventies voor deze doelgroep. Hack_Right kent twee doelen, namelijk het voorkomen van recidive bij deelnemers en het ICT-talent van deelnemers ontwikkelen binnen de kaders van de wet. De hoofddoelen probeert Hack_Right te bereiken door in te spelen op verschillende criminogene factoren voor cybercriminaliteit.

We hebben van deze interventie geen effectevaluatie gedaan, maar wel een plan- en procesevaluatie. Daarvoor analyseerden we beleidsdocumenten, interviewden we de ontwikkelaars, uitvoerders en jongeren die Hack_Right doorliepen (Schiks et al., 2021, 2023). We schreven een genuanceerd rapport waarin tot in detail de uitvoering van Hack_Right werd beschreven. Wat ik vooral opvallend vond, was het grote enthousiasme van alle betrokkenen bij deze interventie. De deelnemende jongeren waren soms wat kritischer, maar over het algemeen zagen ze zeker in dat deze interventie een tweede kans voor ze was (opvallend was dat de meeste jongeren het vooral erg leken te vinden dat hun apparatuur zo lang in beslag was genomen).

Een kritische kanttekening die we maakten, was echter ook meteen een belangrijke: de wetenschappelijke basis om Hack_Right te starten ontbreekt grotendeels. Het klopt dat er nog geen effectieve interventies zijn die specifiek gericht zijn op cybercriminelen, maar er is nog maar erg weinig empirisch

onderzoek naar kenmerken van cybercriminelen. We weten dus simpelweg niet, als we het hebben over cybercriminelen, of we het hebben over een groep daders met een afwijkend profiel ten opzichte van de daders van allerlei vormen van traditionele offline delicten. Er zijn nog bijna geen studies gedaan naar criminogene factoren bij dit type dader en er is dus nog veel onbekend. Er is zelfs discussie over of traditionele beschermende factoren – zoals het hebben van werk – nog wel een beschermende factor is; werk in de ICT-sector zou ook juist gelegenheden kunnen bieden om cyberdelicten te plegen. Dat er nog weinig empirisch onderzoek gedaan is naar de kenmerken van cybercriminelen, valt de initiatiefnemers van Hack_Right natuurlijk niet aan te rekenen en hoeft ook niet te betekenen dat er geen nieuwe interventie nodig is. Duidelijk is dat Hack_Right grotendeels is ontstaan vanuit een praktijkvraag: politie, OM, reclassering en Halt signaleren dat er een grote instroom van verdachten van cybercrimes is en zoeken naar de beste interventie om recidive te voorkomen. Wel concluderen we dat er rekening mee moet worden gehouden dat toekomstig wetenschappelijk onderzoek naar kenmerken van cybercriminelen kan uitwijzen dat de kenmerken van cybercriminelen niet of nauwelijks verschillen van daders van traditionele vormen van criminaliteit.

Dan GoogleAds. Iets dieper wil ik ingaan op studies rondom een politie-interventie waarbij jongeren via GoogleAds – advertenties op Google dus – gericht worden voorgelicht over de gevolgen van het uitvoeren van DDoS-aanvallen (aanvallen waarbij online systemen worden platgelegd door er heel veel informatie(verzoeken) heen te sturen). De GoogleAds-campagne past goed binnen de situationele criminaliteitspreventie (SCP) (Clarke, 1980). Binnen SCP zijn er vijf mechanismen met in totaal 25 technieken ontwikkeld die criminaliteit tegen moeten gaan. De mechanismen zijn: *increase the effort to commit crime*, *increase the risk of being detected when committing crime*, *reduce the rewards of crime*, *reduce provocations to potential offenders*, *and remove excuses for non-compliance with the norm* (Clarke & Eck 2003; Cornish & Clarke 2003). In de GoogleAds-campagne worden de advertenties gebruikt om mensen die op Google zoeken met DDoS-gerelateerde zoektermen voor te lichten over de gevolgen van het uitvoeren DDoS-aanvallen. Dit is in lijn met de 23ste maatregel binnen SCP: *alerting consciences.*

Collier en collega's lieten in 2019 zien dat toen de National Crime Agency in het Verenigd Koninkrijk een voorlichtingscampagne gericht op potentiële plegers van DDoS-aanvallen uitvoerde er een 'drop' in het volume van DDoS-aanvallen in het VK zichtbaar was. Uiteraard ging dit als een lopend vuurtje door politieland en ook andere landen wilden deze manier om potentiële plegers van DDoS-aanvallen voor te lichten en af te schrikken inzetten. Dankzij goede contacten bij de Nationale Politie in Nederland wisten collega Moneva en ikzelf ervoor te zorgen dat we betrokken werden bij het opzetten van de Nederlandse campagne. Een mooie anekdote die ik zowel wetenschappers als praktijkmensen niet wil onthouden: er waren bij de politie wel wat zorgen, omdat wij – de wetenschappers – het proces wellicht te veel gingen vertragen, doordat het nu allemaal 'wetenschappelijk goed' moest gebeuren. Gelukkig was het juist andersom: door de interne bureaucratie binnen de politie duurde het nog een tijd voordat we daadwerkelijk de interventie uit konden zetten.

Onze voornaamste bijdrage – en ook meteen het verschil met de campagne in het Verenigd Koninkrijk waarbij de politie niet met de onderzoekers had samengewerkt – was dat we begonnen met een pilotstudie waarbij we verschillende teksten testten die te lezen waren in de advertenties: van de klassieke afschrikwekkende tekst die ook in het VK gebruikt was ('DDoS-aanval is strafbaar!') tot een meer teasende en *blamende* tekst ('DDoS-aanval verpest het voor iedereen') (zie Moneva et al., 2023). Daarnaast hebben we in een tweede studie het effect van de campagne op het volume van DDoS-aanvallen bekeken (Moneva & Leukfeldt, 2023).

We stelden samen met politiemedewerkers een lijst op met zoektermen. Die lijst bestond onder andere uit op dat moment actieve tools om DDoS-aanvallen mee uit te voeren. Zodra gebruikers via Google zoeken op een van deze zoektermen, krijgt de gebruiker een van onze advertenties te zien (dus iemand die zoekt naar een tool om een dergelijke aanval uit te voeren krijgt als bovenste zoekresultaat een advertentie met informatie over de gevolgen van een DDoS-aanval).
Tijdens het eerste deel van ons onderzoek, waarbij we keken naar de interactie van gebruikers met verschillende advertenties, werden de advertenties in een campagne van veertien weken in totaal 71.475 keer getoond. Daarnaast bleek dat er op 4457 van die advertenties was geklikt om meer informatie te krijgen (een *engagement ratio* van 6,2%).

Een van de conclusies die we trokken, was dat dit klaarblijkelijk een heel interessante manier is om de doelgroep die zoekt naar informatie om DDoS-aanvallen te plegen te bereiken. Al helemaal als je ook kijkt naar de kosten: die waren relatief laag, terwijl de doelgroep bereikt kan worden op een moment waarop ze daadwerkelijk stappen zetten om mogelijk een delict te plegen. Verder liet de studie zien dat dit een hele nieuwe manier is om inzicht te krijgen in de doelgroep. Google levert informatie over de achtergrondkenmerken van de 'zoekers' en over op welke moment gezocht (en geklikt) wordt (en dat bleek het vaakst te zijn na middernacht in het weekend).

De vervolgstap was om te kijken of de campagne daadwerkelijk een effect had op het volume van DDoS-aanvallen in Nederland. In de tussentijd waren meerdere landen geïnteresseerd in het uitvoeren van de interventie en kregen we de mogelijkheid om mee te kijken naar zeven campagnes in totaal zes Europese landen. In Moneva en Leukfeldt (2023) presenteren we de resultaten van deze quasi-experimentele en cross-nationale evaluatie. We maakten gebruik van data afkomstig van het Cambridge Cybercrime Centre die inzicht geven in het volume van DDoS-aanvallen voor en tijdens de campagne (zie Collier et al., 2019; Thomas et al., 2017). Dit deden we in totaal in twaalf landen: zes voerden de campagne uit en zes niet. De resultaten waren echter niet zo rooskleurig als die in het VK een paar jaar eerder (Collier et al., 2019). Wat blijkt namelijk? In tien landen zien we geen significant effect, in één land zien we een significante afname en in één land een significante toename. Wel is duidelijk te zien dat de trendlijn in de meeste landen tijdens de campagne daalt of minimaal gelijkt blijft. Meer over de details van deze analyse is uiteraard te vinden in de al aangehaalde studie. Belangrijker is dat we dus niet 'even makkelijk' konden aantonen dat deze veelbelovende interventie het beoogde effect heeft. Nu zijn er al tal van redenen te bedenken waarom Collier en collega's wel een effect zagen en wij niet (in het VK waren op dat moment bijvoorbeeld meerdere interventies in gebruik) en is het ook vooral zaak om meer gedetailleerde data te krijgen over de DDoS-aanvallen, zodat we veel beter kunnen kijken naar de aanvallen die deze specifieke doelgroep waarschijnlijk uitvoert, maar de belangrijkste les die ik leerde, was dat dergelijke interventies alleen al interessant zijn, omdat je op deze manier heel direct (en snel en goedkoop) bij geïnteresseerde jongeren kan komen. Je gebruikt de platformen die ze zelf gebruiken om ze te informeren. Het is wat mij betreft dan ook vooral zaak om veel meer te leren wat wel en niet werkt bij het gebruik van online platformen binnen interventies. Om die reden gaan we niet alleen door met de studies op Google, maar ook op YouTube, Instagram, Snapchat en Telegram.

5. Op naar de volgende stap: naar een empirisch onderbouwde aanpak van cybercrime

Het mag duidelijk zijn: cybercrime is groeiende en we moeten komen tot een betere aanpak ervan. Goede ideeën zijn er in overvloed, maar of die ideeën ook enig effect hebben, is onduidelijk. We moeten toe naar een meer empirisch onderbouwde aanpak van cybercrime. Met alleen een goed idee komen we er niet. Cybercrime is '*here to stay*' en we moeten dus investeren in een goede kennisbasis. De bijdrage van de wetenschap zie ik op twee manieren: empirisch onderzoek naar het fenomeen cybercrime en onderzoek naar het effect van interventies.

Empirisch onderzoek naar het fenomeen van cybercrime is hard nodig om te begrijpen hoe de aanpak er überhaupt uit moet zien. Om te weten waar de focus moet liggen, is inzicht nodig in de daders, de ingroeimechanismen, de manier waarop ze samenwerken in netwerken, maar ook in de slachtoffers, hun risicofactoren, de impact en de gevolgen. Het gaat dus om de lange termijn en dat vereist meerjarige samenhangende onderzoeksprogramma's. Zolang die er niet zijn, bouw ik zelf langs twee lijnen verder. Uiteraard ga ik verder met de onderzoeken naar de aard van cybercriminele netwerken. Met Edward Kleemans, Robby Roks, Jonathan Lusthaus, Tom Holt en hopelijk in de toekomst vele anderen blijven we empirisch onderzoeken hoe de netwerken er nou precies uitzien. Verder begeleid ik momenteel samen met Bibi van de Berg promovendus Marco Romagna bij zijn onderzoek naar hacktivisten: wat zijn daar nou de ingroeimechanismen en hoe zien samenwerkingsverbanden eruit? Sifra Matthijsse voert een mooi promotieonderzoek uit naar ransomware. Ze ontwikkelde al een crime script om inzichtelijk te maken welke stappen cybercriminelen zetten om dat delict uit te voeren en momenteel bestuderen we waarom slachtoffers wel/niet betalen, onderhandelen en melding maken bij de politie. Samen met Susanne van 't Hoff-de Goede en Jelle Brands mag ik haar begeleiden. Hannah Kool en Joeri Loggen – die ik beide met Asier Moneva begeleid – doen promotieonderzoek naar de ingroeimechanismen bij verschillende vormen van cybercrime. Hannah kijkt daarbij specifiek naar de rol van CaaS als onderdeel van de *pathway into cybercrime*. Joeri zoomt in op de jonge plegers van online oplichting. Bij de begeleiding van Joeri is ook Arjan Blokland betrokken. Luuk Bekkers doet dan weer onderzoek naar een specifieke laag van veel cybercriminele netwerken: de *money mules.* Samen met Remco Spithoven en Edward Kleemans kijken we daarbij naar hoe het ronselproces er precies uitziet en ook binnen dit promotieonderzoek is er aandacht voor de aard van de netwerken. Dan is er natuurlijk nog de net gestarte ERC-beurs, waardoor de komende vijf jaar meerdere mensen onderzoek gaan doen naar de *pathways into* en *pathways out of* cybercrime. Jildau Borwell is daarbij de *linking pin* met de politie, omdat we nauw samenwerken met het Cybercrime Offender Prevention Squad van de Nationale Politie.

Dan het onderzoeken van het effect van interventies. Er zijn momenteel tal van interventies die worden ingezet om potentiële of beginnende cybercriminelen te informeren, om het cybercriminelen moeilijker te maken delicten te plegen of om slachtoffers weerbaarder te maken. In deze oratie heb ik al twee van dergelijke interventies behandeld: Hack_Right en het inzetten van GoogleAds door de politie. Momenteel zijn we zelf ook nog bezig met het opzetten van soortgelijke onderzoeken naar interventies op YouTube, maar ook kijken we kritisch mee naar interventies zoals ReBootCMP en de stopgesprekken met *money mules*. Ook kijken we naar de mogelijkheden om online platformen juist te gebruiken om slachtoffers te bereiken. Binnen het promotieonderzoek van Sifra Matthijsse kijken we bijvoorbeeld naar het online hulpzoekgedrag van slachtoffers om te leren hoe we deze doelgroep kunnen bereiken direct na hun slachtofferschap. Merel van Leuken is net gestart met een promotieonderzoek naar de alternatieve afdoening van online fraude, waarbij slachtoffers via een civiele procedure geld terug proberen te krijgen van de vermeende oplichters. Allemaal interventies waarbij we als wetenschappers nauw samenwerken met de praktijk. Alleen op die manier kunnen we samen verder komen. Het mag duidelijk zijn dat de lijst met lopende projecten binnen deze lijn lang niet zo lang is als die binnen de lijn 'empirisch onderzoek naar het fenomeen'. Ik hoop dan ook dat we met de leerstoel Governing Cybercrime een bijdrage kunnen leveren aan het stimuleren van onderzoek op juist dit gebied om zo te komen tot een empirisch onderbouwde aanpak van cybercrime.

Tot slot wil ik nog stilstaan bij de rol van het onderwijs en in het bijzonder de bachelor Cybercrime & Cybersecurity van onze universiteit. Het unieke aan deze bachelor is namelijk dat deze vanuit drie faculteiten is ontwikkeld en wordt gegeven. Uniek in Nederland, maar broodnodig. Cybercrime en cybersecurity moet je immers niet vanuit één discipline benaderen:

het zijn zowel technische, juridische, bestuurskundige als criminologische aspecten die een rol spelen bij het begrijpen en aanpakken van cybercrime. De gezamenlijke bachelor zal er niet alleen voor zorgen dat er een nieuwe generatie studenten de arbeidsmarkt op komt voor wie het normaal is om vanuit – en in samenwerking met – verschillende disciplines naar een cyberprobleem te kijken, maar zal er ook voor zorgen dat er een brede community ontstaat van mensen die binnen de verschillende faculteiten bezig zijn met onderwijs en/of onderzoek naar cybercrime en cybersecurity.

6. Dankwoord

Ik dank het college van bestuur van de Universiteit Leiden en de besturen van de Faculteit Governance & Global Affairs (ISGA) en de Faculteit Rechtsgeleerdheid voor mijn aanstelling als bijzonder hoogleraar, en voor het in mij gestelde vertrouwen. Ook bedank ik het bestuur van het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR), die deze bijzondere leerstoel heeft gevestigd en financiert. In het bijzonder dank ik Erwin Muller, Joanne van der Leun, Beate Volker, Peter van der Laan, Bibi van den Berg, Maarten Kunst en Jan Crijns voor hun inspanningen rondom de totstandkoming van deze leerstoel.

Verder ben ik dank verschuldigd aan een heleboel getalenteerde mensen waar ik de afgelopen jaren mee heb samengewerkt. Zonder de samenwerking met jullie waren er nooit zo veel mooie onderzoeken uitgevoerd en had ik hier vandaag niet gestaan. Ik begin bij het begin: mijn promotor en leidinggevende toen ik nog een beginnend onderzoeker was, Wouter Stol. Dank dat je hebt laten zien dat onderzoek doen echt heel leuk is en dat goed wetenschappelijk onderzoek en impact maken in de praktijk best te combineren zijn. Eenzelfde rol hebben iets later in mijn carrière Edward Kleemans en Catrien Bijleveld gespeeld. Edward, met jou werk ik al samen sinds mijn proefschrift en we hebben inmiddels tal van gezamenlijke projecten uitgevoerd. Dank dat je al je ervaring met me gedeeld hebt de afgelopen jaren. Catrien, jij hebt me aangenomen bij het NSCR en dankzij jouw enorme energie en stimulans zijn we vanaf toen echt gaan bouwen aan criminologisch onderzoek naar cybercrime in Nederland en daarbuiten. Dank ook aan mijn collega's van de Haagse Hogeschool. Allereerst het college van bestuur en in het bijzonder Elisabeth Minneman voor het vertrouwen in mij waardoor dit allemaal te combineren is. Volgens mij laten we zien dat fundamenteel wetenschappelijk onderzoek en praktijkgericht onderzoek heel goed samengaan. In de praktijk zie ik dat natuurlijk dagelijks door alle mensen op het NSCR en de HHS waar ik mee samenwerk aan verschillende projecten. Dit gaan we de komende tijd uitbouwen met collega's van de Universiteit Leiden, in het bijzonder natuurlijk de collega's van de faculteiten ISGA en Strafrecht & Criminologie en alle docenten en onderzoekers die betrokken zijn bij de bachelor Cybercrime & Cybersecurity. Dank ook aan de collega-lectoren binnen het Centre of Expertise Cybersecurity – Marcel, Gerard en Peter – en de collega's van de faculteiten ITD en BRV waar we nauw mee samenwerken. Iedere dag ben ik blij dat we vanuit verschillende disciplines samen kunnen werken aan dit interessante onderwerp.

Het voert te ver om iedereen te noemen waar ik met veel plezier mee samenwerk, maar in ieder geval wil ik hier enkele NSCR-collega's noemen: Steve, Sjoukje, Elanie, Arjan, Hannah, Teun, Stijn. En uiteraard ben ik iedereen binnen 'mijn' eigen HHS-team zeer dankbaar dat ik met ze mag werken: Susanne, Asier, Marco, Luuk, Joeri, Sifra, Merel, Isabelle, Milou, Michelle, Jildau, Tijmen. Dank ook de mensen die het onderzoek mogelijk maken, zoals Maaike, Assia, Guus en vele anderen. Dan nog al die onderzoekers van andere instellingen en praktijkmensen met wie ik samenwerk. Echt fantastisch dat dit zo kan! Remco, Jurjen, Robby, Luca, Marleen, Floor, Wouter, Lonneke, Peter, Sten, Karijn.

En *last but not least* natuurlijk het thuisfront. Wat is het toch fijn om een warme, hechte, stabiele thuissituatie te hebben. Waarvan je weet dat het goed zit. Dank lieve Lian dat we al meer dan twintig jaar bij elkaar zijn. En dank lieve kids – Lynn,

Vere en Joa – dat jullie mijn leven zo verrijken. Datzelfde geldt natuurlijk voor mijn lieve moeder en broer – en mijn vader die dit helaas niet meer mee kan maken. Ook dank aan mijn schoonfamilie: bij jullie heb ik me vanaf het eerste moment thuis gevoeld. Dan ook een beetje mijn thuisfront: al mijn (hardloop)vrienden. Dank voor al die mooie gesprekken tijdens die vele lange trainingen, mooie trails, marathons, ultramarathons en het verdiende biertje erna. In de regen, brandende zon of gewoon onder uitstekende condities. Ik zou het iedereen gunnen.

Ik heb gezegd.

Referenties

Beerthuizen, M.G.C.J., T. Sipma & A.M. van der Laan (2020) *Aard en omvang van dader- en slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland*. Den Haag: WODC.

Bekkers, L. & E.R. Leukfeldt (2022) Recruiting money mules on Instagram: A qualitative examination of online involvement mechanisms into cybercrime. *Deviant Behaviour*, *44*(2), 1-17. DOI:10.1080/01639625.2022.2073298

Bekkers, L., A. Moneva & E.R. Leukfeldt (2022) Understanding cybercrime involvement: a quasi-experiment on engagement with money mule recruitment ads on Instagram. *Journal of Experimental Criminology*, *20*(2), 1-20. DOI:10.1007/s11292-022-09537-7

Bekkers, L.J.M., S. van 't Hoff-de Goede, E. Misana-ter Huurne, Y. van Houten, R. Spithoven & E.R. Leukfeldt (2023) Protecting Your Business against Ransomware Attacks? Explaining the Motivations of Entrepreneurs to Take Future Protective Measures against Cybercrimes Using an Extended Protection Motivation Theory Model. *Computers & Security*, *27*(april 2023). DOI:10.1016/j.cose.2023.103099

Blokland, A.A.J. & P. Nieuwbeerta (2010) *International Handbook of Life course criminology.* London: Routledge.

Bluhm, K., M. Andriessen, M. van de Wal, M. Berkenpas, D. de Boer, E.R. Leukfeldt, R. Spithoven & J. Jansen (2024) *Een eerste blik op het verloop en de werking van cyberweerbaarheidsprojecten in Nederland: Procesevaluaties van CCV City Deal projecten*.

Boekhoorn, P. (2019) *De aanpak van cybercrime door regionale eenheden van de politie - van intake van cybercrime naar opsporing en vervolging* (Politiekunde 102). Politie & Wetenschap.

Boes, S. & E.R. Leukfeldt (2017) Fighting Cybercrime: a Joint Effort. In: Hakim, S. & Clark, R.M. (ed.) Cyber-physical security at the state, provincial and local level: protecting critical infrastructure. New York: Springer Science.

Broadhurst, R., P. Grabosky, M. Alazab & S. Chon (2014) Organization and cyber crime: an analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology*, *8*(1), 1-20.

Bunt, H.G. van de & E.R. Kleemans (2007) *Georganiseerde criminaliteit in Nederland*. Den Haag: WODC.

Button, M., L. Sugiura, D. Blackbourn, R. Kapend, D. Shepherd & V. Wang (2020) *Victims of computer misuse main findings.* University of Portsmouth.

CBS (2023) *ICT, kennis en economie 2023*. Den Haag/Heerlen/Bonaire: CBS.

Clarke, R. V. (1980). "Situational" crime prevention: Theory and practice. British Journal of Criminology, 20(2),136–147. https://doi.org/10.1093/oxfordjournals.bjc.a047153

Clarke, R.V. & J.E. Eck (2003) *Become a Problem-Solving Crime Analyst: In 55 Small Steps*. London: Jill Dando Institute of Crime Science.. doi.org/10.4324/9781315060965

Collier, B., D.R. Thomas, R. Clayton & A. Hutchings (2019) Booting the Booters: Evaluating the Effects of Police Interventions in the Market for Denial-of-Service Attacks (Internet Measurement Conference). Amsterdam Netherlands: ACM. DOI:10.1145/3355369.3355592

Cornish, D.B. & R.V. Clarke (2003) Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies*, (16), 41-96.

Cross, C., K. Richards & R.G. Smith (2016) The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice*, (518), 1-14.

Domenie, M.M.L., E.R. Leukfeldt, J.A. van Wilsem, J. Jansen & W. Stol (2012) *Slachtofferschap van delicten met een digitale component onder burgers. Hacken, malware, persoonlijke en financiële delicten in kaart gebracht.* NHL Hogeschool.

Farrington, D.P. (2003) Developmental and life-course criminology: key theoretical and empirical issues-the 2002 Sutherland award address. *Criminology*, *41*(2), 221-225.

Grabosky, P. (2007) The Internet, Technology, and Organized Crime. *Asian Criminology*, *2*(2), 145-161.

Graham, A., T.C. Kulig & F.T. Cullen (2020) Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice. *Policing, 43*(1), 1-16.

Hadlington, L., K. Lumsden, A. Black & F. Ferra (2018) A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. *Policing: A Journal of Policy and Practice*, *15*(1), 34-43.

Harkin, D., C. Whelan & L. Chang (2018) The challenges facing specialist police cyber-crime units: An empirical analysis. *Police Practice and Research*, *19*(6), 519-536.

Hendriks, J. & G.J. Stams (2024) Landelijke kwaliteitskader. Effectieve jeugdinterventies voor preventie van jeugdcriminaliteit. Den Haag: Ministerie van Justitie en Veiligheid.

Hoff-de Goede, M.S. van 't, S. van de Weijer & E.R. Leukfeldt (2023) Explaining cybercrime victimization using a longitudinal population-based survey experiment. Are personal characteristics, online routine activities, and actual self-protective online behavior related to future cybercrime victimization? *Journal of Crime and Justice*, 472-491. DOI:10.1080/0735648X.2023.2222719Hutchings, A. (2014) Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change*, *62*(1), 1-20.

Kleemans, E.R., E.A.I.M. van den Berg & H.G. van de Bunt (1998) *Georganiseerde criminaliteit in Nederland. Rapportage op basis van de WODC-monitor*. Den Haag: WODC.

Kleemans, E.R., M.E.I. Brienen & H.G. van de Bunt (2002) *Georganiseerde criminaliteit in Nederland. Tweede rapportage op basis van de WODC-monitor*. Den Haag: WODC.

Kleemans, E.R. & H.G. van de Bunt (1999) The social embeddedness of organized crime. *Transnational Organized Crime, 5(1), 19-36.*

Kleemans, E.R. & C.J. de Poot (2008) Criminal careers in organized crime and social opportunity structure. *European Journal of Criminology*, *5*(1), 69-98.

Kleij, van der R., S. van 't Hoff-De Goede, S. van de Weijer & E.R. Leukfeldt (2023) Social engineering and the disclosure of personal identifiable information: Examining the relationship and moderating factors using a population-based survey experiment. *Journal of Criminology*, *56*(2-3), 278-293. DOI:10.1177/26338076231162660

Kruisbergen, E.W. (2023) Voorkomen is beter van genezen…, toch? Over goede bedoelde maar potentieel schadelijke vormen van preventie van ondermijning. *Tijdschrift voor Veiligheid*, *22*(3), 3-24.

Kruisbergen, E.W., H.G. van de Bunt & E.R. Kleemans (2012) *Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit*. Den Haag: WODC.

Kruisbergen, E.W., E.R. Leukfeldt, E.R. Kleemans & R. Roks (2018) *Georganiseerde criminaliteit en ICT: Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit*. Den Haag/Amsterdam: WODC/NSCR.

Kruisbergen, E.W., R.A. Roks & E.R. Kleemans (2019) *Georganiseerde criminaliteit in Nederland: daders, verwevenheid en opsporing*. Den Haag: WODC.

Leukfeldt, E.R. (2014) Cybercrime and social ties: Phishing in Amsterdam. *Trends in Organized Crime*, *17*(4), 231-249.

Leukfeldt, E.R. (ed.) (2017) *Research agenda the human factor in cybercrime and cybersecurity*. Den Haag: Eleven International Publishing.

Leukfeldt, E.R., S. van 't Hoff-de Goede & R. Roks (2025, n.n.g.) Cybercriminelen. In: B. van den Berg, E. Muller, P. Oldengarm & D. Weggemans (eds.), *Handboek digitale veiligheid*.

Leukfeldt, E.R. & T.J. Holt (2020) Examining the Social Organization Practices of Cybercriminals in the Netherlands Online and Offline. *International Journal of Offender Therapy and Comparative Criminology*, *64*(5), 522-538.

Leukfeldt, E.R. & E.R. Kleemans (2021) Breaking the walls of silence: analyzing criminal investigations to better understand cybercrime. In: A. Lavorgna & T.J. Holt (eds.), *Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches* (pp. 127-144). Palgrave Macmillan Cham.

Leukfeldt, E.R., E.R. Kleemans & W.Ph. Stol (2017a) Origin, growth and criminal capabilities of cybercriminal net-

works: An international empirical analysis. *Crime, Law and Social Change*, *67*(1), 39-53.

Leukfeldt, E.R., E.R. Kleemans & W.P. Stol (2017b) The use of online crime markets by cybercriminal networks: A view from within. *American Behavioral Scientist*, *61*(11), 1387-1402.

Leukfeldt, E.R. & R.A. Roks (2020) Cybercrimes on the streets of the Netherlands? An exploration of the intersection of cybercrimes and street crimes. *Deviant Behavior*, *42*(1), 1-12. DOI:10.1080/01639625.2020.1755587

Leukfeldt, E.R., R. Spithoven & E. Misana-ter Huurne (2020) De lokale aanpak van cybercrime. Risicocommunicatie als antwoord op een grenzeloos vraagstuk. *Cahiers Politiestudies*, *2020*(3) 203-223.

Leukfeldt, E.R., S. Veenstra, M. Domenie & W.P. Stol (2013a) *De strafrechtketen in een gedigitaliseerde samenleving. Een onderzoek naar de strafrechtelijke afhandeling van cybercrime.* De Bilt/Leeuwarden: PAC/NHL.

Leukfeldt, E.R., S. Veenstra & W.P. Stol (2013b) High Volume Cyber Crime and the Organization of the Police. The results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology*, *7*(1) 1-17.

Loggen, J. & E.R. Leukfeldt (2022) Unraveling the crime scripts of phishing networks: an analysis of 45 court cases in the Netherlands. *Trends in Organized Crime*, *25*(6). DOI:10.1007/s12117-022-09448-z

Loggen, J., A. Moneva & E.R. Leukfeldt (2023) A systematic narrative review of pathways into, desistance from, and risk factors of financial-economic cyber-enabled crime. *Computer, Law and Security Review*, *52*(april 2024). DOI:10.1016/j.clsr.2023.105858

Loggen, J., A. Moneva & E.R. Leukfeldt (2024) Pathways into, desistance from, and risk factors related to cyber-dependent crime: A systematic narrative review. *Victims and offenders*, 1-32. DOI:10.1080/15564886.2024.2370295

Lusthaus, J. (2016) *Cybercrime: the industry of anonymity*. Oxford: University of Oxford.

Lusthaus, J., E. Kleeman, E.R. Leukfeldt, M. Levi & T.J. Holt (2023) Cybercriminal networks in the UK and Beyond: Network structure, criminal cooperation and external interactions. *Trends in Organized Crime*, *27*(3), 364-387. DOI:10.1007/s12117-022-09476-9

Matthijsse, S.R., M.S. van 't Hoff-de Goede & E.R. Leukfeldt (2023) Your files have been encrypted: a crime script analysis of ransomware attacks. *Trends in Organized Crime*. DOI:10.1007/s12117-023-09496-z

McGuire, M. & S. Dowling (2013a) *Chapter 1: Cyber-dependent crimes*. London: Home Office UK.

McGuire, M. & S. Dowling (2013b) *Chapter 2: Cyber-enabled crimes*. London: Home Office UK.

Moneva, A. & E.R. Leukfeldt (2023) The effect of online ad campaigns on DDoS-attacks: A cross-national difference-in-differences quasi-experiment. *Criminology & Public Policy*, *22*(4), 869-894. DOI:10.1111/1745-9133.12649

Moneva, A., Leukfeldt, E. R., & Van der Stoel, M. (2024). Countering cybercrime tutorials with online video ad campaigns: A quasi-experiment on YouTube. *24th Annual Conference of the European Society of Criminology*. Bucharest, Romania. https://www.eurocrim2024.com/

Moneva, A., E.R. Leukfeldt & W. Klijnsoon (2023) Alerting Consciences to Reduce Cybercrime: A Quasi-experimental Design Using Warning Banners. *Journal of Experimental Criminology*, *19*, 835-862. DOI:10.1007/s11292-022-09504-2

Reiss, A.J. (1988) Co-offending and criminal careers. In: M. Tonry & N. Morris (eds.), *Crime and Justice. A Review of Research*. Chicago: Chicago University Press.

Reiss, A.J. & D.P. Farrington (1991) Advancing knowledge about co-offending: results from a prospective longitudinal survey of London males. *Journal of criminal law and criminology*, *82*(2), 360-395.

Rogers, E.M. (2003) *Diffusion of Innovations* (5th ed.). New York: Free Press.

Roks, R.A., E.R. Leukfeldt & J.A. Densley (2020)The Hybridization of Street Offending in the Netherlands. *British Journal of Criminology*. DOI:10.1093/bjc/azaa091

Romagna, M. & E.R. Leukfeldt (2024a) Hacktivism: from Loners to Formal Organizations? Assessing the Social Organization of Hacktivist Networks. *Deviant Behavior*.

Romagna, M. & E.R. Leukfeldt (2024b) Social Opportunity Structures in Hacktivism: Exploring Online and Offline Social Ties and the Role of Of-fender Convergence Settings in Hacktivist Networks. *Victims and offenders*. DOI:10.1080/15564886.2024.2372054

Ruiter, S., M. van Leuken, T. van Ruitenburg, J. Schiks & E.R. Leukfeldt (2023) *In- en doorstroom van online criminaliteit in de strafrechtketen*. Den Haag: WODC.

Schiks, J.A.M., M. van 't Hoff-de Goede & E.R. Leukfeldt (2021) *Een alternatief voor jeugdige hackers? Plan- en procesevaluatie van Hack_Right*. Den Haag: Sdu uitgevers.

Schiks, J.A.M., M. van 't Hoff-de Goede & E.R. Leukfeldt (2022) *Op zoek naar de parels bij de lokale aanpak van cybercriminaliteit en gedigitaliseerde criminaliteit. Een verkennend onderzoek* (P&W verkenningen 89). Politie & Wetenschap.

Schiks, J.A.M., S. van 't Hoff-de Goede & E.R. Leukfeldt (2023) An alternative intervention for juvenile hackers? A qualitative evaluation of the Hack_Right intervention. *Journal of Crime and Justice*, 492-510. DOI:10.1080/0735648X.2023.2252394

Shaw, C.R. & H.D. McKay (1931) *Report on the Causes of Crime: Volume II*. Washington: Government Printing Office.

Sutherland, E.H. (1937) *The Professional Thief*. Chicago: The University of Chicago Press.

Thomas, D.R., R. Clayton & A.R. Beresford (2017) *2017 APWG symposium on electronic crime research (eCrime)*, 79-84. DOI:10.1109/ECRIME.2017.7945057

Tollenaar, N., J. Beijers & A.M. van der Laan (2024) *Monitor zelfgerapporteerde jeugddelinquentie 2023*. Den Haag: WODC.

Prof.dr. E.R. Leukfeldt

Rutger Leukfeldt bekleedt sinds 2023 de bijzondere leerstoel Governing Cybercrime die is gevestigd en wordt gefinancierd door het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR). Daarnaast is Rutger directeur van het Centre of Expertise Cybersecurity van de Haagse Hogeschool. Het onderwijs en onderzoek van Rutger richt zich op de human factor in cybercrime. Wie zijn daders, wat zijn hun werkwijzen? Wat zijn risicoprofielen van slachtoffers? En hoe kunnen we de aanpak van cybercrime het beste inrichten? Rutger heeft meer dan 130 cybercrime publicaties op zijn naam staan (waaronder meer dan 70 peer reviewed publicaties, 6 boeken en tal van vakpublicaties en rapporten). Hij is voorzitter van de Cybercrime Working Group van de European Society of Criminology (ESC) en een van de oprichters van de jaarlijkse Human Factors in Cybercrime Conference.

Universiteit Leiden