In- en doorstroom van online criminaliteit in de strafrechtketen

Stijn Ruiter
Merel van Leuken
Teun van Ruitenburg
Jim Schiks
Rutger Leukfeldt

Amsterdam, 2023

Nederlands Studiecentrum
Criminaliteit en Rechtshandhaving

In- en doorstroom van online criminaliteit in de strafrechtketen

Stijn Ruiter

Merel van Leuken

Teun van Ruitenburg

Jim Schiks

Rutger Leukfeldt

Amsterdam, 2023

Dit onderzoek is uitgevoerd in opdracht van het WODC

nscr Nederlands Studiecentrum Criminaliteit en Rechtshandhaving

Dankwoord

De weg naar deze eindrapportage was er een met vele hobbels en uitdagingen. Gezien het eindresultaat zijn we blij dat we hebben doorgezet. Een studie als deze is alleen mogelijk dankzij de inzet van veel verschillende mensen. De voorzitter en leden van de begeleidingscommissie (zie Bijlage 12) hebben een belangrijke rol gespeeld bij de totstandkoming van dit rapport. Wij danken hen voor de prettige samenwerking en hun kritische feedback op conceptversies. We willen Rik Geven van Bureau Management Informatie van de politie en Jeroen de Ridder, voormalig medewerker van de Fact Factory van het Openbaar Ministerie, bedanken voor het meedenken en ontsluiten van de gegevens van de politie en het Openbaar Ministerie. Ook danken we Nikolaj Tollenaar voor het delen van analysecode en tooling, waarmee wij konden voortbouwen op een eerdere WODC-studie. Mara van Dalen danken we voor haar bijdrage aan het annoteren van de BVH-registraties. Ten slotte bedanken we alle medewerkers van de politie, het Openbaar Ministerie, de zittende magistratuur en de experts uit binnen- en buitenland, die door het beantwoorden van onze vele vragen een belangrijke bijdrage hebben geleverd aan deze studie.

Stijn Ruiter, Merel van Leuken, Teun van Ruitenburg, Jim Schiks en Rutger Leukfeldt

Inhoudsopgave

Samenvatting

Onze huidige samenleving is in sterke mate gedigitaliseerd. Met de digitalisering van de maatschappij is ook criminaliteit gedigitaliseerd en daarmee is het werkaanbod van politie en justitie veranderd. De strafrechtketen krijgt meer en meer te maken met delicten met een digitale component, ook wel online criminaliteit genoemd. Enerzijds is er sprake van nieuwe delicten, bijvoorbeeld het hacken van een database met persoonsgegevens of het platleggen van websites of netwerken. Dit soort delicten valt onder de noemer cybercrime. Anderzijds zijn er traditionele vormen van criminaliteit waarbij ICT een steeds belangrijkere rol speelt bij de realisatie daarvan. Voorbeelden zijn het plegen van fraude via internet en stalking. Dergelijke delicten vallen onder de noemer gedigitaliseerde criminaliteit.

Uit slachtofferenquêtes blijkt dat tegenwoordig meer burgers slachtoffer worden van hacken, online oplichting en online fraude dan van fietsendiefstal. Burgers en bedrijven worden daarnaast van nog veel meer vormen van online criminaliteit slachtoffer: van malware of ransomware tot phishing, cyberstalking en cyberbedreiging. Hoewel het inmiddels duidelijk is dat online criminaliteit een groeiend probleem is en dat er veel slachtoffers worden gemaakt, lijkt de in- en doorstroom van online criminaliteit in de strafrechtketen achter te blijven bij de ontwikkeling van het slachtofferschap van online criminaliteit zoals gerapporteerd in de Veiligheidsmonitor van het Centraal Bureau voor de Statistiek. Terwijl er blijkbaar veel slachtoffers worden gemaakt, is het aantal veroordelingen van daders van online criminaliteit gering.

Eerder onderzoek laat zien dat er in ieder geval drie oorzaken ten grondslag liggen 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. Naast deze oorzaken voor daadwerkelijk minder in- en doorstroom van online criminaliteit in de strafrechtketen, doet zich ook het probleem voor dat veel vormen van online criminaliteit - met name vormen van gedigitaliseerde criminaliteit - niet als zodanig herkenbaar zijn in de registraties van politie en justitie. Daarmee is mogelijk niet alleen de feitelijke in- en doorstroom gering, maar is er daarnaast ook beperkt zicht op de in- en doorstroom die er wel degelijk is.

Onderhavig onderzoek is erop gericht meer zicht te bieden op de in- en doorstroom van online criminaliteit in de strafrechtketen. Naast inzicht in de actuele in- en doorstroom biedt het onderzoek ook inzicht in mogelijke knelpunten binnen de strafrechtketen, *good practices* en verbetermogelijkheden.

Het onderzoek beantwoordt de volgende onderzoeksvragen:

1. Zijn er volgens de literatuur vormen van online criminaliteit waarvan verdachten niet of nauwelijks de strafrechtketen instromen? Zo ja, welke? Welke verklaringen worden er in de literatuur gegeven voor die lage instroom?
2. Wat zijn de meest recente cijfers over 2018-2020 met betrekking tot de instroom en doorstroom van online criminaliteit in de strafrechtketen?
3. Welke knelpunten kunnen geïdentificeerd worden binnen de in- en doorstroom van online criminaliteit in de strafrechtketen?
4. In hoeverre hebben andere landen ook te maken met de onder vraag 3 geconstateerde knelpunten? Welke ervaringen zijn er in andere landen met het oplossen van deze knelpunten?
5. Welke verbeteringen kunnen per schakel van de strafrechtketen worden doorgevoerd om de strafrechtpleging bij online criminaliteit te bevorderen?

Onderzoeksmethoden

Om de onderzoeksvragen te beantwoorden hebben we gebruik gemaakt van verschillende onderzoeksmethoden.

We deden een internationaal literatuuronderzoek om inzicht te krijgen in welke vormen van online criminaliteit niet of nauwelijks instromen in de strafrechtketen, welke verklaringen daarvoor zijn, welke knelpunten binnen de strafrechtketen kunnen zorgen voor beperkte doorstroom van zaken en wat mogelijke verbeterpunten zijn binnen de diverse schakels van de strafrechtketen om de doorstroom van zaken juist te bevorderen.

Voor de kwantitatieve analyse van de in- en doorstroom van online criminaliteit in de strafrechtketen namen we BVH-registraties van de politie als startpunt. Omdat veel vormen van online criminaliteit niet als zodanig herkenbaar worden geregistreerd in de systemen, ontwikkelden we *predictive textmining* modellen. Dergelijke modellen kunnen op basis van relevante tekstkenmerken documenten met grote hoeveelheden tekst automatisch classificeren. We maakten daarbij gebruik van *supervised machine learning*. Bij deze techniek wordt een model getraind aan de hand van voorbeelddocumenten waarvan vooraf handmatig is vastgesteld welk label zij dienen te hebben. Na de training wordt verondersteld dat het model nieuwe documenten zelf van het juiste label kan voorzien. We ontwikkelden de modellen op basis van een selectieve steekproef (n=7.500) waarin relatief veel registraties van online criminaliteit voorkwamen en pasten de modellen vervolgens toe op een grote willekeurige steekproef (n=300.000) van unieke BVH-registraties uit de jaren 2018-2020. Voor het vaststellen van de doorstroom in de strafrechtketen koppelden we de BVH-gegevens aan gegevens ontleend aan het systeem Betere Opsporing door Sturing op Zaken (BOSZ). Voor het

vaststellen van de doorstroom richting OM en rechtspraak hebben we vervolgens de gegevens over de naar het OM ingezonden verdachten gekoppeld aan gegevens ontleend aan het Geïntegreerd Processysteem Strafrecht (GPS). Om na te gaan in hoeverre de in- en doorstroom van online criminaliteit afwijkend is, herhaalden we dezelfde analyses voor drie andere vormen van criminaliteit (vermogenscriminaliteit, misdrijven tegen de lichamelijke integriteit en fraudedelicten).

Naast het literatuuronderzoek en de grootschalige kwantitatieve analyse van gegevens van politie en justitie zijn voor dit onderzoek allerlei gesprekken gevoerd. Het doel van de interviews met actoren binnen de verschillende schakels van de strafrechtketen was om zicht te krijgen op algemene knelpunten in de in- en doorstroom van online criminaliteit in de strafrechtketen. In totaal interviewden we 34 actoren binnen de strafrechtketen, waarvan 26 werkzaam waren bij de politie, 6 bij het OM en 2 bij de zittende magistratuur. Er is gesproken met medewerkers uit verschillende teams, waaronder basisteams (BT), de districtsrecherche (DR) en de Dienst Regionale Recherche (DRR) binnen de volgende 5 eenheden van de politie: Den Haag, Noord-Holland, Noord-Nederland, Midden-Nederland en Zeeland-West-Brabant. Binnen het OM zijn officieren van justitie die online criminaliteit in hun portefeuille hebben geïnterviewd. Hier zijn de parketten geselecteerd die samenwerken met de geselecteerde eenheden van de politie. Bij de zittende magistratuur zijn twee rechters bevraagd die zaken met een online component hebben behandeld.

Om zicht te krijgen op eventuele *good practices* in andere landen die ook in Nederland toepasbaar zouden kunnen zijn, interviewden we 5 internationale experts (uit het Verenigd Koninkrijk, de Verenigde Staten en Australië). Doel van deze interviews was om zicht te krijgen op de mate waarin andere landen ook te maken hebben met de knelpunten die we in de interviews met actoren binnen de strafrechtketen vernamen en welke ervaringen er in die landen zijn met het oplossen van deze knelpunten. De resultaten van de literatuurstudie, kwantitatieve analyses en interviews zijn ten slotte bediscussieerd met experts van binnen en buiten politie en justitie. De discussiebijeenkomsten zijn tevens gebruikt om te inventariseren welke mogelijke oplossingen er zijn om de geïdentificeerde knelpunten te verbeteren. In totaal deden 5 experts aan de discussiesessies mee.

Wel slachtofferschap, geen instroom

Eerder onderzoek laat zien dat de aangiftebereidheid onder slachtoffers van online criminaliteit over het algemeen lager is dan bij slachtoffers van traditionele delicten. Uit Nederlandse studies blijkt dat ongeveer 13% van de slachtoffers van online criminaliteit melding doet bij de politie. De bereidheid van slachtoffers om aangifte te doen bij de politie verschilt voor verschillende vormen van online criminaliteit. Bij delicten waar IT niet alleen het middel maar ook het doelwit is (cybercrimes) lijkt de aangiftebereidheid lager te liggen

dan bij delicten waarbij IT alleen als hulpmiddel wordt gebruikt (gedigitaliseerde criminaliteit). Uit eerdere studies blijkt dat het type online criminaliteit een belangrijke voorspeller is voor de aangiftebereidheid van online criminaliteit. Verder is de (waargenomen) ernst van een delict een belangrijke voorspeller: hoe ernstiger het delict, hoe eerder aangifte wordt gedaan.

Er worden in de literatuur verschillende verklaringen genoemd waarom slachtoffers van online criminaliteit geen aangifte doen. Zo weten individuen en bedrijven niet altijd dat ze slachtoffer zijn of zien slachtoffers online incidenten zoals malware-infecties niet als criminaliteit. In de gevallen waarbij slachtoffers wel op de hoogte zijn van hun slachtofferschap, kunnen verschillende factoren ertoe leiden dat ze toch geen aangifte doen. Een veelgenoemde verklaring is dat individuen de ernst en impact van online delicten als laag ervaren en daardoor minder snel geneigd zijn om aangifte te doen. In andere gevallen is er geen of weinig (financiële) schade of is de schade al vergoed door bijvoorbeeld verzekeringsmaatschappijen of financiële instellingen. Verder kan schaamte een rol spelen bij het niet melden van slachtofferschap. Ten slotte kan spelen dat slachtoffers een gebrek aan vertrouwen hebben in de politie om daders van online criminaliteit op te sporen en aan te houden.

In- en doorstroom in cijfers

De in- en doorstroom van online criminaliteit in de strafrechtketen is voor de jaren 2018-2020 geanalyseerd. Daartoe zijn BVH-registraties van de politie uit die periode als startpunt genomen. In het BVH-systeem registreert de politie incidenten, meldingen en aangiften en de aan de incidenten gekoppelde acties zoals processen-verbaal van verhoor van getuigen of verdachten. Omdat de verschillende vormen van online criminaliteit niet systematisch in de BVH-registraties kunnen worden geïdentificeerd aan de hand van bijvoorbeeld unieke maatschappelijke klassen, zijn *predictive textmining* modellen ontwikkeld die gebruikmaken van alle bij een BVH-registratie behorende registraties van *bevindingen*, *toelichtingen*, *verklaringen* en *MO-teksten.* Er zijn afzonderlijke modellen ontwikkeld om negen verschillende typen online criminaliteit te onderscheiden: vier vormen van cybercrime (hacking, malware, ransomware en DDoS-aanval) en vijf vormen van gedigitaliseerde criminaliteit (online bedreiging, online stalking, online smaad/laster/belediging, online oplichting en *money muling*), waarbij we online oplichting nog uitsplitsten naar phishing, online identiteitsfraude, online aan- en verkoopfraude, VIN-fraude, helpdeskfraude en overige online oplichting. De *predictive textmining* modellen hadden niet voor alle vormen van online criminaliteit een voldoende goede *performance* om ermee de afzonderlijke vormen van online criminaliteit in BVH-registraties te kunnen identificeren. Voor de overkoepelende labels cybercrime en gedigitaliseerde criminaliteit als ook voor de afzonderlijke labels hacking, online oplichting, phishing, online identiteitsfraude,

online aan- en verkoopfraude, VIN-fraude en helpdeskfraude was de *performance* goed en voor die vormen konden daarmee beschrijvende analyses van de in- en doorstroom in de strafrechtketen worden gepresenteerd.

Door de modellen met een goede *performance* toe te passen op een grote steekproef (n=300.000) van BVH-registraties kon de in- en doorstroom van online criminaliteit in de periode 2018-2020 worden bestudeerd. BVH-registraties met een aangifte vormen een duidelijk startpunt van de strafrechtketen en BVH-registraties die geclassificeerd zijn als online criminaliteit en waarbij tenminste 1 aangifte is geregistreerd markeren dan ook wat we in kwantitatieve analyse de *instroom* van online criminaliteit in de strafrechtketen hebben genoemd.

De belangrijkste bevinding uit de kwantitatieve analyse van in- en doorstroom van online criminaliteit in de strafrechtketen is gelegen in de lage aantallen. We startten de analyse met een relatief grote steekproef van BVH-registraties (n=300.000) om vervolgens vast te stellen dat de meeste vormen van online criminaliteit in minder dan 1% (met maximum van 4% voor alle gedigitaliseerde criminaliteit tezamen) van de registraties voorkwam. Van de hoge prevalentie die wordt vastgesteld in slachtofferenquêtes zien we in BVH-registraties dus weinig terug. Vervolgens bleek in ongeveer 25% van de registraties geen sprake te zijn van een aangifte en van alle registraties met een aangifte werd maar in ongeveer 10% van de gevallen ook een verdachte gekoppeld. De belangrijkste conclusie moet dan ook luiden: we vinden zelfs met de toepassing van geavanceerde *predictive textmining* modellen maar weinig registraties van online criminaliteit in de strafrechtketen. De instroom in de vorm van aangiften is al niet groot, maar omdat er maar in ongeveer 10% van de gevallen een verdachte wordt gekoppeld, is de doorstroom nog veel geringer.

Verder laten de resultaten van de grootschalige kwantitatieve analyses zien dat BVH-registraties die als gedigitaliseerde criminaliteit zijn geclassificeerd aanzienlijk meer voorkomen dan registraties van cybercrime. De 25% van de BVH-registraties die geclassificeerd zijn als cybercrime of gedigitaliseerde criminaliteit waarbij geen sprake was van een aangifte wijst erop dat er in het BVH-systeem ook best vaak mutaties over online criminaliteit worden gemaakt zonder dat er sprake is van een aangifte. Wanneer we deze cijfers echter vergelijken met die voor andere vormen van criminaliteit, dan valt op dat dit niet uniek is voor online criminaliteit. Bij misdrijven tegen de lichamelijke integriteit (32%) en fraudedelicten (51%) liggen de percentages zelfs nog aanzienlijk hoger, terwijl het percentage bij vermogensdelicten (11%) juist lager is. Het maken van een BVH-mutatie zonder een aangifte op te nemen is dus niet uniek voor online criminaliteit.

Het lage percentage BVH-registraties van online criminaliteit met een aangifte waarbij ook tenminste 1 verdachte staat geregistreerd (8% voor cybercrime en 10% voor gedigitaliseerde criminaliteit) blijkt flink te variëren tussen afzonderlijke vormen van online criminaliteit, van slechts 2% bij online aan- en

verkoopfraude tot 18% bij helpdeskfraude. Daarbij blijkt bovendien dat bij de vormen van online criminaliteit die relatief veel voorkomen juist relatief weinig verdachten worden geregistreerd.

88% van de verdachten van cybercrime en 85% van de verdachten van gedigitaliseerde criminaliteit was meerderjarig, al valt op dat het aandeel minderjarige verdachten wat hoger is bij helpdeskfraude (21%) en juist wat lager bij VIN-fraude (8%), online identiteitsfraude (8%) en online oplichting (9%).

Voor een aanzienlijk deel van de meerderjarige verdachten van online criminaliteit zien we een overige of onbekende afdoening geregistreerd staan bij politie of OM (samen goed voor 43%), terwijl dit bij minderjarige verdachten ook maar in mindere mate voorkomt (33%). Het aandeel van de verdachten van online criminaliteit die helemaal doorstromen naar de rechtbank verschilt weinig tussen meerderjarige en minderjarige verdachten, en ligt rond eenderde. Minderjarige verdachten krijgen vaker een afdoening bij de politie (6%) dan meerderjarigen verdachten (1%).

Om de in- en doorstroom van online criminaliteit in perspectief te plaatsen, zijn dezelfde analyses gedaan voor drie andere vormen van criminaliteit, te weten *vermogenscriminaliteit*, *misdrijven gericht tegen de lichamelijke integriteit*, en *fraudedelicten*. We zien aanzienlijk meer BVH-registraties van vermogenscriminaliteit dan van online criminaliteit. De aantallen voor misdrijven gericht tegen de lichamelijke integriteit liggen juist net iets lager en voor fraudedelicten zien we nog veel minder registraties. Het percentage BVH-registraties waarbij ook tenminste 1 aangifte was geregistreerd lag hoger bij vermogenscriminaliteit dan bij online criminaliteit, maar bij de andere vormen van criminaliteit lag het juist lager. Bij vermogenscriminaliteit zien we ongeveer even vaak een verdachte geregistreerd staan (in 12% van de gevallen) als bij online criminaliteit (10%). Bij fraudedelicten ligt het percentage BVH-registraties met aangifte waarbij tenminste 1 verdachte is geregistreerd aanzienlijk hoger (31%), terwijl dit bij misdrijven gericht tegen de lichamelijke integriteit nog veel hoger (59%) ligt. De ophelderingspercentages liggen bij deze laatste twee vormen van criminaliteit dus aanzienlijk hoger dan bij online criminaliteit en vermogenscriminaliteit. Voor misdrijven tegen de lichamelijke integriteit is dit niet zo verwonderlijk, aangezien dader en slachtoffer vrijwel altijd direct met elkaar in contact zullen zijn geweest en er dan ook vaak sprake is van daderindicatie, terwijl bij online criminaliteit en vermogenscriminaliteit de verdachte vaak niet direct in beeld zal zijn. Dit verklaart echter niet het verschil in ophelderingspercentages bij online en offline fraudedelicten.

Zodra er een verdachte in beeld is, zien we ook bij vermogenscriminaliteit en misdrijven tegen de lichamelijke integriteit dat minderjarige verdachten vaker een afdoening bij de politie krijgen dan meerderjarige verdachten. Verder valt op dat een hoog percentage meerderjarige verdachten van vermogenscriminaliteit

helemaal doorstroomt tot de rechtbank (55%). Ook bij misdrijven tegen de lichamelijke integriteit (46%) en fraudedelicten (43%) ligt dit percentage aanzienlijk hoger dan bij online criminaliteit (32%).

Knelpunten volgens de literatuur en volgens actoren binnen de strafrechtketen

Intake

Uit de literatuur blijkt dat de politie niet altijd een aangifte opneemt wanneer slachtoffers van online criminaliteit contact opnemen met de politie. Dat kan komen doordat intakemedewerkers denken dat het niet om een strafbaar feit gaat (bijvoorbeeld in hacking zaken), dat het om een civiele zaak gaat (bijvoorbeeld bij online fraude) of meer algemeen dat intakemedewerkers de ernst van het slachtofferschap als laag inschatten. Indien er wel een aangifte wordt opgenomen, dan lijkt het succesvol opnemen van een aangifte afhankelijk te zijn van het begrip en de kennis van de intakemedewerker die de aangifte van online criminaliteit opneemt. Deze kennis is echter niet altijd (voldoende) aanwezig bij intakemedewerkers.

Respondenten geven aan dat ze een gebrek aan kennis van online criminaliteit zien onder intakemedewerkers, terwijl juist een kwalitatief hoogstaande aangifte voor een succesvolle doorstroom in de strafrechtketen zorgt. Een knelpunt is verder dat de aangifte ook afhankelijk is van (de kennis van) de aangever. Het ‘verhaal’ van de aangever is lang niet altijd helder. Burgers weten zelf ook niet altijd precies wat er is gebeurd. Des te belangrijker is het voor intakemedewerkers om de juiste vragen te stellen. Het geautomatiseerde aangifteproces via de website van de politie maakt het mogelijk om beter door te vragen.

Zowel de experts die deelnamen aan de discussiesessies als de internationale respondenten die geïnterviewd zijn herkennen het beeld dat naar voren kwam uit de literatuur en interviews. Tijdens de expertsessies werd meermaals gewezen op de belangrijke rol die intakemedewerkers spelen bij het leggen van een goede basis voor verder opsporingsonderzoek. Zonder de juiste informatie is de kans op vroegtijdig uitval volgens de experts groter.

Casescreening

Er is relatief weinig onderzoek dat zich richt op de casescreening van zaken online criminaliteit door de politie. Uit het onderzoek dat wel is gedaan ontstaat het beeld dat online criminaliteit zaken minder snel worden opgepakt dan traditionele zaken. Verklaringen hiervoor zijn dat de afhandeling van dergelijke zaken veel tijd kost, een gebrek aan capaciteit, het internationale karakter van online criminaliteit en de kwaliteit van de opgenomen aangiften.

Uit de interviews komen verschillende redenen naar voren waarom zaken van online criminaliteit binnen het screeningsproces uitvallen. De belangrijkste reden die door respondenten wordt genoemd is het gebrek aan

opsporingsindicatie en meer concreet het ontbreken van een verdachte. Hoewel dit geen uniek probleem is, speelt dit volgens respondenten in het bijzonder bij online criminaliteit, omdat daders zichzelf en de illegaal verkregen inkomsten makkelijker en effectiever kunnen afschermen. Daarbij blijkt het voor online criminaliteit lastiger dan voor traditionele criminaliteit in te schatten of een zaak voldoende opsporingsindicatie bevat. Voor het al dan niet oppakken van een zaak speelt ook de financiële schade een rol. Is sprake van een 'gering' schadebedrag dan wordt een zaak niet of minder snel opgepakt.

Opsporing

Ook wanneer wordt besloten om een zaak op te pakken, kunnen er verschillende redenen zijn waarom een zaak tijdens de opsporing alsnog uitstroomt. Uit de literatuur komen vier factoren naar voren die de opsporing van online criminaliteit bemoeilijken. Ten eerste wordt het gebrek aan prioriteit binnen politieorganisaties genoemd, wat onder meer versterkt wordt door de complexiteit van deze opsporingszaken en het beperkte bewustzijn van de risico's van online criminaliteit. Ten tweede bestaat er te weinig kennis en vaardigheden onder politiemedewerkers om opsporingsonderzoeken inzake online criminaliteit (effectief) op te pakken. Ten derde komt uit de literatuur naar voren dat ook bij de opsporing te weinig capaciteit aanwezig is om online criminaliteit op te pakken, waarbij politiemedewerkers met specialistische kennis moeilijker binnen de politieorganisatie te behouden zijn. Tot slot geldt dat de complexiteit van online criminaliteit de opsporing van daders verder bemoeilijkt. Dit komt bijvoorbeeld door het internationale karakter van online criminaliteit en de vluchtigheid van digitale gegevens.

De knelpunten die in de literatuur worden benoemd, zijn op soortgelijke wijze teruggekomen tijdens de interviews en worden ook benoemd in de discussiesessie: een gebrek aan prioriteit, een gebrek aan kennis, een gebrek aan capaciteit en de complexiteit van online criminaliteitszaken. Voor wat betreft het gebrek aan prioriteit werd door respondenten vooral gesproken over de gepercipieerde lagere (sociale) impact van online criminaliteit, hoewel dit door een deel van de respondenten als onterecht wordt beschouwd. Algemeen gesteld lijken de werkprocessen van de politieorganisatie nog voornamelijk te zijn ingericht op traditionele vormen van criminaliteit. Heterdaadsituaties, bijvoorbeeld bij winkeldiefstallen, krijgen voorrang op online criminaliteit zaken. Tegelijkertijd dient te worden opgemerkt dat de afgelopen jaren een duidelijke kentering zichtbaar is, waarbij verschillende teams speciaal zijn ingericht op het opsporen van online criminaliteit. Volgens respondenten wordt online criminaliteit door collega's nog vaak (onterecht) als iets ingewikkelds gezien. Ondanks toegenomen prioriteit voor het aanpakken van online criminaliteit, geeft het overgrote deel van de respondenten aan dat zowel de basisteams, de districtsrecherches als de cybercrimeteams, om verschillende redenen, kampen met een capaciteitsgebrek.

Tijdens de interviews wordt ook genoemd dat de opsporing van online criminaliteit complex is en dat deze complexiteit een knelpunt kan vormen voor de goede doorstroom hiervan. Alle factoren die online criminaliteit complex (kunnen) maken en in de literatuurstudie werden genoemd, werden ook tijdens de interviews genoemd. Veruit het meest genoemd was het internationale karakter van online criminaliteit en de perceptie dat het verkrijgen en behouden van digitaal bewijs lastig is door de vluchtigheid van gegevens in de online wereld. Daarnaast benoemen respondenten dat de politie als gevolg van wet- en regelgeving vaak over onvoldoende opsporingsmogelijkheden beschikt om digitaal bewijs veilig te kunnen stellen. In aanvulling op de literatuur wijzen respondenten ook nog op het potentieel grote aantal slachtoffers dat met online criminaliteit gepaard gaat en de mogelijkheid dat slachtoffers vaak niet binnen dezelfde eenheid woonachtig zijn.

Tot slot is aan bod gekomen dat het internationale karakter van online criminaliteit en het feit dat er vaak veel verschillende slachtoffers in meerdere eenheden zijn een gebrek aan eigenaarschap in de hand kan werken. Wanneer niet duidelijk is aan welk opsporingsteam een zaak toebehoort, kan dit er toe leiden dat een zaak niet wordt opgepakt.

De internationale respondenten schetsen eenzelfde beeld als de Nederlandse respondenten. Alhoewel het per land verschillend is, lijkt de situatie in het VK, de VS en Australië zelfs nog complexer door de veelheid van lokale politieregio's en de organisatie van de politie op federaal en statelijk niveau. Respondenten geven bijvoorbeeld aan dat het voor casescreeners lastig kan zijn om te bepalen waar een zaak 'gedraaid' moet worden omdat in veel gevallen lokale politiediensten zijn die een zaak kunnen oppakken, maar dat er ook landelijk opererende teams zijn die zich richten op georganiseerde misdaad en/of fraude en cybercrimes inmiddels ook in hun takenpakket hebben. Als een zaak dan naar een 'verkeerd' team gaat, dan is de kans volgens respondenten groot dat die nooit wordt opgepakt.

OM en ZM

Er bestaat weinig onderzoek dat ingaat op de knelpunten in de doorstroom van zaken binnen het OM of de ZM. In 2012 werd door Leukfeldt *et al.* nog geconcludeerd dat gespecialiseerde officieren van justitie op het gebied van online criminaliteit weinig of geen online criminaliteitszaken krijgen. Verder leken in dat onderzoek rechters geen knelpunten te ervaren in de afhandeling van online criminaliteitszaken, hoewel ze wel meer tijd kosten om goed te kunnen doorgronden. Andere knelpunten omtrent de vervolging van online criminaliteit zijn hetzelfde als voor de opsporing, en hebben te maken met wet- en regelgeving, bewijsvoering en de complexiteit van online criminaliteitszaken.

Opvallend is dat alle respondenten aangeven dat het merendeel van de knelpunten bij de politie ligt en in mindere mate bij OM en ZM. Over het algemeen stellen de respondenten dat er bij OM en ZM minder

problemen zijn op het gebied van capaciteit als het gaat om de afhandeling van online criminaliteit. Ook is het duidelijk dat online criminaliteit prioriteit heeft. Dat wil overigens niet zeggen dat er – met name bij het OM – buiten de politie geen knelpunten benoemd zijn. Zo geven respondenten bijvoorbeeld aan dat ook bij het OM – en in mindere mate ook ZM – er sprake is van digitale koudwatervrees. Een punt dat enkele malen tijdens de interviews aan bod kwam en ook door experts tijdens de discussiesessies werd benoemd is dat er wel knelpunten zijn door de gehanteerde definities van online criminaliteit. Streefdoelen van het OM met betrekking tot online criminaliteit zouden met name betrekking hebben op cybercrime in enge zin. Vormen van gedigitaliseerde criminaliteit kunnen daardoor eerder buiten de boot vallen volgens respondenten en experts. Dit komt overeen met bevindingen uit de literatuur en heeft volgens respondenten deels te maken met de wijze waarop online criminaliteit (juridisch) gedefinieerd wordt. Tenslotte geven zowel respondenten als experts tijdens de discussiesessie aan dat zaken kunnen uitstromen omdat het OM in plaats van dagvaarden kiest voor een alternatieve afdoeningswijze zoals '*knock-and-talk*'- of 'stop'-gesprekken. Dergelijke interventies zijn volgens respondenten en experts niet terug te zien in de gebruikelijke statistieken.

Verbetermogelijkheden volgens de literatuur, actoren binnen de strafrechtketen en experts uit binnen- en buitenland

Geen instroom

In de literatuur worden enkele suggesties gedaan om de aangiftebereidheid onder slachtoffers van online criminaliteit te verhogen. Een eerste aanbeveling betreft het inzetten van publieke bewustwordingscampagnes waarin de noodzaak wordt benadrukt om online criminaliteit te melden bij de politie. Een andere suggestie is om uniforme en gedegen aangiftesystemen op te zetten, bijvoorbeeld in de vorm van online aangiftesystemen. Zo zouden online aangiftesystemen de aangiftebereidheid van gebruikers om aangifte te doen van online criminaliteit verhogen. In Australië is bijvoorbeeld een online aangiftesysteem ontwikkeld speciaal voor online criminaliteit. Ten slotte wordt in de literatuur geopperd om de opportuniteitskosten (tijd, moeite en financiële kosten) voor het doen van aangifte te verminderen en de waargenomen voordelen van het aangifteproces te verhogen.

Intake en case screening

Uit de interviews blijkt dat het aangifteproces een belangrijke stap is in het proces van in- en doorstroom van online criminaliteit. Om de eerdergenoemde knelpunten in de intake van aangiften online criminaliteit te kunnen verbeteren, wordt in de literatuur aanbevolen om training op maat te geven aan intake- en servicemedewerkers. Ook respondenten en experts gaven tijdens de discussiesessie aan dat het goed

opleiden van intake medewerkers en/of casescreeners van groot belang is om de kwaliteit van aangiften te verbeteren.

Een door respondenten veelgenoemde verbetering betreft het landelijke clusteren en screenen van aangiften. Centralisatie zou ervoor moeten zorgen dat meer aangiften relevante informatie over verdachten bevatten en daarmee de opsporingskansen worden vergroot. Daarnaast kan het volgens respondenten tevens de efficiëntie van het politiewerk vergroten en het mogelijk maken om trends te signaleren en op basis daarvan de prioriteit te bepalen (bijvoorbeeld welke aangiften als eerste moeten worden opgepakt). Daarbij benadrukken respondenten het belang van geautomatiseerde dataverrijking en -analyse, met name omdat online criminaliteit minder tot de verbeelding zou spreken.

We merken graag op dat in lijn met het centraal verzamelen en screenen van online criminaliteitszaken, meerdere respondenten wijzen op bestaande initiatieven zoals het LMIO, de ECTF en Operatie Centurion.

Buitenlandse respondenten geven aan dat in het VK, de VS en Australië op eenzelfde manier wordt gezocht om problemen met betrekking tot intake en case screening op te lossen. Het meest kunnen we leren van de situatie in het VK en Australië. In het VK is er sprake van een gecentraliseerde intake van fraudezaken. In Australië zijn er voor verschillende vormen van criminaliteit centrale meldpunten waar burgers en bedrijven aangifte kunnen doen, waarna de aangifte naar het juiste politieteam wordt gestuurd. Sinds enkele jaren is er ook een landelijk meldpunt voor online criminaliteit. Een belangrijke les die we volgens respondenten van beide initiatieven kunnen leren is dat de centrale afhandeling van aangiften zorgt voor een veel betere registratie van aangiften en dat daarmee het totale aantal aangiften simpelweg snel omhoog zal gaan. Dat zegt echter niets over de verdere doorloop binnen de strafrechtketen. Respondenten geven aan dat ook verderop in de keten (van opsporingsteams tot OM en ZM) de capaciteit moet worden vergroot omdat er anders wel meer aangiften zijn die binnenstromen, maar er bij toename van de instroom gebrek aan capaciteit ontstaat om zaken op te pakken. De respondenten uit het VK geven daarbij aan dat ze zien dat er relatief veel aangiften alsnog meteen uitstromen, maar dat de aangiften die gebundeld en verrijkt zijn met informatie over de verdachte(n) er wel voor zorgen dat de zaken die ze doorsturen naar teams vaker succesvol worden opgepakt.

Opsporing

In de literatuur worden met name suggesties gedaan om het proces van de opsporing van online criminaliteit te verbeteren die gericht zijn op het wegnemen van koudwatervrees. Zo zouden trainingen ervoor kunnen zorgen dat rechercheurs bewuster worden over de mogelijke ernst van deze vormen van criminaliteit en zien dat onderzoeken lang niet altijd complex zijn. Daarnaast wordt genoemd dat opsporingsteams kunnen worden versterkt met mensen van buiten de politie omdat sommige burgers over meer expertise beschikken

op het gebied van online criminaliteit dan traditionele politiemedewerkers. Ten slotte wijzen studies er op dat er meer (inter-)nationale samenwerking nodig is tussen opsporingsinstanties zodat kennis over online criminaliteit, forensische methodes en opsporingstechnieken kunnen worden gedeeld.

Een punt voor verbetering aangaande de fase van opsporing die door zowel respondenten bij de politie als het OM wordt genoemd, houdt in dat het recherchewerk niet eindeloos door hoeft te gaan. Respondenten merken op dat daders van online criminaliteit meerdere slachtoffers tegelijkertijd kunnen maken en dat het soms lijkt alsof er eindeloos veel aangiften aan elkaar kunnen worden gekoppeld. Er moet volgens sommige respondenten dan ook 'slimmer worden opgespoord'. Het is niet altijd nodig om ál het bewijsmateriaal te verzamelen. Er kunnen ook vaker kosten-baten-overwegingen worden gemaakt en worden bekeken wat de investering (in tijd en menskracht) op gaat leveren.

OM en ZM

Door het beperkte aantal studies omtrent de in- en doorstroom van online criminaliteit bij het OM en de ZM, ontbreken aanbevelingen omtrent deze fasen in de strafrechtketen. Sommige aanbevelingen die in de literatuur worden genoemd om de in- en doorstroom van online criminaliteit te verbeteren hebben betrekking op meerdere fasen in de strafrechtketen of zelfs de gehele strafrechtketen. Zo wordt aanbevolen om lange termijnplannen te maken om vaardigheden van medewerkers te verbeteren, moet de effectiviteit van bestaande trainingen worden verbeterd en wordt aanbevolen aan strafrechtketenorganisaties om actief samen te werken met andere relevante publieke en private organisaties, zoals banken, online marktplaatsen, helpdesks en creditcard organisaties.

Tijdens de interviews werden er niet veel knelpunten omtrent de vervolging van online criminaliteit genoemd. Datzelfde geldt dan ook voor de mogelijke verbeterpunten. Een punt dat respondenten noemen en dat door experts tijdens de discussiesessies werd aangedragen is het organiseren van geschikte cursussen voor zowel OM als ZM om de koudwatervrees weg te nemen. Over andere verbeterpunten die genoemd werden bestaat verdeeldheid. Zo oordelen enkele officieren dat er een portefeuille 'gedigitaliseerde criminaliteit' (brede zin) aan officieren zou moeten worden toegekend, terwijl momenteel alleen portefeuillehouders 'cybercrime' (enge zin) zijn aangesteld. Anderen geven juist aan dat elke officier met dergelijke zaken aan de slag zou moeten kunnen en hiermee ervaring op zou moeten doen. Met betrekking tot de rechtspraak wordt als verbeterpunt genoemd om zogenoemde 'gelabelde' zittingen te organiseren. Hiermee wordt gedoeld op zittingen waarop in principe alleen online criminaliteitszaken worden behandeld. Op die manier behandelen rechters die gespecialiseerd zijn op dit thema deze zaken. De interviews laten wel zien dat er verschillend wordt gedacht over het belang van een gespecialiseerde groep rechters op dit thema.

Conclusies

Hoewel online criminaliteit volgens onderzoek gebaseerd op slachtofferenquêtes tegenwoordig tot de grootste vorm van criminaliteit behoort, blijken de meeste vormen van online criminaliteit door de wijze waarop het in de strafrechtketen wordt geregistreerd vaak niet als zodanig herkenbaar. Het zou enorm helpen wanneer bij de registratie van criminaliteit een uitgebreidere en ook regelmatig geactualiseerde lijst specifieke delicttypen zou worden gehanteerd, waardoor de verschillende verschijningsvormen op systematische wijze in kaart kunnen worden gebracht. Dit verbetert het informatiebeeld, maakt een gerichtere aanpak van de knelpunten in de strafrechtketen mogelijk en voorkomt dat een volgende studie wederom complexe analyses moet uitvoeren in een poging om de in- en doorstroom in beeld te brengen.

Waar de prevalentie van online criminaliteit op basis van slachtofferenquêtes juist erg hoog wordt geschat, vallen in de kwantitatieve analyses van BVH-registraties met name de lage instroomcijfers op. Gedigitaliseerde criminaliteit komt ongeveer 4 keer vaker voor dan cybercrime, maar de meeste vormen van online criminaliteit komen in minder dan 1% (het maximum ligt op 4% voor alle gedigitaliseerde criminaliteit tezamen) van de BVH-registraties voor. Dit beeld past bij wat bekend is over de lagere aangiftebereidheid bij online criminaliteit in vergelijking met die bij traditionele criminaliteit: veel gevallen van online criminaliteit stromen dus simpelweg nooit de strafrechtketen in.

De geïnterviewde experts zien de grootste uitdagingen aan de voorkant van de strafrechtketen, bij de politie. Met name de intake van online criminaliteit zou te wensen overlaten omdat kennis en expertise ontbreken. Dit zou ertoe leiden dat bij online criminaliteit er niet altijd een aangifte wordt opgenomen en soms alleen een melding wordt geregistreerd, waarmee de grootste bron van instroom (aangiften door burgers en bedrijven) stokt. Enerzijds klopt dit beeld met onze bevindingen. We constateerden immers dat waar de prevalentie van online criminaliteit op basis van slachtofferenquêtes erg hoog wordt geschat, in onze kwantitatieve analyses van BVH-registraties juist de lage instroomcijfers opvallen. Er is dus een groot verschil tussen door burgers ervaren – en in slachtofferenquêtes gerapporteerd – slachtofferschap en door de politie geregistreerd slachtofferschap. Verder troffen we in de kwantitatieve analyses inderdaad BVH-registraties van online criminaliteit zonder aangifte aan. Dit betrof ongeveer een kwart van de registraties. Dit is echter niet uniek voor online criminaliteit, want bij andere vormen van criminaliteit zagen we zelfs nog hogere percentages BVH-registraties zonder aangifte. Het is om die reden aan te raden om in vervolgonderzoek te kijken naar de discrepantie tussen ervaren slachtofferschap door burgers en door de politie geregistreerd slachtofferschap. Verder is het van belang om voor verschillende vormen van criminaliteit een nadere analyse te maken van de situaties waarin de politie een melding registreert in plaats van een aangifte opneemt.

Als slachtoffers van online criminaliteit wel aangifte hebben gedaan, dan blijkt dat er in 90% van de gevallen geen verdachte wordt geïdentificeerd. Dit wijst op een laag ophelderingspercentage en in combinatie met de al zeer beperkte instroom leidt het ertoe dat maar weinig zaken doorstromen in de strafrechtketen. Het percentage BVH-registraties met een aangifte waarbij tenminste één verdachte wordt geïdentificeerd verschilt overigens weinig tussen cybercrime en gedigitaliseerde criminaliteit, al valt op dat de percentages registraties met verdachte(n) juist laag zijn bij die vormen van online criminaliteit die het meest geregistreerd worden. Blijkbaar lukt het bij die zaken die het grootste deel van het werkaanbod van de politie bepalen het minst goed om er verdachten aan te koppelen. Met name het lage percentage bij online aan- en verkoopfraude (2%) is opvallend, aangezien er bij die vorm toch vaak bankrekeninggegevens beschikbaar zouden moeten zijn.

Hoewel de respondenten verschillende redenen noemden waarom opsporing bij online criminaliteit lastig is en dat er koudwatervrees bestaat, zijn lage ophelderingspercentages niet uniek voor online criminaliteit. Ook bij vermogenscriminaliteit zien we lage percentages (bij 12% van de BVH-registraties met een aangifte zagen we ook tenminste 1 verdachte geregistreerd staan), terwijl deze juist aanzienlijk hoger liggen bij fraudedelicten (31%) en al helemaal bij misdrijven tegen de lichamelijke integriteit (59%). Het verschil met misdrijven tegen de lichamelijke integriteit is wellicht niet zo verwonderlijk, omdat in die gevallen er vaak sprake zal zijn geweest van direct contact tussen dader en slachtoffer, waardoor er daderindicatie zal zijn. Het grote verschil tussen offline en online fraudedelicten is echter niet op deze wijze te verklaren. Hoewel we in deze studie niet kunnen uitsluiten dat de waargenomen verschillen samenhangen met verschillen in opsporingsinzet, komt uit de interviews naar voren dat de aanwezigheid van dader- of opsporingsindicatie een grote rol speelt bij de keuze om zaken op te pakken. Respondenten gaven aan dat dit bij online criminaliteit vaker ontbreekt waardoor zaken al sneuvelen bij de casescreening of verder niet succesvol worden opgepakt. Het ontbreken van dader- of opsporingsindicatie is echter niet uniek voor online criminaliteit, want dit speelt ook vaak bij vermogensdelicten.

Hoewel onder de respondenten consensus lijkt te bestaan dat de grootste uitdagingen in de in- en doorstroom van online criminaliteit binnen de strafrechtketen liggen binnen de politie, laten de kwantitatieve analyses zien dat er voor een aanzienlijk deel van de naar het OM ingestuurde verdachten sepots worden geregistreerd. Dat beeld zien we overigens ook voor de drie andere typen delicten waarmee we online criminaliteit vergeleken hebben. De redenen voor de sepots hebben we niet onderzocht, maar het beeld is dus niet uniek voor online criminaliteit. Daarmee lijkt het voor het verbeteren van de in- en doorstroom van online criminaliteit binnen de strafrechtketen inderdaad verstandig om vooral de aandacht te richten op de knelpunten en uitdagingen binnen de politie.

1. Inleiding

Onze huidige samenleving is in sterke mate gedigitaliseerd. Met de digitalisering van de maatschappij is ook criminaliteit gedigitaliseerd en daarmee het werkaanbod van politie en justitie veranderd. De strafrechtketen krijgt meer en meer te maken met delicten met een digitale component, ook wel online criminaliteit genoemd.

Delicten met een digitale component worden in de regel in twee categorieën ingedeeld (Holt & Bossler, 2014; Leukfeldt, 2017). Enerzijds is er sprake van nieuwe delicten, bijvoorbeeld het hacken van een database met persoonsgegevens of het platleggen van websites of netwerken. Dit soort delicten valt onder de noemer cybercrime (ook wel cybercrime in enge zin of *computer-dependent* criminaliteit genoemd). Anderzijds zijn er traditionele vormen van criminaliteit waarbij ICT een steeds belangrijkere rol speelt bij de realisatie daarvan. Voorbeelden zijn het plegen van fraude via internet en stalking. Dergelijke delicten vallen onder de noemer gedigitaliseerde criminaliteit (ook wel cybercrime in brede zin of *computer-enabled* criminaliteit genoemd). In dit onderzoek hanteren we in lijn met recente WODC-publicaties de overkoepelde term online criminaliteit voor alle delicten met een digitale component (zie bijvoorbeeld Rokven *et al.*, 2017; De Cuyper en Weijters, 2016, Beerthuizen *et al.,* 2020). Hieronder vallen zowel delicten onder de noemer cybercrime als gedigitaliseerde criminaliteit.

Het is inmiddels duidelijk dat online criminaliteit een groeiend probleem is en dat er veel slachtoffers worden gemaakt. Uit slachtofferenquêtes blijkt bijvoorbeeld dat hacken tegenwoordig vaker voorkomt dan fietsendiefstal (respectievelijk 6,9% en 4% in de 12 maanden voorafgaand aan het onderzoek – Akkermans *et al.*, 2022). Verder werd 9,7% van de burgers in Nederland slachtoffer van online oplichting en fraude (Akkermans *et al.*, 2022). Eerder slachtofferonderzoek laat zien dat burgers en bedrijven van nog veel meer vormen van online criminaliteit slachtoffer worden: van malware of ransomware tot phishing, cyberstalking en cyberbedreiging (zie bijvoorbeeld Domenie *et al.*, 2012; Holt *et al.*, 2018).

De in- en doorstroom van online criminaliteit in de strafrechtketen lijkt echter achter te blijven bij de ontwikkeling van het slachtofferschap van online criminaliteit zoals gerapporteerd in de Veiligheidsmonitor van CBS (Akkermans *et al.*, 2022). Terwijl er veel slachtoffers worden gemaakt, is het aantal veroordelingen van daders van online criminaliteit gering. Dit beeld komt overeen met de studie van Leukfeldt *et al.* uit 2012 waarbij de doorstroom van online criminaliteit binnen de strafrechtketen werd bestudeerd. Het onderzoek van Leukfeldt *et al.*, maar ook recentere studies laten zien dat er in ieder geval drie oorzaken ten grondslag liggen 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. De lage aangiftebereidheid en de wijze waarop de politie de aanpak van online criminaliteit heeft georganiseerd kunnen ervoor zorgen dat een deel van de zaken nooit de strafrechtketen 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 (OM). 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.

De drie hierboven genoemde mogelijke oorzaken geven redenen waarom er daadwerkelijk minder in- en doorstroom van online criminaliteit in de strafrechtketen zou zijn, maar er doet zich ook nog het probleem voor dat veel vormen van online criminaliteit - met name vormen van gedigitaliseerde criminaliteit - niet als zodanig herkenbaar zijn in de registraties van politie en justitie. Daarmee is mogelijk niet alleen de feitelijke in- en doorstroom gering, maar is er daarnaast ook beperkt zicht op de in- en doorstroom die er wel degelijk is. Onderhavig onderzoek moet meer zicht bieden op de in- en doorstroom van online criminaliteit in de strafrechtketen. Naast inzicht in de actuele in- en doorstroom moet het onderzoek ook inzicht bieden in mogelijke knelpunten binnen de strafrechtketen, *good practices* en verbetermogelijkheden.

Leeswijzer

In hoofdstuk 2 bespreken we eerst de onderzoeksvragen en -methoden. In hoofdstuk 3 komt aan bod of en in hoeverre er sprake is van het niet instromen van zaken online criminaliteit in de strafrechtketen. Daarna volgt in hoofdstuk 4 een beschrijving van het proces dat volgt wanneer slachtoffers wel aangifte doen bij de politie: van de intake en casescreening door de politie tot uitspraak van de rechter. Deze beschrijving wordt gevolgd door een presentatie van de resultaten van kwantitatieve analyses van recente gegevens van politie en OM die inzicht geven in de mate van in- en doorstroom van online criminaliteit binnen de strafrechtketen. Hoofdstuk 5 gaat dieper in op de knelpunten binnen de doorstroom van dergelijke zaken binnen de strafrechtketen en in hoofdstuk 6 worden mogelijke verbetermogelijkheden beschreven. Ten slotte bevat hoofdstuk 7 de conclusies en aanbevelingen.

2. Onderzoeksvragen en -methoden

Onderzoeksvragen

Dit onderzoek heeft tot doel om meer inzicht te bieden in de in- en doorstroom van online criminaliteit binnen de strafrechtketen. Tevens moet er zicht ontstaan op de knelpunten en verbetermogelijkheden. We formuleren daarom 5 onderzoeksvragen waar dit onderzoek antwoord op moet geven:

1. Zijn er volgens de literatuur vormen van online criminaliteit waarvan verdachten niet of nauwelijks de strafrechtketen instromen? Zo ja, welke? Welke verklaringen worden er in de literatuur gegeven voor die lage instroom?
2. Wat zijn de meest recente cijfers over 2018-2020 met betrekking tot de instroom en doorstroom van online criminaliteit in de strafrechtketen?
    a. Hoeveel registraties van online criminaliteit zien we in het Basisvoorziening Handhaving (BVH) systeem van de politie?
    b. Bij welk aandeel van de BVH-registraties van online criminaliteit is er ook sprake van een aangifte?
    c. Bij welk aandeel van de registraties met een aangifte wordt tenminste één verdachte gekoppeld?
    d. In welke mate stromen de geïdentificeerde verdachten door in de strafrechtketen en op welk punt (reeds bij politie, bij OM of rechtspraak) zien we afdoeningen?
    e. Hoe verhouden de cijfers die antwoord geven op vragen 2a t/m 2d zich tot dezelfde cijfers voor enkele andere vormen van criminaliteit?
3. Welke knelpunten kunnen geïdentificeerd worden binnen de in- en doorstroom van online criminaliteit in de strafrechtketen?
4. In hoeverre hebben andere landen ook te maken met de onder vraag 3 geconstateerde knelpunten? Welke ervaringen zijn er in andere landen met het oplossen van deze knelpunten?
5. Welke verbeteringen kunnen per schakel van de strafrechtketen worden doorgevoerd om de strafrechtpleging bij online criminaliteit te bevorderen?

Onderzoeksmethoden

Om de hierboven geformuleerde onderzoeksvragen te beantwoorden hebben we gebruik gemaakt van verschillende onderzoeksmethoden. Hieronder worden de verschillende methoden beschreven. Aan

het eind van deze paragraaf staat in Figuur 1 weergegeven welke onderzoeksmethoden ingezet zijn om welke onderzoeksvragen te beantwoorden.

Literatuuronderzoek

De internationale literatuurstudie had tot doel om inzicht te krijgen in welke vormen van online criminaliteit niet of nauwelijks instromen in de strafrechtketen, welke verklaringen daarvoor zijn en welke aanpassingen binnen de strafrechtketen mogelijk te maken zijn om die instroom te verhogen. Daarnaast had de literatuurstudie tot doel om breder te kijken naar knelpunten binnen de strafrechtketen die kunnen zorgen voor beperkte doorstroom van zaken. Nadrukkelijk was ook het doel om in kaart te brengen wat mogelijke verbeterpunten zijn binnen de diverse schakels van de strafrechtketen om de doorstroom van zaken juist te bevorderen.

Kwantitatieve analyses

Voor de kwantitatieve analyse van de in- en doorstroom van online criminaliteit in de strafrechtketen namen we - in navolging van Tollenaar *et al.* (2019) - BVH-registraties van de politie als startpunt. Omdat veel vormen van online criminaliteit niet als zodanig herkenbaar worden geregistreerd in de systemen, ontwikkelden we *predictive textmining* modellen. Dergelijke modellen kunnen op basis van relevante tekstkenmerken documenten met grote hoeveelheden tekst automatisch classificeren. Voor onderhavig onderzoek betekent dit dat BVH-registraties met tekstvelden - waarin bijvoorbeeld bevindingen van verbalisanten en verklaringen van slachtoffers, verdachten of getuigen zijn opgenomen - een of meerdere vormen van online criminaliteit als label konden krijgen toegewezen. We maakten daarbij gebruik van *supervised machine learning*. Bij deze techniek wordt een model getraind aan de hand van voorbeelddocumenten waarvan vooraf handmatig is vastgesteld welk label zij dienen te hebben. Na de training wordt verondersteld dat het model nieuwe documenten zelf van het juiste label kan voorzien. We ontwikkelden de modellen op basis van een selectieve steekproef (n=7.500) waarin relatief veel registraties van online criminaliteit voorkomen en pasten de modellen vervolgens toe op een grote willekeurige steekproef (n=300.000) van unieke BVH-registraties uit de jaren 2018-2020. Voor de registraties uit de grote steekproef gingen we na in hoeverre er sprake was van een aangifte en of er verdachten waren gekoppeld. Voor het vaststellen van de doorstroom in de strafrechtketen koppelden we de BVH-gegevens aan gegevens ontleend aan het systeem Betere Opsporing door Sturing op Zaken (BOSZ). Met deze koppeling kon per geregistreerde verdachte worden nagegaan of deze al vroeg in de strafrechtketen een afdoening kreeg (reprimande, politiestrafbeschikking, HALT) of door de politie werd ingezonden naar het OM. Voor het vaststellen van de doorstroom richting OM en rechtspraak hebben we vervolgens de gegevens over de naar het OM ingezonden verdachten gekoppeld aan gegevens ontleend aan het Geïntegreerd Processysteem

Strafrecht (GPS). Op basis van de GPS-gegevens konden we per verdachte vaststellen of de zaak werd geseponeerd, of de verdachte bij het OM een afdoening kreeg (strafbeschikking of transactie), of dat de verdachte werd gedagvaard en voor de rechter moest verschijnen. Om na te gaan in hoeverre de in- en doorstroom van online criminaliteit afwijkend is, herhaalden we dezelfde analyses voor drie andere vormen van criminaliteit (vermogenscriminaliteit, misdrijven tegen de lichamelijke integriteit en fraudedelicten). Nadere details over de ontwikkeling en toepassing van de *predictive textmining* modellen en de kwantitatieve in- en doorstroomanalyses worden in hoofdstuk 4 gepresenteerd.

Interviews actoren binnen de strafrechtketen

Het doel van de interviews met actoren binnen de verschillende schakels van de strafrechtketen was om zicht te krijgen op algemene knelpunten in de in- en doorstroom van online criminaliteit in de strafrechtketen. In overleg met de begeleidingscommissie van dit onderzoek (zie Bijlage 12 voor een overzicht van de leden) is een lijst opgesteld met te interviewen actoren en is besloten om binnen 5 eenheden van de politie interviews af te nemen. De eenheden waar interviews zijn afgenomen zijn: Den Haag, Noord-Holland, Noord-Nederland, Midden-Nederland en Zeeland-West-Brabant. Hierdoor hebben we binnen de helft van de eenheden interviews af kunnen nemen en is sprake van zowel een verdeling over het hele land als een verdeling tussen meer grootstedelijke gebieden als ook landelijke gebieden. Omdat het ontsluiten van de voor de kwantitatieve analyses benodigde gegevens een aanzienlijk langer traject bleek te zijn dan aanvankelijk gepland, is in afstemming met de begeleidingscommissie afgeweken van het oorspronkelijke plan om de interviews pas te plannen nadat de resultaten van de kwantitatieve analyses bekend waren. Daarmee was het niet mogelijk om in de interviews met respondenten te reflecteren op een mogelijke relatie tussen de in- en doorstroomcijfers en eventuele knelpunten. In totaal interviewden we 34 actoren binnen de strafrechtketen, waarvan 26 werkzaam waren bij de politie (P1 t/m P26), 6 bij het OM (OM1 t/m OM6) en 2 bij de zittende magistratuur (R1 en R2). Doel was om binnen de politieorganisatie in ieder geval te spreken met actoren die een rol hebben bij zowel de in- als de doorstroom van zaken: intakemedewerkers, casescreeners en een teamchef die betrokken is bij het wegingsproces. Er is gesproken met medewerkers uit verschillende teams, waaronder basisteams (BT), de districtsrecherche (DR) en de Dienst Regionale Recherche (DRR). Binnen het OM zijn officieren van justitie die online criminaliteit in hun portefeuille hebben geïnterviewd. Hier zijn de parketten geselecteerd die samenwerken met de eerder geselecteerde politie-eenheden. Bij de zittende magistratuur zijn twee rechters bevraagd die zaken met een online component hebben behandeld.

Expertinterviews buitenland

Om zicht te krijgen op eventuele *good practices* in andere landen die ook in Nederland toepasbaar zouden kunnen zijn, interviewden we 5 internationale experts. Doel van deze interviews was om zicht te krijgen op de mate waarin andere landen ook te maken hebben met de knelpunten die we in de interviews met actoren binnen de strafrechtketen vernamen en welke ervaringen er in die landen zijn met het oplossen van deze knelpunten. Op basis van de ervaring van de onderzoekers en in samenspraak met de begeleidingscommissie zijn 3 landen geselecteerd. Er zijn interviews afgenomen met 3 academische onderzoekers en 2 praktijkmensen uit het Verenigd Koninkrijk (VK), de Verenigde Staten (VS) en Australië.

Discussiesessies

De resultaten van de literatuurstudie, kwantitatieve analyses en interviews zijn ten slotte bediscussieerd met experts van binnen en buiten politie en justitie. Tijdens deze twee online discussiebijeenkomsten konden experts reflecteren op de uitkomsten en op elkaars visie. Daarnaast zijn de discussiebijeenkomsten gebruikt om te inventariseren welke mogelijke oplossingen er zijn om de geïdentificeerde knelpunten te verbeteren. In totaal deden 5 experts aan de discussiesessies mee.

	Literatuurstudie	Kwantitatieve analyse data Politie/OM	Interviews actoren strafrechtketen	Interviews experts	Discussiesessies
1. Niet instromen	■			■	■
2. Cijfers doorstroom		■			■
3. Verschil in instroom		■	■		■
4. Knelpunten doorstroom	■	■	■	■	■
5. *Good practices* buitenland				■	■
6. Verbeterpunten	■	■	■	■	■

Figuur 1 Methodenmatrix

DPIA, ethische toetsing en autorisatie

Bij de analyse van gegevens van politie en OM hebben we te maken met gevoelige gegevens, waaronder persoonsgegevens die in een aangifte, melding of zaak worden geregistreerd. Hiertoe is een *data protection impact assessment* (DPIA) gedaan. Daarnaast is het bij het NSCR beleid om bij dit soort onderzoek ethisch advies in te winnen van de Commissie Ethiek Rechtsgeleerdheid & Criminologisch Onderzoek (CERCO) van de Vrije Universiteit Amsterdam. De commissie heeft positief geadviseerd over de onderzoeksopzet. Ten slotte is ook aan het bevoegd gezag toestemming gevraagd om de benodigde (politie)gegevens te mogen analyseren. Het verkrijgen van de toestemming had

behoorlijk wat voeten in de aarde. Pas na afstemming tussen directie WODC en de Nationale Politie kwam er groen licht, waarna de benodigde gegevens door Bureau Management Informatie van de politie konden worden ontsloten. De benodigde gegevens bevatten ook grote hoeveelheden tekst uit de BVH-registraties (zoals processen-verbaal van aangifte), waarmee de gegevens in sommige gevallen direct herleidbaar waren naar natuurlijke personen. Vanwege zowel de omvang als de ongestructureerde wijze waarop persoonsgegevens in de teksten voorkwamen was het praktisch onmogelijk om deze al voor levering te ano- of pseudonimiseren. De gegevens zijn via een beveiligde downloadomgeving aan het NSCR beschikbaar gesteld, waarna deze in het Secure Analytics Lab (SAL) van het NSCR zijn opgeslagen en geanalyseerd. Het SAL betreft een *air-gapped* faciliteit met strikte procedures voor de im- en export van gegevens dat wordt beheerd door NSCR-datamanagement onder toeziend oog van de NSCR *data protection officer*.

3. Wel slachtofferschap, geen instroom

Inleiding

In dit hoofdstuk gaan we allereerst in op de vraag of en in hoeverre er sprake is van het niet instromen van online criminaliteit in de strafrechtketen. Op basis van de literatuurstudie laten we zien wat er reeds bekend is over vormen van online criminaliteit die niet of nauwelijks de strafrechtketen instromen en welke verklaringen daarvoor worden gegeven.

Het niet instromen van aangiften

Niet alle delicten stromen de strafrechtketen in, waardoor er dus delicten zijn die nooit onder de aandacht van de politie komen (Harrendorf, 2018). Zo hebben sommige delicten geen slachtoffers, zijn er slachtoffers die niet door hebben dat zij slachtoffer zijn en zijn er slachtoffers die besluiten om niet naar de politie te stappen. Ook zijn er delicten waarvan wel melding wordt gemaakt bij de politie, maar geen aangifte wordt gedaan. Bij een aangifte verzoekt de aangever namelijk tot strafvervolging door een proces-verbaal te ondertekenen, bij een melding wordt de politie slechts op de hoogte gesteld van de situatie (CBS, 2020). Iemand die bij de politie een melding komt doen, kan bijvoorbeeld (door gesprekken met de politie) beseffen dat het doen van aangifte tijdrovend en een emotioneel zwaar proces kan zijn of simpelweg niet op strafvervolging uit zijn. Voor de leesbaarheid van dit hoofdstuk zal met betrekking tot de instroom van zaken worden gesproken over aangiften.

Traditionele criminaliteit

De Veiligheidsmonitor 2019 van het Centraal Bureau voor de Statistiek (CBS) laat zien dat slachtoffers van traditionele criminaliteit in Nederland in 31,9 % van de ondervonden delicten zeggen melding te hebben gedaan bij de politie. In hetzelfde jaar zeggen slachtoffers in 22,9% van de ondervonden delicten aangifte te hebben gedaan (CBS, 2020). Vergeleken met eerdere jaren lijkt er sprake te zijn van een lichte daling in de melding- en aangiftepercentages van ondervonden delicten (in 2012 was het meldingspercentage 38,4% en het aangiftepercentage 28,7%). In de meest recente Veiligheidsmonitor 2021 is het meldingspercentage echter 35,1% en wordt in 29,3% van de ondervonden delicten aangifte gedaan (Akkermans *et al.*, 2022). Hierbij dient evenwel te worden opgemerkt dat de onderzoeksopzet van de Veiligheidsmonitor 2021 afwijkt van eerdere edities van de Veiligheidsmonitor. Door deze methodologische trendbreuk zijn de uitkomsten van deze laatste editie niet één-op-één vergelijkbaar met die van de Veiligheidsmonitor 2019 en eerder.

De beslissing van slachtoffers om wel of geen aangifte te doen bij de politie wordt beïnvloed door verschillende factoren. In de literatuur wordt hierbij onderscheid gemaakt tussen economische,

sociaal-demografische, psychologische en omgevingsfactoren (zie bijvoorbeeld studies van Goudriaan *et al.*, 2006; Torrente *et al.*, 2017; Van de Weijer *et al.*, 2019). Zo blijkt dat de ernst en het type delict belangrijke voorspellers zijn voor het wel of niet doen van aangifte bij de politie. Van ernstigere delicten (met bijvoorbeeld financiële of materiële schade) wordt vaker aangifte gedaan dan van minder ernstige delicten (Goudriaan *et al.*, 2005; Tarling & Morris, 2010; Kääriäinen & Sirén, 2011; Van de Weijer *et al.*, 2020). Van delicten als woninginbraak en autodiefstal wordt het vaakst aangifte gedaan en van vernielingen, bedreigingen en seksuele delicten het minst vaak (Goudriaan *et al.*, 2006; Van de Weijer & Bernasco, 2016). Verder laten studies zien dat verschillende sociaal-demografische factoren een relatie hebben met het doen van aangifte, zij het dat de gevonden verbanden minder sterk zijn dan bij de ernst van het delict (Goudriaan *et al.*, 2006; Van de Weijer & Bernasco, 2016; Torrente *et al.*, 2017). Zo blijken vrouwen, ouderen, en personen met een partner meer geneigd te zijn om aangifte te doen dan mannen, jongeren en mensen zonder partner. Tot slot blijkt dat het aangiftegedrag statistisch significant verschilt tussen landen en regio's (Torrente *et al.*, 2017). Zo is de kans dat er aangifte wordt gedaan van slachtofferschap in Zuid- en Oost-Europese landen de helft kleiner dan in Noord- en Centraal-Europese landen.

Aangiftebereidheid online criminaliteit

Eerder onderzoek laat zien dat de aangiftebereidheid onder slachtoffers van online criminaliteit over het algemeen lager is dan bij slachtoffers van traditionele delicten (Krone & Johnson, 2007; Domenie *et al.*, 2013; Van de Weijer & Bernasco, 2016; Van de Weijer *et al.*, 2019; De Paoli *et al.*, 2020). Uit studies in Nederland blijkt dat ongeveer 13% van de slachtoffers van online criminaliteit melding doet bij de politie (Domenie *et al.*, 2013; CBS, 2020; Van de Weijer *et al.*, 2020). Het percentage slachtoffers dat aangifte doet van online criminaliteit ligt lager en neemt volgens cijfers van de Veiligheidsmonitor 2019 licht toe: 7,1% in 2012 en 8,2% in 2019 (CBS, 2020). Deze stijging zet sterk door in de meest recente Veiligheidsmonitor 2021 (Akkermans *et al.,* 2022), waar 46,5% van de slachtoffers melding doet bij de politie en 18,7% aangifte.[1] Daarnaast blijkt dat 33,2% van de slachtoffers (ook) melding doet bij andere organisaties zoals banken, helpdesks of andere instanties dan de politie (Van de Weijer *et al.*, 2020).

Enkele studies hebben de aangiftebereidheid voor specifieke vormen van online criminaliteit vergeleken met soortgelijke offline vormen van criminaliteit. Zo blijkt uit de studie van Graham *et al.* (2020) dat voor de delicttypen ongewenst contact, diefstal en bedreiging met geweld de

[1] In verband met de hierboven genoemde trendbreuk in de laatste editie van de monitor geldt ook hier dat deze cijfers zich minder goed laten vergelijken met voorgaande jaren.

aangiftebereidheid lager is bij de online variant dan bij de offline variant. Bij ongewenste seksuele opmerkingen is de aangiftebereidheid echter hoger bij de online variant vergeleken met de offline variant. Ook bij online fraude wordt juist een hogere aangiftebereidheid gevonden dan bij traditionele fraude (Kemp, 2020).

De bereidheid van slachtoffers om aangifte te doen bij de politie verschilt voor verschillende vormen van online criminaliteit (Domenie *et al.*, 2013; Van de Weijer & Bernasco, 2016; Van de Weijer *et al.*, 2019; Van de Weijer *et al.*, 2020; CBS, 2020; Akkermans *et al.*, 2022). Uit eerdere studies blijkt dat – net als voor traditionele criminaliteit – het type online criminaliteit een belangrijke voorspeller is voor de aangiftebereidheid van online criminaliteit (Jong *et al.*, 2018; Van de Weijer *et al.*, 2020). Ook de (waargenomen) ernst van een delict is weer een belangrijke voorspeller: hoe ernstiger het delict, hoe eerder aangifte wordt gedaan door slachtoffers (Jong *et al.*, 2018; Van de Weijer *et al.*, 2020; Graham *et al.*, 2020). Bij delicten waar IT niet alleen het middel maar ook het doelwit is (cybercrimes) lijkt de aangiftebereidheid lager te liggen dan bij delicten waarbij IT alleen als hulpmiddel wordt gebruikt (gedigitaliseerde criminaliteit), zo concluderen Van de Weijer *et al.* (2020). De aangiftebereidheid van hacking-delicten ligt daarbij het laagst, met percentages die variëren tussen de 3,0% (CBS, 2020) en 11,7% (Van de Weijer *et al.*, 2020). Ook bij malware besmettingen, ransomware en DDoS-aanvallen ligt de aangiftebereidheid met respectievelijk 4,2% en 5,7% en 10% relatief laag (Van de Weijer *et al.*, 2020). Bij minder technische online delicten ligt de aangiftebereidheid hoger. Zo varieert de aangiftebereidheid bij aan- en verkoopfraude tussen de 18,1% (Van de Weijer & Bernasco, 2016) en 25,6% (Van de Weijer *et al.*, 2020), bij identiteitsfraude tussen de 16,2% (Van de Weijer & Bernasco, 2016) en 47,4% (Van de Weijer *et al.*, 2020) en ligt de aangiftebereidheid bij cyberpesten en cyberstalking respectievelijk onder de 14% (Van de Weijer & Bernasco, 2016; CBS, 2020; Akkermans *et al.*, 2022) en 30% (Van de Weijer *et al.*, 2020; Akkermans *et al.*, 2022).

De resultaten omtrent aangiftebereidheidspercentages dienen wel met enige voorzichtigheid te worden geïnterpreteerd. Zo zijn de resultaten uit enkele van de genoemde studies gebaseerd op kleine steekproeven. Bovendien worden veelal vignettenstudies gebruikt om de intentie om aangifte te doen bij de politie te meten, terwijl uit de studie van Van de Weijer *et al.* (2020) blijkt dat er een discrepantie bestaat tussen de intentie om aangifte te doen en het daadwerkelijke aangiftegedrag. De aangiftebereidheid in vignetten lag namelijk met twee derde een stuk hoger dan het daadwerkelijke aangiftepercentage (13%). Ten slotte gebruiken de studies verschillende definities voor de verschillende typen online criminaliteit.

Verklaringen lage aangiftebereidheid online criminaliteit

Er worden in de literatuur verschillende (mogelijke) verklaringen genoemd waarom slachtoffers van online criminaliteit geen aangifte doen. Ten eerste weten individuen niet altijd dat ze slachtoffer zijn (Goodman & Brenner, 2002; Wall, 2008; Domenie *et al.*, 2012; Yar & Steinmetz, 2019; De Paoli *et al.*, 2020). Zo kan het bij computervredebreuk het geval zijn dat een dader een computer is binnengedrongen, maar dat slachtoffers dit niet door hebben. Als individuen wel op de hoogte zijn, kan het zijn dat ze niet toe willen geven dat ze slachtoffer zijn of zich schamen voor hun slachtofferschap (De Paoli *et al.*, 2020; Goodman & Brenner, 2002; Wall, 2008; Goucher, 2010; Button *et al.*, 2020). Slachtoffers kunnen bijvoorbeeld gevoelens van schaamte ervaren omdat zij op een phishing-link hebben geklikt of geld hebben overgemaakt na een oplichting via een online handelsplatform. Een andere veelgenoemde verklaring is dat individuen de ernst en impact van online delicten als laag ervaren en daardoor minder snel geneigd zijn om aangifte te doen (Wall, 2008; Yar & Steinmetz, 2019; Leukfeldt *et al.*, 2012; Jong *et al.*, 2018; Van de Weijer *et al.*, 2020; Graham *et al.*, 2020; De Paoli *et al.*, 2020; Button *et al.*, 2020). Soms is er geen (financiële) schade of is de financiële schade al vergoed door bijvoorbeeld verzekeringsmaatschappijen of financiële instellingen (Button *et al.*, 2020; Leukfeldt *et al.*, 2012). In andere gevallen zien slachtoffers online incidenten zoals malware-infecties niet als criminaliteit (Button *et al.*, 2020). Een vierde verklaring die wordt genoemd, is het gebrek aan vertrouwen van slachtoffers in de politie om daders van online criminaliteit op te sporen en aan te houden (Goucher, 2010; Domenie *et al.*, 2013; De Paoli *et al.*, 2020; Graham *et al.*, 2020; Van de Weijer *et al.*, 2020). Zo blijkt uit een recente studie van Graham *et al.* (2020) dat het vertrouwen in de politie om daders van online criminaliteit te kunnen identificeren en aan te houden lager ligt dan bij traditionele vormen van criminaliteit. Bovendien vonden Van de Weijer *et al.* (2020) dat een van de belangrijkste redenen voor slachtoffers om geen aangifte te doen is dat ‘de politie er niks aan doet’. Aan de andere kant vonden Jong *et al.* (2018) geen verband tussen de attitude van mensen tegenover de politie en de aangiftebereidheid en bleek zelfs dat respondenten die eerder aangifte hebben gedaan en daar ontevreden over waren, een hogere aangiftebereidheid hebben dan respondenten die nog nooit aangifte hebben gedaan.

Tenslotte worden er verklaringen genoemd omtrent de mogelijkheden om aangifte te doen. Zo kan er onder slachtoffers een gebrek aan bewustzijn bestaan van de mogelijkheid om aangifte te doen (De Paoli *et al.*, 2020; Button *et al.*, 2020). Slachtoffers zijn dan simpelweg niet op de hoogte dat zij aangifte kunnen doen van de online delicten. Daarnaast zijn er voor slachtoffers meerdere manieren om een melding of aangifte te doen: zo heeft de politie meerdere aangiftemodaliteiten (telefonisch, op het bureau of via internet) en zijn er (niet aan de politie gelinkte) alternatieve meldingskanalen bij banken, de Fraudehelpdesk of internet serviceproviders (Cross, 2018; Van de Weijer *et al.*, 2020). In dit verband

merkte Wall (2007) op dat het tijd nodig heeft voordat burgers zich hebben aangepast aan dergelijke nieuwe mogelijkheden. Andere studies vonden geen statistisch significante verschillen in de relatie tussen het aantal aangiftemogelijkheden bij de politie (bijvoorbeeld via telefoon of internet) en de aangiftebereidheid (Jong *et al.*, 2018; Van de Weijer *et al.*, 2020).

Andere factoren, zoals demografische factoren, laten wisselende resultaten zien of zijn nog beperkt onderzocht in relatie tot online criminaliteit. Zo vonden Van de Weijer *et al.* (2019) dat herhaald slachtofferschap, inkomen en opleidingsniveau negatief samenhangen met de meldingsbereidheid van slachtoffers. Herhaalde slachtoffers en mensen met een hoger inkomen of hoger opleidingsniveau zijn minder snel geneigd om een melding te doen van online criminaliteit bij de politie dan personen die voor het eerst slachtoffer zijn geworden en slachtoffers met een lager opleidingsniveau en een lager inkomen. Herhaalde slachtoffers zijn wel sneller geneigd om melding te doen bij andere organisaties dan de politie, ten opzichte van personen die voor de eerste keer slachtoffer zijn geworden (Domenie *et al.*, 2013; Cross *et al.*, 2016; Van de Weijer *et al.*, 2019). In een latere studie van Van de Weijer *et al.* (2020) worden echter geen statistisch significante verschillen gevonden met betrekking tot inkomen en opleidingsniveau. Ook lijken er verschillen te zijn tussen online delicten in de factoren die bepalen of iemand wel of geen melding doet (zie Van de Weijer *et al.*, 2019 voor gedetailleerde beschrijvingen van deze verschillen). Zo blijken oudere slachtoffers bij online fraude minder vaak aangifte doen bij de politie dan jongere slachtoffers, terwijl bij hacking oudere slachtoffers juist vaker aangifte doen dan jongere slachtoffers. Ten slotte zijn er enkele demografische factoren gevonden die de meldingsbereidheid van online delicten beïnvloeden, die voor traditionele criminaliteit precies andersom zijn (Van de Weijer *et al.*, 2019). Zo zijn bij online criminaliteit mannen meer geneigd om melding te doen dan vrouwen, slachtoffers met een niet-westerse migratieachtergrond meer geneigd om melding te doen dan slachtoffers met een Nederlandse achtergrond, mensen zonder baan meer geneigd om melding te doen dan mensen met baan en zijn mensen met een lager inkomen meer geneigd om melding te doen dan mensen met een hoger inkomen. In een vervolgstudie van Van de Weijer *et al.* (2020) wordt echter maar een beperkt aantal statistisch significante verbanden gevonden tussen demografische factoren en meldingsbereidheid.

Naast burgers kunnen ook organisaties aangifte doen van online criminaliteit. Voor deze organisaties worden enkele specifieke verklaringen genoemd voor het niet doen van aangifte (Jewkes & Yar, 2008; Brown, 2015; Van den Eeden *et al.*, 2021). Zo kan een bedrijf reputatieschade ondervinden wanneer bekend wordt dat het slachtoffer is van online criminaliteit (Jewkes & Yar, 2008; Van den Eeden *et al.*, 2021). Ook zijn er bedrijven die vinden dat zij in vergelijking met de politie een beter begrip hebben van de problemen en een effectievere manier hebben om deze problemen aan te pakken. Hiermee hangt samen dat bedrijven een andere doelstelling hebben dan de politie. Waar de politie wil bewijzen

dat een delict heeft plaatsgevonden, is het voor organisaties belangrijker om het binnendringen te stoppen, verliezen te minimaliseren en negatieve publiciteit te voorkomen (Brown, 2015; De Paoli *et al.*, 2020; Van den Eeden *et al*., 2021).

Resumé

Eerder onderzoek laat zien dat de aangiftebereidheid onder slachtoffers van online criminaliteit over het algemeen lager is dan bij slachtoffers van traditionele delicten. Uit Nederlandse studies blijkt dat ongeveer 13% van de slachtoffers van online criminaliteit melding doet bij de politie. De bereidheid van slachtoffers om aangifte te doen bij de politie verschilt voor verschillende vormen van online criminaliteit. Bij delicten waar IT niet alleen het middel maar ook het doelwit is (cybercrimes) lijkt de aangiftebereidheid lager te liggen dan bij delicten waarbij IT alleen als hulpmiddel wordt gebruikt (gedigitaliseerde criminaliteit). Uit eerdere studies blijkt dat – net als voor traditionele criminaliteit – het type online criminaliteit een belangrijke voorspeller is voor de aangiftebereidheid van online criminaliteit. Verder is – wederom net als bij traditionele criminaliteit – de (waargenomen) ernst van een delict een belangrijke voorspeller: hoe ernstiger het delict, hoe eerder aangifte wordt gedaan.

Er worden in de literatuur verschillende verklaringen genoemd waarom slachtoffers van online criminaliteit geen aangifte doen. Zo weten individuen en bedrijven niet altijd dat ze slachtoffer zijn of zien slachtoffers online incidenten zoals malware-infecties niet als criminaliteit. In de gevallen waarbij slachtoffers wel op de hoogte zijn van hun slachtofferschap, kunnen verschillende factoren ertoe leiden dat ze toch geen aangifte doen. Een veelgenoemde verklaring is dat individuen de ernst en impact van online delicten als laag ervaren en daardoor minder snel geneigd zijn om aangifte te doen. In andere gevallen is er geen of weinig (financiële) schade of is de schade al vergoed door bijvoorbeeld verzekeringsmaatschappijen of financiële instellingen. Verder kan schaamte een rol spelen bij het niet melden van slachtofferschap. Ten slotte kan spelen dat slachtoffers een gebrek aan vertrouwen hebben in de politie om daders van online criminaliteit op te sporen en aan te houden.

4. In- en doorstroom in cijfers

Inleiding

Alvorens we in dit hoofdstuk een kwantitatieve analyse van de in- en doorstroom van online criminaliteit in de strafrechtketen presenteren, geven we eerst een korte beschrijving van het proces van de in- en doorstroom in de praktijk, zoals beschreven door de respondenten tijdens de interviews.

Het proces van in- en doorstroom in de strafrechtketen

Slachtoffers die besluiten aangifte te doen bij de politie kunnen dit in Nederland op verschillende manieren en via verschillende kanalen doen. Afhankelijk van het type delict kan aangifte worden gedaan via internet, telefonisch of fysiek op het politiebureau. Ook kan het voorkomen dat een slachtoffer aangifte doet op de locatie waar het slachtofferschap heeft plaatsgevonden. Het eerste contact van aangevers met de politie loopt in de meeste gevallen via een Regionaal Service Center (RSC). Na registratie zet het RSC meldingen in de regel door naar het basisteam in de plaats waar het delict heeft plaatsgevonden. Het proces voor de afhandeling van online criminaliteit verschilt op hoofdlijnen niet van de afhandeling van traditionele criminaliteitszaken.

Zowel voor traditionele als online delicten geldt dat een zaak nog op andere manieren dan middels een aangifte de strafrechtketen kan instromen. Een eerste manier waarop delicten anders dan via aangiften ter kennis van de politie kunnen komen, is via 'het blauw op straat'. Bijvoorbeeld via een (112-)melding of wanneer een dader op heterdaad wordt betrapt door de politie. Verder kan de politie ambtshalve een aangifte opnemen als het slachtoffer geen aangifte wil of kan doen (bijvoorbeeld in het geval van moord). Tenslotte is het mogelijk dat politiemedewerkers binnen een lopende zaak op een nieuw feit of dader stuiten.

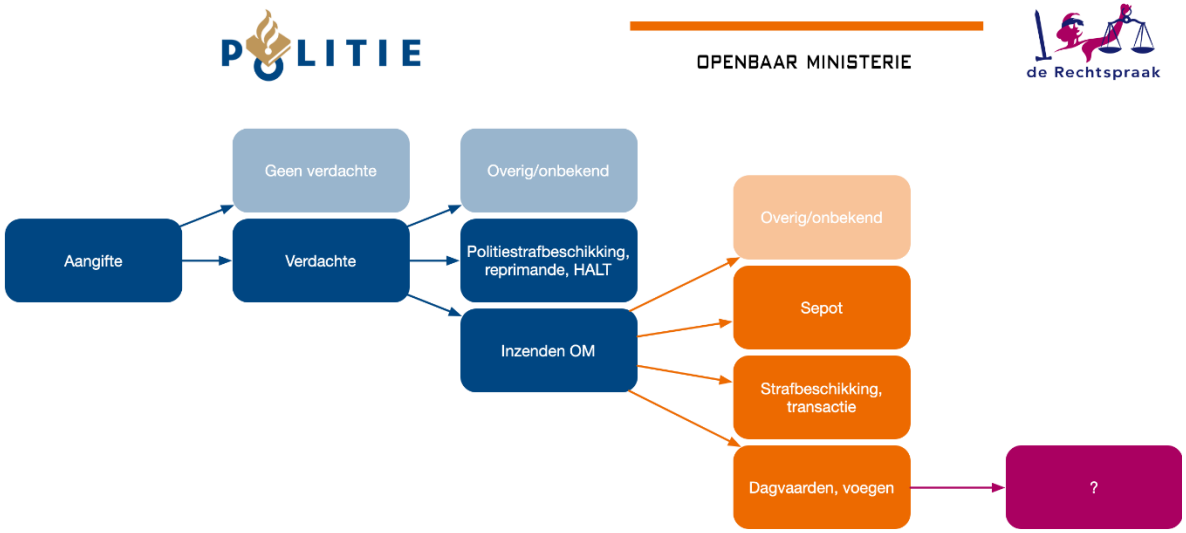
Net als het reguliere aangifteproces verloopt de casescreening en toewijzing aan een opsporingsteam voor traditionele en online delicten op gelijksoortige wijze. Nadat een aangifte via een van de aangiftemodaliteiten wordt opgenomen, komt deze terecht bij casescreeners. Zij selecteren welke aangiften in aanmerking komen voor nader strafrechtelijk onderzoek en wijzen een zaak af of zetten deze door naar een dossiermanager. De dossiermanager wijst vervolgens de zaak toe aan een van de verschillende opsporingsteams binnen de politieorganisatie. Casescreeners onderzoeken of een aangifte voldoende aanknopingspunten heeft om tot opsporing over te gaan. Daarbij onderzoeken ze of de aangifte dader- of andere opsporingsindicaties bevat.

In dit deel van het proces kunnen aangiften van enkele vormen van online criminaliteit ook geclusterd worden door specialistische politieteams zoals de Electronic Crimes Taskforce (ECTF) of het Landelijk Meldpunt Internetoplichting (LMIO). Het LMIO verzamelt bijvoorbeeld online aangiften van aan- en

verkoopfraude. Daarna onderzoekt het LMIO of aangiften aan elkaar gekoppeld kunnen worden, bijvoorbeeld omdat hierin hetzelfde bankrekeningnummer, IP-adres en/of e-mailadres voorkomt. Verder heeft iedere eenheid een cybercrimeteam. Het is mogelijk dat aangiften vanuit de intake direct worden doorgezet naar een dergelijk team, bijvoorbeeld omdat bij het opnemen van de aangifte specialistische kennis vereist is. Cybercrimeteams gaan echter ook proactief op zoek naar zaken. Dit doen zij met focus op een bepaalde thematiek.

Via de casescreeners komen aangiften met voldoende opsporingsindicatie terecht bij een van de opsporingsteams binnen de politieorganisatie: basisteams, districtsrecherches, regionale recherche of gespecialiseerde teams. Als onderdeel van de opsporingstaak van de politie verrichten de teams onderzoek naar strafbare feiten onder het gezag van de officier van justitie. Verschillende criteria bepalen naar welk team een zaak gaat, waaronder het aantal jaar straf dat op het delict staat, het aantal aangiften, de complexiteit van het strafbare feit en de rol van de verdachte in het criminele netwerk.

Nadat een opsporingsonderzoek is uitgevoerd en wanneer een concrete verdachte in beeld is, kan de politie ervoor kiezen om een zaak door te sturen naar het OM of onder het gezag van een officier van justitie een andere beslissing te nemen. Overige beslissingen in de opsporingsfase bestaan uit een strafbeschikking, Halt-straf, reprimande of onvoorwaardelijk sepot. Wanneer een zaak wordt ingezonden naar het OM, kan het OM besluiten een verdachte te dagvaarden, een zaak (voorwaardelijk of onvoorwaardelijk) te seponeren of om een strafbeschikking op te leggen. Een zaak waarbij de verdachte een dagvaarding ontvangt stroomt door naar de zittende magistratuur. De rechter kan dan een verdachte schuldig verklaren of vrijspreken. Wanneer een verdachte wordt schuldig verklaard, dan kan de rechter een voorwaardelijke of onvoorwaardelijke straf of maatregel opleggen, soms met bijzondere voorwaarden.



Figuur 2 Schematische weergave van in- en doorstroom in de strafrechtketen

Figuur 2 geeft de in- en doorstroom in de strafrechtketen schematisch weer zoals deze in dit hoofdstuk voor online criminaliteit op basis van grootschalige kwantitatieve gegevens van de politie en het OM voor de jaren 2018-2020 in beeld zal worden gebracht.

Bronnen voor in- en doorstroomanalyses

In dit deel gaan we kort in op de mogelijkheden die verschillende bronnen bieden voor het verrichten van in- en doorstroomanalyses van online criminaliteit. We lichten toe waarom cijfers van het CBS niet volstaan, waarna we beschrijven welke bronnen we voor het onderhavige onderzoek wel zullen gebruiken.

CBS-cijfers geven beperkt beeld

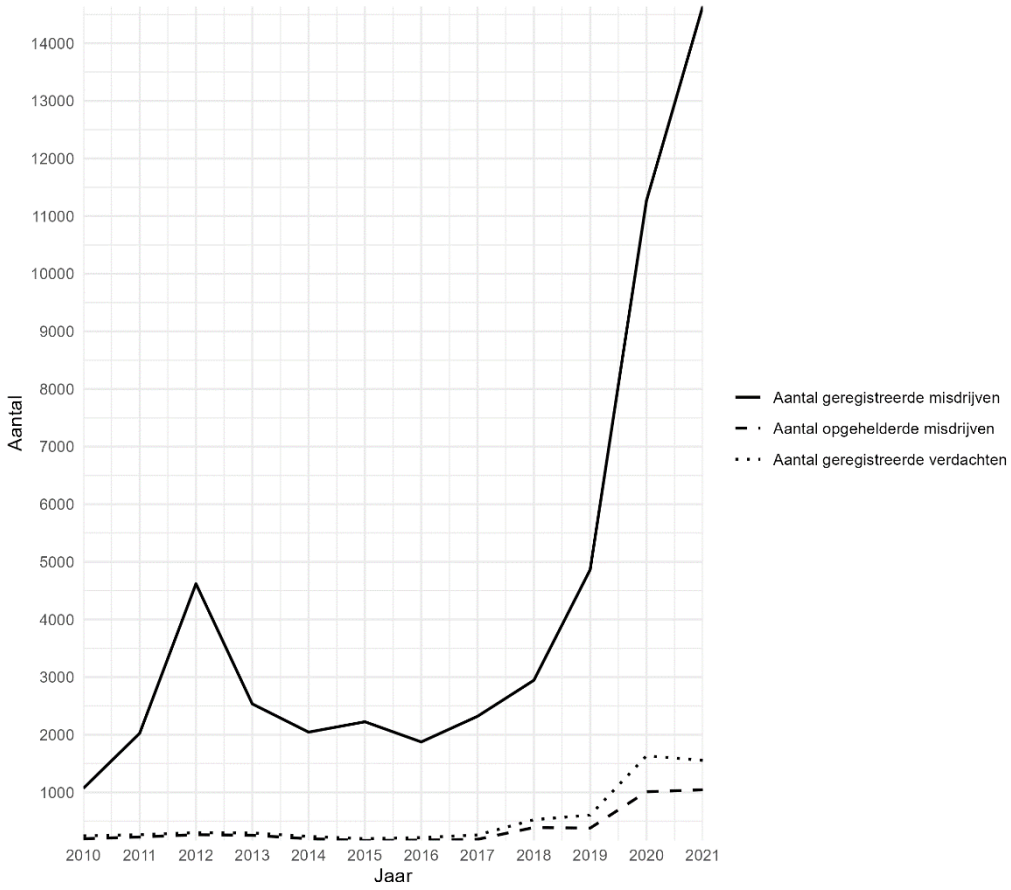
Het CBS registreert jaarcijfers over geregistreerde criminaliteit waarbij alle verschillende vormen van criminaliteit worden ingedeeld volgens de Standaard Classificatie Misdrijven (Politie) 2010. De enige vorm van online criminaliteit die in die classificatie onderscheiden wordt betreft computervredebreuk zoals omschreven in het Wetboek van Strafrecht, artikel 138ab. Figuur 3 laat de ontwikkeling zien in het totaal aantal geregistreerde misdrijven die in de periode 2010-2021 als computervredebreuk gerubriceerd werden en de bijbehorende aantallen opgehelderde misdrijven en geregistreerde verdachten. Wat vooral opvalt is de snelle stijging in het aantal geregistreerde gevallen van computervredebreuk, van jaarlijks enkele duizenden in de jaren 2010 tot 2019 tot bijna 15.000 registraties in het jaar 2021. Het CBS merkt bij deze cijfers echter het volgende op:

> "Sinds 30 april 2020 is het mogelijk om via internet aangifte te doen van WhatsAppfraude (vriend-in-noodfraude). Hiervan werd veelvuldig gebruik gemaakt. In de maanden mei tm december 2020 werden circa 20.000 aangiften van WhatsAppfraude gedaan. Deze aangiften zijn echter niet allemaal als valsheid in geschrifte geregistreerd maar een deel is (ten onrechte) als computervredebreuk geregistreerd." (Centraal Bureau voor de Statistiek, 2023).

Deze opmerking van het CBS wijst op het probleem dat verschillende vormen van online criminaliteit in de politiesystemen niet altijd juist gerubriceerd worden. Maar zelfs al zouden dit soort registratiefouten niet worden gemaakt, dan nog zouden deze CBS-cijfers geen volledig beeld geven van de instroom van online criminaliteit in de strafrechtketen. Bepaalde vormen van online criminaliteit worden immers gerubriceerd onder andere categorieën, zoals blijkt uit de opmerking over de vele gevallen van vriend-in-noodfraude (VIN-fraude) die eigenlijk als valsheid in geschrifte hadden moeten worden geregistreerd. De CBS-cijfers geven kortom een zeer beperkt beeld van de instroom van online criminaliteit in de strafrechtketen en we zullen in deze studie dan ook van andere bronnen gebruik moeten maken.

Overigens is het van belang om de snelle stijging van het aantal geregistreerde gevallen van computervredebreuk te bezien in de context van dalende criminaliteitscijfers. In dezelfde periode daalde de totaal geregistreerde criminaliteit van 1.200.825 misdrijven in 2010 naar 757.795 misdrijven in 2021. De ontwikkeling in geregistreerde computervredebreuk gaat dus tegen de dalende trend in, maar deze cijfers hebben alleen betrekking op een klein deel van alle online criminaliteit en de trends in andere vormen van online criminaliteit blijven hiermee dus buiten zicht.

Naast de stijging in het aantal geregistreerde gevallen van computervredebreuk laat Figuur 3 ook zien dat het aantal opgehelderde gevallen en het aantal geregistreerde verdachten in recente jaren is gestegen van enkele honderden in de jaren 2010-2019 tot boven de duizend in 2020, al zien we daar in 2021 geen verdere groei.



Figuur 3 Registraties computervredebreuk 2010-2021. Bron: CBS Statline (eigen bewerking)

Een beter beeld vraagt om gedetailleerde analyses van politieregistraties

Voor het vaststellen van de instroom nemen we een grote steekproef (n=300.000) van registraties uit de Basisvoorziening Handhaving (BVH) van de politie als startpunt. In het BVH-systeem registreert de

politie incidenten, meldingen en aangiften en de aan de incidenten gekoppelde acties zoals processen-verbaal van verhoor van getuigen of verdachten. In navolging van eerder onderzoek waarin online criminaliteit op basis van BVH-registraties werd geanalyseerd beperken we ons hier niet tot de BVH-registraties van alleen geregistreerde misdrijven omdat "een onbekend deel van de meldingen of acties waarin sprake kan zijn van een ICT-component niet systematisch wordt geregistreerd" (Tollenaar *et al.* 2019:12). We analyseren een steekproef uit alle BVH-registraties en sluiten daarmee op voorhand geen informatie uit, behalve die betrekking heeft op rechercheonderzoeken die enkel in het politieregistratiesysteem Summ-IT[2] en niet in BVH worden geregistreerd. Per registratie kunnen we nagaan of er ook sprake is van een aangifte. Dat is lang niet altijd het geval omdat in BVH niet alleen aangiften worden vastgelegd, maar ook incidenten, meldingen en allerlei andere registraties die met eigen acties van politiemedewerkers te maken hebben. De BVH-registraties met een aangifte vormen een duidelijk startpunt van de strafrechtketen en BVH-registraties die geclassificeerd zijn als online criminaliteit en waarbij tenminste 1 aangifte is geregistreerd, markeren dan ook wat we hier de *instroom* van online criminaliteit in de strafrechtketen zullen noemen. Instroom in de strafrechtketen, die op een andere manier dan middels een aangifte plaatsvindt, valt daarmee buiten de scope van de in dit hoofdstuk gepresenteerde kwantitatieve in- en doorstroomanalyses.

De instroom van online criminaliteit in de strafrechtketen staat aan de linkerkant van Figuur 2 weergegeven. Vervolgens zijn er verschillende stappen in de *doorstroom* te onderscheiden. De eerste stap in de doorstroom wordt bepaald door het al dan niet kunnen koppelen van een verdachte aan de registratie. Voor de bepaling van de verdere doorstroom hebben we de BVH-registraties gekoppeld aan gegevens ontleend aan het systeem Betere Opsporing door Sturing op Zaken (BOSZ). Met deze koppeling kan per geregistreerde verdachte worden nagegaan of deze al vroeg in de strafrechtketen een afdoening krijgt (reprimande, politiestrafbeschikking, HALT) of door de politie wordt ingezonden naar het OM[3]. Voor het vaststellen van de doorstroom richting OM en rechtspraak hebben we vervolgens van de registraties van de naar het OM ingezonden verdachten gekoppeld aan gegevens ontleend aan het Geïntegreerd Processysteem Strafrecht (GPS). Op basis van de GPS-gegevens konden we per verdachte vaststellen of de zaak bij het OM werd geseponeerd, of de verdachte een strafbeschikking of transactie kreeg, of dat de verdachte werd gedagvaard en voor de rechter moest verschijnen[4]. Dagvaarding vormt in dit onderzoek het eindpunt van de doorstroomanalyse. De

[2] Summ-IT betreft het werkprocessensysteem van de recherche.

[3] De wijze waarop alle afzonderlijke in BOSZ gehanteerde afhandelingen voor dit onderzoek zijn gerubriceerd wordt toegelicht in Bijlage 1.

[4] De wijze waarop alle afzonderlijke in GPS gehanteerde afdoeningen voor dit onderzoek zijn gerubriceerd wordt toegelicht in Bijlage 1.

mogelijk verschillende uitkomsten van rechtszaken vallen daarmee buiten de scope van deze studie (vandaar het vraagteken aan de rechterkant van Figuur 2).

Online criminaliteit in politieregistraties

Tollenaar *et al.* (2019) hebben reeds uitgebreid beschreven waarom het lastig is om voor BVH-registraties vast te stellen of het een registratie van online criminaliteit betreft. Politiemedewerkers die meldingen of aangiften opnemen stellen vast om wat voor vorm van criminaliteit het gaat en leggen dit vast op basis van een maatschappelijke klasse. Hoewel in het Gegevensmodel Nationale Politie 2013 de maatschappelijke klasse F90 (cybercrime)[5] voorkomt, wordt dit in het BVH-systeem niet altijd (correct) gehanteerd. Bovendien betreft F90 een verzamelcategorie voor de verschillende verschijningsvormen van cybercrime in enge zin. Voor de meeste vormen van gedigitaliseerde criminaliteit bestaan geen specifieke maatschappelijke klassen, waardoor dergelijke delicten vaak als traditionele delicten gerubriceerd worden. Dit zijn precies de redenen waarom de cijfers van het CBS onvoldoende inzicht geven in de instroom van online criminaliteit in de strafrechtketen. Het blijkt daarmee dus onmogelijk om op basis van gestructureerde informatie uit het BVH-systeem, zoals de maatschappelijke klassen, allerlei verschillende verschijningsvormen van online criminaliteit in kaart te brengen. De meeste BVH-registraties bevatten echter wel veel ongestructureerde tekst (zoals de processen-verbaal van aangifte of verhoor en bevindingen) op basis waarvan te achterhalen valt of er sprake is van online criminaliteit en van welke vorm.

Jaarlijks worden miljoenen BVH-registraties gemaakt, waarvan slechts een (klein) deel betrekking zal hebben op online criminaliteit. Het handmatig doorzoeken van de vrije tekstvelden is daarmee ondoenlijk. Om die reden hebben we voor dit onderzoek in navolging van Tollenaar *et al.* (2019) gebruik gemaakt van *predictive textmining*, een techniek waarbij we *machine learning* modellen hebben ontwikkeld die BVH-registraties automatisch kunnen classificeren op basis van alle in de registraties aanwezige tekst. In het vervolg van dit hoofdstuk gaan we eerst in op de wijze waarop we deze classificatiemodellen hebben ontwikkeld, waarna we ze toepassen om de in- en doorstroom van online criminaliteit in de strafrechtketen te analyseren.

[5] De maatschappelijke klasse F90 staat voor 'cybercrime' en bevat 'alle vormen van bezitsaantasting waarbij de computer zowel het middel als het doel is' (Tollenaar *et al.*, 2019).

Ontwikkeling classificatiemodellen voor bepaling online criminaliteit in politieregistraties

In dit onderzoek worden negen typen online criminaliteit onderscheiden: vier vormen van cybercrime (hacken, malware, ransomware en DDoS-aanval) en vijf vormen van gedigitaliseerde criminaliteit (online bedreiging, online stalking, online smaad/laster/belediging, online oplichting en *money muling*), waarbij we online oplichting nog uitsplitsen naar phishing, online identiteitsfraude, online aan- en verkoopfraude, VIN-fraude, helpdeskfraude en overige online oplichting. Definities voor de verschillende vormen van online criminaliteit zijn te vinden in Bijlage 2.

Predictive textmining modellen

Een *predictive textmining* model kan op basis van relevante tekstkenmerken documenten met grote hoeveelheden tekst automatisch classificeren. Tollenaar *et al.* (2019) hebben laten zien dat de door hen ontwikkelde *predictive textmining* modellen in staat waren om sommige vormen van online criminaliteit zeer accuraat te classificeren. Voor onderhavig onderzoek betekent dit dat BVH-registraties met tekstvelden - waarin bijvoorbeeld bevindingen van verbalisanten en verklaringen van slachtoffers, verdachten of getuigen zijn opgenomen - een of meerdere vormen van online criminaliteit als label kunnen krijgen toegewezen. We maken daarbij gebruik van *supervised machine learning*. Bij deze techniek wordt een model getraind aan de hand van voorbeelddocumenten waarvan vooraf handmatig is vastgesteld welke labels zij dienen te hebben. Na de training wordt verondersteld dat het model nieuwe documenten van het juiste label kan voorzien. In het vervolg van deze paragraaf worden de stappen besproken die nodig zijn om *predictive textmining* toe te passen op de BVH-registraties: dataselectie, databewerking, en de feitelijke ontwikkeling van de *predictive textmining* modellen.

Dataselectie

Het steekproefkader bestaat uit alle politieregistraties in het BVH-systeem in de jaren 2018 tot en met 2020. Van BVH-registraties willen we vaststellen welke een of meerdere vormen van online criminaliteit bevatten. In de periode 2018-2020 waren er in totaal 10.420.594 unieke BVH-registraties. Een overzicht van het steekproefkader is weergegeven in Tabel 1.

Tabel 1 Steekproefkader

	2018	2019	2020	Totaal
Unieke BVH-registraties	3.373.766	3.404.970	3.641.858	10.420.594

Voor dit onderzoek zijn twee verschillende steekproeven uit BVH getrokken. Een selectieve steekproef waarin relatief veel online criminaliteit voorkomt om de *predictive textmining* modellen mee te ontwikkelen en een grote aselecte steekproef die in het volgende deel van dit hoofdstuk gebruikt zal

worden voor de beschrijvende analyses van in- en doorstroom van online criminaliteit in de strafrechtketen.

Selectieve steekproef

Om de *predictive textmining* modellen voor de verschillende vormen van online criminaliteit te ontwikkelen zijn train- en testdatasets van BVH-registraties nodig die tekstelementen bevatten en waarvan bekend is of zij een of meerdere vormen van online criminaliteit bevatten. De tekstelementen die voor dit onderzoek worden gebruikt, bestaan uit de bij een BVH-registratie behorende registraties van *bevindingen*, *toelichtingen*, *verklaringen* en *MO-teksten*. Onderzoekers dienen de datasets op basis van de tekstelementen van labels van de verschillende vormen van online criminaliteit te voorzien; het zogenaamde annoteren. Voor het trainen van de *predictive textmining* modellen is het van belang dat er voldoende registraties van online criminaliteit in de datasets aanwezig zijn, omdat er anders te weinig informatie is om goed presterende classificatiemodellen te ontwikkelen. Om dit probleem zoveel mogelijk te voorkomen, maken we voor de train- en testdataset in navolging van Tollenaar *et al.* (2019) gebruik van een selectie van BVH-registraties waarvoor we van tevoren al weten dat ze relatief veel online criminaliteit bevatten. De selectie bestaat uit (1) registraties die naar voren komen uit een cybercrime query die op basis van een uitgebreide combinatie van specifieke woorden registraties van online criminaliteit uit alle BVH-registraties filtert, exclusief registraties met maatschappelijke klasse F90 (n=625.864) en (2) een steekproef van 5.000 registraties per jaar met de maatschappelijke klasse F90. De query die is gebruikt om registraties online criminaliteit te filteren is overgenomen van Tollenaar *et al.* (2019) en opgenomen in Bijlage 3. In overeenstemming met het onderzoek van Tollenaar *et al.* (2019) is gekozen voor een train- en testdataset van in totaal 7.500 registraties. De train- en testdataset bestaat uit 5.000 registraties uit de query online criminaliteit en 2.500 registraties met de maatschappelijke klasse F90, beide getrokken op basis van een naar het absolute aantal per jaar gewogen steekproef. Een overzicht van de getrokken selectieve steekproef voor de train- en testdataset is weergegeven in Tabel 2.

Tabel 2 Selectieve steekproef voor train- en testdataset

Jaar	2018	2019	2020	Totaal 2018-2020
Unieke BVH-registraties (steekproefkader)	3.373.766	3.404.970	3.641.858	10.420.594
Selectieve steekproef				
Query online criminaliteit (zonder F90)	167.302	194.572	263.990	625.864
Steekproef query (zonder F90)	5.000	5.000	5.000	15.000
F90				22.065
Selectieve steekproef query + F90 (1)				37.065
Registraties met missende of lege documenten				63
Selectieve steekproef query + F90 met tekstelementen (2)				37.002
Gewogen steekproef query (zonder F90)	1.337	1.554	2.109	5.000
Gewogen steekproef F90	428	675	1.397	2.500
Selectieve steekproef voor annotatie				7.500

De selectieve steekproef van de query + F90 (2) (n=37.002) bevatte 24.520 bevindingen, 61.892 toelichtingen, 38.361 verklaringen en 1.646 MO-teksten. Dit laat zien dat er voor de beoordeling van een individuele BVH-registratie vaak over (meerdere) toelichtingen, verklaringen en bevindingen kan worden beschikt, maar slechts in sommige gevallen over MO-teksten.

Aselecte steekproef

Voor de jaren 2018-2020 is uit het steekproefkader een aselecte steekproef van 300.000 BVH-registraties getrokken (100.000 BVH-registraties per jaar). Voor 3.012 van de 300.000 BVH-registraties (1%) waren de tekstdocumenten *bevindingen*, *toelichtingen*, *verklaringen* en *MO-teksten* leeg. Registraties zonder tekst bevatten geen informatie op basis waarvan kan worden bepaald op welke typen delicten ze eventueel betrekking hebben. Na het verwijderen van de registraties zonder tekst bestond de aselecte steekproef uit 296.988 unieke BVH-registraties. Een overzicht van de getrokken aselecte steekproef wordt weergegeven in Tabel 3.

Tabel 3 Aselecte steekproef voor in- en doorstroom analyses

Jaar	2018	2019	2020	Totaal 2018-2020
Unieke BVH-registraties (steekproefkader)	3.373.766	3.404.970	3.641.858	10.420.594
Aselecte steekproef				
Aselecte steekproef	100.000	100.000	100.000	300.000
Registraties met missende documenten				3.012
Aselecte steekproef voor in- en doorstroomanalyse				296.988

Annoteren selectieve steekproef

Voor het annoteren van de selectieve steekproef van 7.500 BVH-registraties hebben we de door Tollenaar *et al.* (2019) ontwikkelde annotatietool aangepast. De annotatietool is een technisch hulpmiddel dat de tekstelementen uit de BVH-registraties op een overzichtelijke manier aan de annoteurs presenteert, waarmee zij eenvoudig de registraties kunnen beoordelen en van labels kunnen voorzien. Omdat we in onderhavig onderzoek meer verschillende typen online criminaliteit willen onderscheiden dan in de studie van Tollenaar *et al.* (2019), is de annotatietool uitgebreid. Een screenshot van de aangepaste annotatietool is weergegeven in Bijlage 4. De annoteurs kregen specifieke instructies die ze moesten helpen BVH-registraties van de juiste labels te voorzien (zie Bijlage 5). In de annotatietool gaven de annoteurs per BVH-registratie aan of ze meenden dat de registratie betrekking had op een of meerdere vormen van online criminaliteit. Ze hadden tevens de optie om aan te geven dat ze het niet zeker wisten.

Tabel 4 Intercodeurbetrouwbaarheden (n=500)

	Frequenties		**Overeenstemming tussen annoteurs: ...**			
	Annoteur 1	Annoteur 2	... er is sprake van deze vorm van online criminaliteit	... er is geen sprake van deze vorm van online criminaliteit	Kappa	z[1]
1. Hacking	161	164	85,7%	93,6%	0,90	6,66***
2. Malware	12	10	69,2%	99,2%	0,81	4,80***
3. Ransomware	6	7	85,7%	99,8%	0,92	7,22***
4. DDoS-aanval	3	4	75,0%	99,8%	0,86	5,79***
5. Online bedreiging	35	38	65,9%	97,2%	0,83	5,08***
6. Online stalking	15	9	41,2%	97,8%	0,57	-0,61
7. Online smaad/laster/belediging	17	27	46,7%	96,5%	0,62	0,47
8. Online oplichting	283	284	92,9%	91,6%	0,92	7,19***
8.1 Phishing	78	78	77,3%	95,1%	0,85	5,54***
8.2 Online identiteitsfraude	198	198	86,8%	92,0%	0,90	6,57***
8.3 Online aan- en verkoopfraude	97	91	91,8%	98,0%	0,95	7,90***
8.4 VIN-fraude	33	35	94,3%	99,4%	0,97	8,23***
8.5 Helpdesk-fraude	32	33	80,6%	98,5%	0,89	6,37***
8.6 Overig	0	2	-	-	-	-
9. Money muling	5	3	33,3%	98,8%	0,50	-2,39**

[1] Toetswaarde voor Cohen's kappa > 0,6; ** p<.01; *** p<.001

Het annoteren van de 7.500 BVH-registraties is uitgevoerd door twee onderzoekers. De eerste 500 annotaties zijn door beide annoteurs uitgevoerd waarmee we de interbeoordelaarsbetrouwbaarheid (IBB) konden bepalen. De resultaten van de IBB-test voor de afzonderlijke vormen van online criminaliteit zijn weergegeven in Tabel 4 en de kruistabellen per vorm van online criminaliteit zijn

opgenomen in Bijlage 6. Over het algemeen was er grote overeenstemming tussen de labels van de twee annoteurs (Cohen's kappa rond 0,80 of hoger), maar voor online stalking, online smaad/laster/belediging en *money muling* was de initiële overeenstemming relatief laag.

Naar aanleiding van de resultaten van de IBB-test hebben de annoteurs alle registraties met niet-overeenkomstige labels samen doorgenomen. Op basis van deze inspectie zijn de instructies voor de annoteurs aangescherpt zodat ze bij de resterende annotaties op overeenkomstige wijze labels konden toekennen (zie de overige instructies in Bijlage 5).

Tabel 5 Beschrijvende statistieken geannoteerde steekproef (n=7.500)

	n	%
1. Hacking	2.293	30,6
2. Malware	106	1,4
3. Ransomware	67	0,9
4. DDoS-aanval	41	0,5
Cybercrime	2.333	31,1
5. Online bedreiging	405	5,4
6. Online stalking	135	1,8
7. Online smaad/laster/belediging	291	3,9
8. Online oplichting	4.000	53,3
8.1 Phishing	1.214	16,2
8.2 Online identiteitsfraude	487	6,5
8.3 Online aan- en verkoopfraude	2.685	35,8
8.4 VIN-fraude	507	6,8
8.5 Helpdesk-fraude	1.371	18,3
8.6 Overig online oplichting	32	0,4
9. Money muling	139	1,9
Gedigitaliseerde criminaliteit	4.786	63.8

Tabel 5 laat zien in hoeveel gevallen er in de selectieve steekproef volgens de annoteurs sprake was van de verschillende vormen van online criminaliteit. BVH-registraties konden overigens positief scoren op meerdere vormen van online criminaliteit omdat de verschillende verschijningsvormen van online criminaliteit elkaar niet uitsluiten. Dat is de reden waarom de afzonderlijke aantallen niet optellen tot de aantallen die we zien bij de overkoepelende labels cybercrime en gedigitaliseerde criminaliteit. We hebben voor het label *Cybercrime* de labels Hacking, Malware, Ransomware en DDoS-aanval samengenomen. Voor het label *Gedigitaliseerde criminaliteit* zijn de overige labels samengenomen. In totaal werden in de selectieve steekproef 2.333 (31,1%) registraties van cybercrime vastgesteld en 4.786 (63,8%) registraties van gedigitaliseerde criminaliteit. Relatief veel registraties hadden betrekking op Hacking (n=2.293), Online oplichting (n=4.000), Phishing (n=1.214), Online aan- en verkoopfraude (n=2.685) en Helpdeskfraude (n=1.371), terwijl registraties van Ransomware (n=67), DDoS-aanval (n=41) en Overige online oplichting (n=32) juist erg weinig bleken voor te komen.

Voorbewerking tekstelementen

Voordat we op basis van de teksten uit BVH *machine learning* modellen kunnen ontwikkelen, dienen de ongestructureerde teksten uit de BVH-registraties te worden omgezet in gestructureerde data. Tollenaar *et al.* (2019) hebben laten zien dat *predictive textmining* modellen voor online criminaliteit het best presteerden wanneer gebruik werd gemaakt van het feitelijk woordgebruik (hoe vaak bepaalde woorden in een tekst voorkomen, de zogenaamde lexicografische *features*). Om die reden hebben we per BVH-registratie de afzonderlijke tekstelementen uit de *bevindingen*, *toelichtingen*, *verklaringen* en *MO-teksten* eerst gecombineerd en vervolgens met behulp van het R package `udpipe` (Wijffels, 2022) en het voor Nederlands geschikte taalmodel `dutch-alpino-ud-2.5-191206.udpipe` gelemmatiseerd tot losse woorden zoals ze in het woordenboek voorkomen. We hebben daarbij alle lemma's van maar 1 karakter lang en alle lemma's die door het taalmodel als interpunctie of cijfer waren gelabeld en daarnaast stopwoorden[6] verwijderd, omdat deze niet informatief zijn om BVH-registraties succesvol te kunnen classificeren. De resterende lemma's zijn vervolgens per BVH-registratie weer gecombineerd tot een tekst.

Ontwikkeling predictive textmining modellen

Voor de ontwikkeling van de *predictive textmining* modellen hebben we gebruik gemaakt van het voor *machine learning* in R gangbare `tidymodels` *framework* (Kuhn and Wickham, 2020). Voor zowel de algemene labels cybercrime en gedigitaliseerde criminaliteit als ook elk van de 15 afzonderlijke labels die zijn weergegeven in Tabel 5 zijn aparte LASSO logistische regressiemodellen voor binaire classificatie ontwikkeld. Bij het logistische regressiemodel wordt een lineaire combinatie van predictoren gebruikt om de log-odds te modelleren. De modellen die Tollenaar *et al*. (2019) ontwikkelden lieten een betere *performance* zien wanneer de ruwe tellingen van de lemma's als predictoren werden gebruikt dan wanneer gebruik gemaakt werd van zogenaamde *term frequency - inverse document frequency*. Om die reden is hier gekozen om de frequenties waarin lemma's in een tekst voorkomen te gebruiken als de predictoren. Omdat het aantal verschillende lemma's in een tekst enorm groot kan zijn, is het handig om gebruik te maken van het LASSO algoritme. Dit betreft een zogenaamd regularisatie algoritme dat helpt bij het selecteren van enkel de meest relevante

[6] De volgende stopwoorden zijn verwijderd: aan, al, alles, als, altijd, andere, ben, bij, daar, dan, dat, de, der, deze, die, dit, doch, doen, door, dus, een, eens, en, er, ge, geen, geweest, haar, had, heb, hebben, heeft, hem, het, hier, hij, hoe, hun, iemand, iets, ik, in, is, ja, je, kan, kon, kunnen, maar, me, meer, men, met, mij, mijn, moet, na, naar, niet, niets, nog, nu, of, om, omdat, onder, ons, ook, op, over, reeds, te, tegen, toch, toen, tot, u, uit, uw, van, veel, voor, want, waren, was, wat, werd, wezen, wie, wil, worden, wordt, zal, ze, zelf, zich, zij, zijn, zo, zonder, zou.

predictoren, omdat het de coëfficiënten van de minder relevante predictoren op 0 stelt. Voor het schatten van het model is gebruik gemaakt van de `glmnet` engine.

Voor elk van de in totaal 17 labels (de 2 overkoepelende online criminaliteit labels en de 15 afzonderlijke labels) zijn daartoe de volgende stappen doorlopen:

1. De 7.500 geannoteerde BVH-registraties werden op basis van een naar label gestratificeerde steekproef gesplitst in een training set (n=5.624; 75%) en een test set (n=1.876; 25%).
2. De in de voorbewerking weer tot een tekst samengevoegde lemma's zijn met behulp van het `spacyr` *package* en het `nl_core_news_sm` taalmodel opnieuw opgedeeld in losse woorden. Vervolgens zijn zowel de ruwe tellingen van de losse woorden (unigrammen) als van de combinatie van opeenvolgende woorden (bigrammen) als predictoren gebruikt, waarbij we voor zowel de uni- als bigrammen het maximum aantal predictoren in het model middels *tuning* hebben geoptimaliseerd. Voor de *tuning* is gebruik gemaakt van `max_tokens`: 2.000, 3.000, 4.000 en 5.000.
3. De mate van regularisatie is tevens middels *tuning* geoptimaliseerd. De `penalty` parameter is daartoe in 20 gelijke stappen tussen 0 en 1 gevarieerd.
4. We maakten gebruik van zogenaamde 10-*fold cross-validation*, waarbij de training set willekeurig is opgedeeld in 10 datasets van nagenoeg gelijke grootte.
5. We maakten gebruik van *oversampling* op basis van het *nearest neighbors* SMOTE algoritme, waardoor het aantal gevallen van de *minority class* werd opgehoogd zodat een gebalanceerde dataset ontstaat. Tabel 5 laat immers zien dat er geenszins sprake was van een gebalanceerde dataset, omdat voor het merendeel van de 7.500 cases er geen sprake was van online criminaliteit (online oplichting en het overkoepelende label gedigitaliseerde criminaliteit vormen de uitzondering, want voor die labels is online criminaliteit de *majority class*). Een dermate ongebalanceerde dataset heeft als risico dat een classificatiemodel ogenschijnlijk een goede *performance* kan geven door simpelweg de grootste klasse te voorspellen.
6. Modelselectie op de 10-*fold cross-validated* training set vond plaats op basis van de *area under the receiver operating characteristic curve* (ROC_AUC), gemiddeld over alle *folds*. Deze maat kan worden geïnterpreteerd als de waarschijnlijkheid dat het model een willekeurig positief voorbeeld (wel sprake van online criminaliteit) hoger rangschikt dan een willekeurig negatief voorbeeld (geen sprake van online criminaliteit). Als het model volledig verkeerd zou voorspellen, dan zou de ROC_AUC gelijk zijn aan 0, terwijl een perfect model een ROC_AUC heeft van 1.
7. Voor de modelevaluatie pasten we het op de training set best presterende model toe op de test set, de geannoteerde data die niet gebruikt waren om het model mee te ontwikkelen. Een

goed model moet immers ook voor dit soort nieuwe data een goede *performance* laten zien en voor de test set kunnen we dat evalueren door de voorspelde labels te vergelijken met de werkelijke (geannoteerde) labels. Op basis van het LASSO logistische regressiemodel is daartoe voor elk observatie de kans berekend dat van de specifieke vorm van online criminaliteit sprake is. Deze voorspelde waarde ligt tussen 0 en 1.

8. Om te classificeren moest vervolgens een `drempelwaarde` worden gekozen op deze voorspelde waarde. Voor voorspelde waarden (of kansen) boven deze `drempelwaarde` zou dan sprake moeten zijn van online criminaliteit en voor waarden onder de `drempelwaarde` moet geen sprake zijn van online criminaliteit. Het is van belang te benoemen dat geen enkel model perfect is en zelfs bij de meest optimale `drempelwaarde` zullen classificatiefouten worden gemaakt. Om classificatiefouten te minimaliseren dient de `drempelwaarde` zo gekozen te worden dat het model een goede fit laat zien. We gebruiken daartoe de fitmaat F_1-waarde, het harmonisch gemiddelde van de fitmaten *precision* en *recall*. Deze drie fitmaten kunnen eenvoudig worden toegelicht aan de hand van de zogenaamde *confusion matrix* (zie Tabel 6). Dit betreft een 2x2-tabel waarin de werkelijke (geannoteerde) labels afgezet worden tegen de door het model voorspelde labels.

Tabel 6 Confusion matrix

		Werkelijk (geannoteerd) label	
		0	1
Voorspeld label	0	True negative (TN)	False negative (FN)
	1	False positive (FP)	True positive (TP)

In een *confusion matrix* staan op de diagonaal (paarse cellen) de aantallen juist geclassificeerde gevallen en de waarden die niet op diagonaal liggen (witte cellen) betreffen de aantallen gemaakte classificatiefouten. Een werkelijk negatief geval (0) dat ook als zodanig wordt voorspeld (0) staat daarmee in de linkerbovenhoek (*true negative*). Een werkelijk positief geval (1) dat ook als zodanig wordt voorspeld (1) staat in de rechteronderhoek (*true positive*). Als een werkelijk positief geval (1) echter negatief (0) wordt voorspeld, dan is sprake van een *false negative* en die vinden we in de rechterbovenhoek. Alle werkelijk negatieve gevallen (0) die juist positief worden voorspeld (1) noemen we *false positives* en deze staan in de linkeronderhoek van de *confusion matrix*.

$$Precision = \frac{TP}{TP + FP}$$

Precision is vervolgens een fitmaat die de proportie correct geclassificeerde gevallen berekent voor de voorspelde klasse.

$$Recall = \frac{TP}{TP + FN}$$

Recall is een fitmaat die aangeeft welke proportie van de werkelijk positieve gevallen ook juist geclassificeerd wordt.

In het ideale geval is tegelijkertijd sprake van een hoge *Precision* en een hoge *Recall*, maar er bestaat in de regel een negatieve samenhang tussen beide fitmaten. Dit heeft als nadeel dat het kiezen van een `drempelwaarde` die zorgt voor een hogere *Precision* zorgt voor een lagere *Recall*, en andersom. Omdat onbekend is welke maat dient te prevaleren, gebruikten we daarom de F_1-waarde, het harmonisch gemiddelde van *Precision* en *Recall*. Voor elk model kozen we vervolgens de `drempelwaarde` waarbij we de hoogste F_1-waarde vonden.

$$F_1 = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}$$

9. F_1-waarden liggen tussen 0 en 1 en hoe dichterbij 1, des te beter is de *performance* van het model. Omdat de voorspellingen gebruikt dienden te worden om voor individuele BVH-registraties in- en doorstroomanalyses te doen, dienden we voldoende zeker te zijn van de voorspelling. Om die reden werden alleen in- en doorstroomanalyses gedaan voor vormen van online criminaliteit waarbij het model een F_1-waarde van tenminste 0,80 liet zien.

Tabel 7 Modelselectie op basis van training set

	penalty	max_tokens	ROC_AUC
Cybercrime	0,00483	5.000	0,975
1. Hacking	0,00483	5.000	0,974
2. Malware	0,02069	2.000	0,947
3. Ransomware	0,00785	2.000	0,973
4. DDoS-aanval	0,03360	5.000	0,967
Gedigitaliseerde criminaliteit	0,00483	2.000	0,943
5. Online bedreiging	0,03360	2.000	0,921
6. Online stalking	0,02069	2.000	0,950
7. Online smaad/laster/belediging	0,00785	5.000	0,916
8. Online oplichting	0,00298	3.000	0,973
8.1 Phishing	0,00785	4.000	0,971
8.2 Online identiteitsfraude	0,00483	4.000	0,962
8.3 Online aan- en verkoopfraude	0,00483	5.000	0,986
8.4 VIN-fraude	0,00785	2.000	0,990
8.5 Helpdesk-fraude	0,01274	4.000	0,985
8.6 Overige online oplichting	0,00483	2.000	0,812
9. Money muling	0,01274	5.000	0,947

Tabel 7 presenteert het resultaat van de hierboven beschreven stappen 2 t/m 6. Voor de verschillende vormen van online criminaliteit geeft het de waarden van de *tuning* parameters van het best presterende model op de training set met de bijbehorende gemiddelde ROC_AUC. Vrijwel alle modellen laten een uitzonderlijk goede *performance* zien met ROC_AUC waarden boven 0,9. Alleen de *performance* van het model voor *overige online oplichting* laat een lagere ROC_AUC zien (0,812). Er waren echter ook maar weinig gevallen in de selectieve dataset gelabeld als *overige online oplichting* (slechts 32 van de 7.500) en dus was er ook weinig informatie om een goed model te ontwikkelen. Desondanks is met een ROC_AUC boven 0,80 de *performance* op de training set toch nog erg goed. Bijlage 7 geeft per type online criminaliteit de model *performance* bij verschillende *tuning* waarden. Voor 5 van de 15 vormen van online criminaliteit gebruikt het best presterende model het maximum aantal van 5.000 uni- en bigrammen. Voor al die modellen is de ROC_AUC al dichtbij 1 en een nog hoger maximum had dus weinig toegevoegd.

Omdat bij *machine learning* altijd het risico op *overfitting* bestaat, is het belangrijk om na te gaan hoe de *performance* is op data die niet zijn gebruikt bij het ontwikkelen van de modellen. Tabel 8 geeft daarom het resultaat van de hierboven beschreven stappen 7 t/m 9[7]. Per label geeft Tabel 8 de `drempelwaarde` bij de hoogst mogelijke F_1-waarde, *Precision* en *Recall* voor de evaluatie op de test set. Het is duidelijk dat niet alle modellen geschikt zijn om te gebruiken voor in- en doorstroomanalyses. De modellen voor de grijs gearceerde cellen in Tabel 8 hebben een te lage F_1-waarde (<0,8) en voor die vormen van online criminaliteit zullen in het vervolg van dit hoofdstuk dus geen afzonderlijke in- en doorstroomanalyses worden gepresenteerd. De gemiddelde F_1-waarde voor de vormen van online criminaliteit waarvoor de performance wel goed genoeg was voor verdere analyse ligt op 0,89 (range: 0,84 - 0,93), een zeer goede *performance*.

De modellen voor de weinig frequente vormen van online criminaliteit in de geannoteerde data (zie voor de aantallen Tabel 5) lieten een lagere *performance* zien dan de modellen voor de vormen van online criminaliteit die vaker voorkwamen. Hoewel we hier niet met zekerheid kunnen stellen dat de lage *performance* te wijten is aan de beperkte omvang van het aantal positieve gevallen in de

[7] De bijbehorende *confusion matrices* en *Precision–Recall* grafieken zijn te vinden in Bijlage 8. In de *Precision–Recall* grafieken wordt *Precision* afgezet tegen *Recall* en ze laten goed zien dat een hogere waarde bereikt kan worden op de ene fitmaat, maar dat die vervolgens direct samenhangt met een lagere waarde op de andere fitmaat wanneer de `drempelwaarde` wordt gevarieerd. In de grafieken worden ook banden van verschillende F_1-waarden weergegeven. Zodra de *Precision–Recall* curve rechtsboven een band uitkomt, dan is er een `drempelwaarde` waarbij tenminste de betreffende F_1-waarde wordt bereikt.

geannoteerde data, is het over het algemeen bij de ontwikkeling van dit soort *supervised machine learning* modellen nuttig om over zoveel mogelijk gegevens te beschikken.

Tabel 8 Modelevaluatie op test set

	Drempelwaarde	F_1-waarde	*Precision*	*Recall*
Cybercrime	0,42	0,90	0,88	0,92
1. Hacking	0,51	0,89	0,89	0,90
2. Malware	0,66	0,55	0,43	0,77
3. Ransomware	0,92	0,55	0,56	0,53
4. DDoS-aanval	0,45	0,56	0,45	0,71
Gedigitaliseerde criminaliteit	0,36	0,91	0,92	0,90
5. Online bedreiging	0,57	0,49	0,37	0,72
6. Online stalking	0,75	0,55	0,50	0,62
7. Online smaad/laster/belediging	0,58	0,56	0,46	0,70
8. Online oplichting	0,34	0,93	0,91	0,95
8.1 Phishing	0,65	0,84	0,80	0,88
8.2 Online identiteitsfraude	0,46	0,90	0,89	0,91
8.3 Online aan- en verkoopfraude	0,51	0,91	0,95	0,87
8.4 VIN-fraude	0,62	0,90	0,89	0,90
8.5 Helpdesk-fraude	0,68	0,85	0,89	0,82
8.6 Overige online oplichting	0,41	0,10	0,06	0,18
9. Money muling	0,90	0,47	0,55	0,41

Bijlage 9 geeft voor de modellen die een goede *performance* laten zien een overzicht van de meest predictieve uni-/bigrammen.

Prevalentiecijfers online criminaliteit op basis van classificatiemodellen

Met behulp van de 9 ontwikkelde classificatiemodellen die een hoge *performance* lieten zien op de test set, zijn alle BVH-registraties in de willekeurige steekproef (n=300.000) die voldoende tekstelementen bevatten geclassificeerd. Per registratie is daarmee bepaald of volgens de modellen sprake was van een van de 9 vormen van online criminaliteit. In dit deel presenteren we eerst de analyse van de in- en doorstroom van die vormen van online criminaliteit, waarna we een vergelijking maken met andere vormen van criminaliteit. Deze vergelijking maakt het mogelijk na te gaan in hoeverre de in- en doorstroom van online criminaliteit afwijkend is.

Voor 297.023 unieke BVH-registraties waren 549.820 tekstvelden beschikbaar (63.257 *bevindingen*, 4.565 *MO-teksten*, 384.709 *toelichtingen* en 97.289 *verklaringen*). Gemiddeld bevatte een BVH-registratie daarmee ruim 1,8 tekstveld (mediaan 1), maar dit aantal varieerde tussen de 1 en 1.191. De tekstvelden zelf varieerden in lengte tussen 1 en 239.745 karakters (gemiddeld 1.606; mediaan 986).

Alle tekst is vervolgens gelemmatiseerd en na verwijdering van lemma's van maar 1 karakter lang, alle interpunctie, cijfers en stopwoorden, bleven 296.946 unieke BVH-registraties (99% van de totale steekproef) over die bruikbaar waren om op basis van de ontwikkelde modellen te voorspellen of het een registratie betrof van een of meerdere vormen van online criminaliteit.

Tabel 9 Prevalentie BVH-registraties verschillende vormen van online criminaliteit in willekeurige BVH-steekproef, (n=300.000[1]) en geschatte prevalentie in populatie (N=10.420.594), periode 2018-2020

	Prevalentie (steekproef)	%	Geschatte prevalentie (populatie)	95% - betrouwbaarheidsinterval
Cybercrime	3.133	1,04	109.945	(106.148 - 113.842)
Hacking	2.309	0,77	81.029	(77.769 - 84.389)
Gedigitaliseerde criminaliteit	11.930	3,98	418.654	(411.323 - 426.079)
Online oplichting	9.562	3,19	335.555	(328.969 - 342.237)
Phishing	1.189	0,40	41.725	(39.391 - 44.161)
Online identiteitsfraude	5.293	1,76	185.745	(180.817 - 190.771)
Online aan- en verkoopfraude	4.568	1,52	160.303	(155.722 - 164.983)
VIN-fraude	955	0,32	33.513	(31.424 - 35.704)
Helpdeskfraude	361	0,12	12.668	(11.396 - 14.044)

[1] Voor 3.054 BVH-registraties was er onvoldoende informatie om op basis van de modellen tot voorspellingen te komen.

Tabel 9 presenteert de omvangschattingen op basis van de classificaties waarbij de in Tabel 8 gepresenteerde drempelwaarden zijn gebruikt. Naast het aantal (en percentage) BVH-registraties in de willekeurige steekproef dat volgens de ontwikkelde *predictive textmining* modellen positief scoort op de verschillende vormen van online criminaliteit wordt ook een schatting (en bijbehorend 95%-betrouwbaarheidsinterval) gegeven voor de totale populatie van 10.420.594 BVH-registraties in de jaren 2018-2020.

Omdat eenzelfde BVH-registratie informatie kan bevatten die op verschillende vormen van online criminaliteit wijst en de *machine learning* modellen ze dus ook bij meer vormen kan hebben geclassificeerd, zijn de in Tabel 9 gepresenteerde omvangschattingen in de steekproef niet wederzijds uitsluitend. Dit leidt dus tot dubbeltellingen en daarom sommeren de afzonderlijke vormen die vallen onder gedigitaliseerde criminaliteit ook niet tot het totaal.

Hoewel de omvangschattingen laten zien dat registraties van gedigitaliseerde criminaliteit ongeveer vier keer vaker voorkomen dan registraties van cybercrime, springen met name de lage prevalentiecijfers in het oog. Gedigitaliseerde criminaliteit zien we in 4 procent van de BVH-registraties terug, terwijl cybercrime in slechts 1 procent van de BVH-registraties wordt gevonden. De hoge prevalentie die wordt vastgesteld in slachtofferenquêtes (Akkermans *et al.*, 2022) zien we in BVH-registraties dus niet terug. Van de verschillende vormen van gedigitaliseerde criminaliteit springt

online oplichting er uit, maar ook online identiteitsfraude en online aan- en verkoopfraude scoren relatief hoog. We zien veel minder BVH-registraties van phishing, VIN-fraude en helpdeskfraude.

In- en doorstroom online criminaliteit: Een beschrijvende analyse van aangiften en verdachten

Omdat het BVH-systeem door politiemedewerkers wordt gebruikt voor het registreren van incidenten, meldingen, aangiften en eigen acties, hebben lang niet alle BVH-registraties in de steekproef betrekking op aangiften. Desondanks kunnen registraties waarbij geen sprake is van een aangifte wel degelijk inhoudelijk betrekking hebben op online criminaliteit en de *machine learning* modellen zullen ook die registraties als zodanig geclassificeerd kunnen hebben. Om die reden is de eerste stap van onze analyse het vaststellen van de mate waarin bij de als online criminaliteit geclassificeerde BVH-registraties ook tenminste 1 aangifte was opgenomen.

We presenteren de resultaten van de analyse van de in- en doorstroom van online criminaliteit in de strafrechtketen voor cybercrime en gedigitaliseerde criminaliteit zowel gecombineerd (online criminaliteit) als apart. Dezelfde analyses zijn gedaan voor alle 7 afzonderlijke vormen van online criminaliteit waarbij de *predictive textmining* modellen een goede *performance* lieten zien, maar het voert te ver om deze elk afzonderlijk te bespreken. Bovendien blijken voor sommige vormen van online criminaliteit de aantallen soms erg laag te worden, waardoor de afzonderlijke analyses met grote voorzichtigheid dienen te worden geïnterpreteerd. Enkele opvallende uitkomsten uit die afzonderlijke analyses zullen we hier wel beschrijven, maar voor overige details verwijzen we de geïnteresseerde lezer naar Bijlage 10.

Instroom in de strafrechtketen

Tabel 10 BVH-registraties online criminaliteit in de willekeurige steekproef zonder en met aangifte

	Zonder aangifte		Met tenminste 1 aangifte		Totaal	
Online criminaliteit	3.392	27%	9.406	73%	12.798	100%
Cybercrime	814	26%	2.319	74%	3.133	100%
Gedigitaliseerde criminaliteit	2.891	24%	9.039	76%	11.930	100%

Tabel 10 laat zien hoeveel BVH-registraties online criminaliteit voorkwamen in de grote steekproef (n=300.000). We splitsen de registraties vervolgens uit naar registraties zonder en met een aangifte. In de analyse betreft het registreren van een aangifte de eerste stap van wat we hier als *instroom* typeren. De cijfers voor online criminaliteit combineren alle registraties die positief zijn geclassificeerd op cybercrime en op gedigitaliseerde criminaliteit, in totaal 12.798 registraties (4.3%) van de 300.000

in de willekeurige steekproef. In 73% van de BVH-registraties die als online criminaliteit waren geclassificeerd was ook tenminste 1 aangifte geregistreerd. Blijkbaar wordt er in BVH nog wel vaker over online criminaliteit gerapporteerd, maar in de meeste gevallen betreft het minimaal een aangifte. Uit de cijfers zelf valt niet te achterhalen hoe het komt dat er bij ruim een kwart van de BVH-registraties geen sprake is van een aangifte.

De cijfers die betrekking hebben op cybercrime en gedigitaliseerde criminaliteit zijn gebaseerd op de classificaties op basis van dezelfde drempelwaarden als die gebruikt werden voor de prevalentieschattingen in Tabel 9 en we zien in Tabel 10 dan ook exact dezelfde totalen terug als in die tabel. Belangrijker zijn echter de getallen in de andere kolommen van Tabel 10. Hoewel de aantallen cybercrime veel lager liggen dan die voor gedigitaliseerde criminaliteit zijn de verhoudingen BVH-registraties met en zonder aangifte nagenoeg gelijk; ongeveer een kwart van de registraties bevat geen aangifte.

Doorstroom in de strafrechtketen

Tabel 11 BVH-registraties online criminaliteit in de willekeurige steekproef met tenminste 1 aangifte, zonder en met verdachte

	Zonder verdachte		Met tenminste 1 verdachte		Totaal	
Online criminaliteit	8.486	90%	920	10%	9.406	100%
Cybercrime	2.127	92%	192	8%	2.319	100%
Gedigitaliseerde criminaliteit	8.174	90%	865	10%	9.039	100%

In Tabel 11 worden de BVH-registraties van online criminaliteit waarvoor tenminste 1 aangifte was geregistreerd uitgesplitst naar registraties zonder en met verdachten. In de analyse betreft dit de eerste stap die te typeren valt als *doorstroom.* Wederom springen de lage cijfers in het oog. Voor slechts 10% van de BVH-registraties van online criminaliteit met een aangifte zien we dat er tenminste 1 verdachte was geregistreerd. Het percentage ligt zelfs nog iets lager voor cybercrime (8%). Kijken we vervolgens in Tabel 12 naar dezelfde cijfers voor de 7 afzonderlijke vormen van online criminaliteit, dan zien we dat deze belangrijke eerste stap in de doorstroom behoorlijk varieert tussen de verschillende vormen van online criminaliteit, van respectievelijk slechts 2% en 6% voor online aan- en verkoopfraude en online oplichting tot wel 11% en 18% voor respectievelijk VIN-fraude en helpdeskfraude. Er bestaan kortom flinke verschillen in de mate waarin het lukt om verdachten te koppelen aan de verschillende vormen van online criminaliteit. Wat verder opvalt is dat de 2 vormen van online criminaliteit met de laagste percentages verdachten (aan- en verkoopfraude en online oplichting) goed zijn voor een aanzienlijk deel van de registraties met een aangifte. Het werkaanbod

van de politie voor wat betreft online criminaliteit zal daarmee grotendeels bepaald worden door deze 2 vormen van gedigitaliseerde criminaliteit, maar bij die vormen worden dus relatief weinig verdachten gekoppeld.

Tabel 12 BVH-registraties afzonderlijke vormen van online criminaliteit in de willekeurige steekproef met tenminste 1 aangifte

	Zonder verdachte		Met tenminste 1 verdachte		Totaal	
Online aan- en verkoopfraude	4.036	98%	62	2%	4.098	100%
Online oplichting	7.894	94%	474	6%	8.368	100%
Hacking	1.698	92%	140	8%	1.838	100%
Phishing	1.017	92%	89	8%	1.106	100%
Online identiteitsfraude	3.982	91%	411	9%	4.393	100%
VIN-fraude	767	89%	95	11%	862	100%
Helpdeskfraude	262	82%	57	18%	319	100%

Hoewel we de analyse van in- en doorstroom van online criminaliteit in de strafrechtketen met een grote steekproef van 300.000 BVH-registraties zijn gestart, zorgt het lage percentage BVH-registraties met een aangifte waarbij tenminste een verdachte is geregistreerd ervoor dat de aantallen bij de analyse van de verdere doorstroom in de strafrechtketen soms erg laag worden, zeker voor specifieke vormen van online criminaliteit. Dit noopt tot voorzichtigheid bij het trekken van algemene conclusies over mogelijke verschillen in doorstroomcijfers.

Omdat er bij een BVH-registratie soms meerdere verdachten kunnen worden gekoppeld verschuift in het vervolg van de beschrijvende doorstroomanalyses de eenheid van analyse van afzonderlijke BVH-registraties naar afzonderlijke verdachten.

Tabel 13 Verhouding meerderjarige en minderjarige verdachten online criminaliteit in de willekeurige steekproef

	Meerderjarige verdachten		**Minderjarige verdachten**	
Cybercrime	222	88%	30	12%
Hacking	164	87%	24	13%
Gedigitaliseerde criminaliteit	887	85%	154	15%
Online oplichting	554	91%	54	9%
Phishing	112	89%	14	11%
Online identiteitsfraude	485	92%	42	8%
Online aan- en verkoopfraude	71	88%	10	12%
VIN-fraude	108	92%	9	8%
Helpdeskfraude	64	79%	17	21%

Tabel 13 laat voor de verschillende vormen van online criminaliteit zien wat de verhouding is tussen meerderjarige en minderjarige verdachten. Hoewel we vanwege de kleine aantallen verdachten bij sommige vormen van online criminaliteit voorzichtig moeten zijn met het trekken van al te sterke conclusies, valt op dat het overgrote merendeel van de verdachten van alle afzonderlijke vormen van online criminaliteit meerderjarig is. Voor cybercrime en gedigitaliseerde criminaliteit zijn respectievelijk slechts 12% en 15% van de verdachten minderjarig. Kijken we naar de afzonderlijke vormen, dan valt op dat het aandeel minderjarige verdachten wat hoger is bij helpdeskfraude (21%) en juist wat lager is bij VIN-fraude (8%), online identiteitsfraude (8%) en online oplichting (9%).

Tabel 14 Doorstroom meerderjarige verdachten online criminaliteit in de willekeurige steekproef

		Online		Cybercrime		Gedigitaliseerde criminaliteit	
Politie	Overig / onbekend	246	26%	74	33%	233	26%
	Politiestrafbeschikking / Halt / reprimande	7	1%	4	2%	7	1%
OM	Overig / onbekend	156	17%	31	14%	148	17%
	Sepot	177	19%	49	22%	167	19%
	Strafbeschikking / transactie	54	6%	8	4%	51	6%
Rechtspraak	Dagvaarden	305	32%	56	25%	281	32%
	Totaal	945	100%	222	100%	887	100%

Tabel 15 Doorstroom minderjarige verdachten online criminaliteit in de willekeurige steekproef

		Online		Cybercrime		Gedigitaliseerde criminaliteit	
Politie	Overig / onbekend	12	7%	5	17%	11	7%
	Politiestrafbeschikking / Halt / reprimande	9	6%	0	0%	9	6%
OM	Overig / onbekend	44	27%	11	37%	40	26%
	Sepot	37	23%	3	10%	37	24%
	Strafbeschikking / transactie	4	2%	0	0%	4	3%
Rechtspraak	Dagvaarden	57	35%	11	37%	53	34%
	Totaal	163	100%	30	100%	154	100%

Tabel 14 en Tabel 15 presenteren de doorstroomcijfers voor respectievelijk meerderjarige en minderjarige verdachten. Voor elke verdachte is nagegaan welke afdoening in BOSZ en/of GPS geregistreerd stond. Ongeveer eenderde van de verdachten van online criminaliteit stroomt helemaal door naar de rechtbank (32% van de meerderjarige verdachten en 35% van de minderjarige verdachten wordt gedagvaard). Bij meerderjarige verdachten eindigt het twee keer zo vaak al bij de politie (in totaal 27%) als bij minderjarige verdachten (in totaal 13%), al zien we wel een groter percentage

minderjarige verdachten dat al bij de politie een afdoening krijgt (6% versus 1% bij meerderjarige verdachten). Bij meerderjarige verdachten zien we meer registraties met een overige/onbekende afdoening (bij politie of OM samen 43%) dan bij minderjarige verdachten (34%). Voor meerderjarige verdachten volgt in 19% van de gevallen een sepot, terwijl dit percentage bij minderjarige verdachten op 23% ligt. 6% van de meerderjarige verdachten krijgt een strafbeschikking of transactie, terwijl dat maar bij 2% van de minderjarige verdachten het geval is.

Het algemene beeld van de doorstroom voor meerderjarige verdachten van online criminaliteit wordt gedomineerd door gedigitaliseerde criminaliteit. We zien bij gedigitaliseerde criminaliteit immers dezelfde verhoudingen als voor online criminaliteit. Voor cybercrime stromen iets minder meerderjarige verdachten helemaal door tot de rechtbank (25%) dan bij gedigitaliseerde criminaliteit (32%) en we zien iets meer registraties met een overige of onbekende afdoening bij de politie (33% versus 26% bij gedigitaliseerde criminaliteit). De aantallen minderjarige verdachten van cybercrime in de willekeurige steekproef van 300.000 BVH-registraties zijn te laag (30) om verschillen in de doorstroom te interpreteren.

Het algemene beeld en opvallende verschillen voor specifieke vormen van online criminaliteit

Het algemene beeld van de doorstroom van online criminaliteit zien we in belangrijke mate weerspiegeld in de afzonderlijke analyses in Bijlage 10. Het merendeel van de BVH-registraties bevat ook een aangifte, al valt op dat de percentages voor de afzonderlijke vormen van online criminaliteit hoger liggen dan die we voor de overkoepelende labels in Tabel 10 zagen. Dit is een aanwijzing dat het percentage BVH-registraties zonder aangifte wat hoger ligt voor die vormen van online criminaliteit waarvoor de *predictive textmining* modellen geen goede *performance* lieten zien. Deze vormen waren immers wel opgenomen in de overkoepelende labels. Het percentage meerderjarige verdachten voor wie het al eindigt (vrijwel altijd met overige/onbekende afdoening) bij de politie ligt vaak hoger dan voor minderjarige verdachten. Daarnaast ligt het percentage minderjarige verdachten dat helemaal tot de rechtbank doorstroomt voor vrijwel alle vormen hoger dan dat bij meerderjarige verdachten (met uitzondering van online aan- en verkoopfraude). Voor veel afzonderlijke vormen van online criminaliteit zijn de aantallen (met name minderjarige) verdachten echter zo laag dat we niet teveel belang moeten hechten aan geobserveerde verschillen.

Bij de doorstroomcijfers voor zowel cybercrime als gedigitaliseerde criminaliteit en zowel voor meerderjarige als minderjarige verdachten zien we relatief veel verdachten met een overige of onbekende afdoening (bij politie of OM). Wanneer we kijken we naar de afzonderlijke vormen van online criminaliteit waarvoor tenminste 100 meerderjarige verdachten geregistreerd waren in de willekeurige steekproef (hacking, online oplichting, phishing, online identiteitsfraude en VIN-fraude),

dan zien we dat tussen de 19% (VIN-fraude) en 29% (online identiteitsfraude) van de meerderjarige verdachten helemaal doorstroomt tot de rechtbank. Bij VIN-fraude zien we dat het voor relatief veel meerderjarige verdachten al ophoudt bij de politie (57%), vrijwel altijd met een onbekende of overige afdoening. Hoewel we meerderjarige verdachten van de andere vormen van online criminaliteit vaker zien doorstromen naar het OM, zien we voor de verdachten die niet worden gedagvaard voornamelijk overige/onbekende afdoeningen of sepots.

Vergelijking met andere typen delicten

Waar we in alle voorgaande analyses telkens keken naar de in- en doorstroom van online criminaliteit, is het voor de duiding van de patronen belangrijk om deze te bezien in het licht van hoe andere vormen van criminaliteit in- en doorstromen in de strafrechtketen. Om die reden presenteren we voor drie andere typen delicten exact dezelfde analyses. We gebruikten daarbij het *Gegevensmodel Nationale Politie 2013* om alle BVH-registraties in onze willekeurige steekproef op basis van de maatschappelijke klasse in te delen in a) vermogenscriminaliteit, b) misdrijven gericht tegen de lichamelijke integriteit, en c) fraude delicten (zie Bijlage 11 voor operationaliseringen). Voor een goede vergelijking moesten we overlap met de verschillende vormen van online criminaliteit voorkomen. BVH-registraties die zowel scoorden op online criminaliteit als deze drie andere vormen van criminaliteit hebben we daarom buiten beschouwing gelaten.

Tabel 16 BVH-registraties andere typen delicten in de willekeurige steekproef zonder en met aangifte

	Zonder aangifte		Met tenminste 1 aangifte		Totaal	
Vermogenscriminaliteit	3.631	11%	28.711	89%	32.342	100%
Misdrijven tegen de lichamelijke integriteit	2.536	32%	5.446	68%	7.982	100%
Fraudedelicten	686	51%	665	49%	1.351	100%

Uit Tabel 16 blijkt dat 32.342 BVH-registraties in de willekeurige steekproef vermogenscriminaliteit betreffen, 7.982 misdrijven tegen de lichamelijke integriteit en 1.351 fraudedelicten. Voor de registraties van vermogensdelicten blijkt dat verreweg het merendeel ook een aangifte bevat (89%). Niet alleen ligt de prevalentie van vermogensdelicten dus aanzienlijk hoger dan bij online criminaliteit, maar ook het percentage registraties met aangifte. De instroomcijfers van misdrijven gericht tegen de lichamelijke integriteit (n=7.982) zijn lager dan het aantal BVH-registraties dat als online criminaliteit was geclassificeerd (n=12.798). We zien daarnaast dat 68% van dergelijke BVH-registraties ook een aangifte betreffen, hetgeen eveneens lager is dan we bij online criminaliteit zagen. Kijken we vervolgens naar de instroom van fraudedelicten (n=1.351), dan zien we dat ongeveer de helft van de BVH-registraties ook een aangifte betreft (49%). Dit percentage is aanzienlijk lager dan bij online

criminaliteit. Er zijn dus relatief veel BVH-registraties aangaande fraude zonder dat er een aangifte is gedaan.

Tabel 17 BVH-registraties andere typen delicten in de willekeurige steekproef met tenminste 1 aangifte

	Zonder verdachte		Met tenminste 1 verdachte		Totaal	
Vermogenscriminaliteit	25.326	88%	3.385	12%	28.711	100%
Misdrijven tegen de lichamelijke integriteit	2.232	41%	3.214	59%	5.446	100%
Fraudedelicten	462	69%	203	31%	665	100%

Tabel 17 laat vervolgens zien dat in 12% van alle registraties van vermogensmisdrijven met een aangifte (n=28.711) ook tenminste 1 verdachte is geregistreerd. Dit percentage is maar iets hoger dan wat we zagen bij cybercrime (8%) en gedigitaliseerde criminaliteit (10%). In een ruime meerderheid van alle registraties van misdrijven tegen de lichamelijke integriteit met een aangifte (n=5.446) blijkt sprake te zijn van tenminste 1 verdachte (59%). Dit percentage registraties met tenminste 1 verdachte ligt veel hoger dan wat we bij online criminaliteit zagen. Vaak zal er bij deze delicten sprake zijn geweest van direct contact tussen dader en slachtoffer, waardoor er daderindicatie zal zijn. Het percentage van alle registraties van fraudedelicten met een aangifte (n=665) waarbij tenminste 1 verdachte is geregistreerd (Tabel 17) ligt met 31% niet alleen veel hoger dan bij cybercrime en gedigitaliseerde criminaliteit in het algemeen, maar ook veel hoger dan bij online aan- en verkoopfraude (2%), online identiteitsfraude (9%) en VIN-fraude (11%) (zie Tabel 12). Kortom, bij online fraudedelicten lukt het veel minder vaak om een verdachte te koppelen dan bij andere fraudedelicten.

Tabel 18 Doorstroom meerderjarige verdachten andere typen delicten in de willekeurige steekproef

		Vermogens-criminaliteit		Misdrijven tegen de lichamelijke integriteit		Fraudedelicten	
Politie	Overig / onbekend	166	4%	215	6%	35	15%
	Politiestrafbeschikking / Halt / reprimande	21	1%	8	0%	0	0%
OM	Overig / onbekend	531	14%	593	18%	39	17%
	Sepot	522	14%	797	24%	47	21%
	Strafbeschikking / transactie	451	12%	216	6%	8	4%
Rechtspraak	Dagvaarden	2.045	55%	1.528	46%	98	43%
	Totaal	3.736	100%	3.357	100%	227	100%

De doorstroom van meerderjarige en minderjarige verdachten van vermogenscriminaliteit, misdrijven tegen de lichamelijke integriteit en fraudedelicten wordt in respectievelijk Tabel 18 en Tabel 19

gepresenteerd. De verhouding tussen meerderjarige verdachten (87%) en minderjarige verdachten (13%) van vermogensdelicten is overeenkomstig aan die bij online criminaliteit. Met 86% meerderjarige en 14% minderjarige verdachten geldt hetzelfde voor misdrijven tegen de lichamelijke integriteit. Bij fraudedelicten zien we echter relatief veel meerderjarige verdachten (92%) en dus maar weinig minderjarige verdachten (8%).

Tabel 18 laat de doorstroom zien van meerderjarige verdachten van vermogenscriminaliteit, misdrijven tegen de lichamelijke integriteit en fraudedelicten. Voor vermogenscriminaliteit valt met name de hoge doorstroom tot de rechtbank op (55% wordt gedagvaard). Deze doorstroom tot aan de rechtbank ligt aanzienlijk hoger dan voor online criminaliteit. Hetzelfde geldt voor misdrijven gericht tegen de lichamelijke integriteit en fraudedelicten; ook daar zien we meer meerderjarige verdachten helemaal doorstromen naar de rechtbank (respectievelijk 46% en 43%) dan wat we zagen bij cybercrime (25%) en gedigitaliseerde criminaliteit (32%). De percentages meerderjarige verdachten met een overige of onbekende afdoening (bij politie of OM) liggen voor deze vormen van criminaliteit lager dan bij online criminaliteit; bij vermogensdelicten telt het op tot 18%, bij misdrijven tegen de lichamelijke integriteit tot 24% en bij fraudedelicten tot 32%, terwijl het bij online criminaliteit om 43% ging.

Tabel 19 Doorstroom minderjarige verdachten andere typen delicten in de willekeurige steekproef

		Vermogens-criminaliteit		Misdrijven tegen de lichamelijke integriteit		Fraudedelicten	
Politie	Overig / onbekend	20	4%	21	4%	2	10%
	Politiestrafbeschikking / Halt / reprimande	117	21%	29	5%	0	0%
OM	Overig / onbekend	138	25%	120	22%	6	29%
	Sepot	76	14%	150	27%	10	48%
	Strafbeschikking / transactie	35	6%	44	8%	1	5%
Rechtspraak	Dagvaarden	162	30%	188	34%	2	10%
	Totaal	548	100%	552	100%	21	100%

Voor minderjarige verdachten van vermogenscriminaliteit zien we in Tabel 19 veel meer afdoeningen bij de politie dan wat we zagen bij online criminaliteit, terwijl net iets minder minderjarige verdachten van vermogenscriminaliteit helemaal doorstromen tot de rechtbank (30% wordt gedagvaard tegen 35% bij online criminaliteit). Het aandeel minderjarige verdachten van vermogenscriminaliteit voor wie bij het OM een sepot of overige/onbekende afdoening geregistreerd staat (in totaal 39%) is daarmee net als bij meerderjarige verdachten kleiner dan bij online criminaliteit. Voor minderjarige verdachten van misdrijven gericht tegen de lichamelijke integriteit zijn de doorstroompercentages juist erg

overeenkomstig aan die van online criminaliteit. Het grote verschil tussen misdrijven gericht tegen de lichamelijke integriteit en online criminaliteit zien we dus bij het kunnen identificeren van verdachten; dit gebeurt veel minder vaak bij online criminaliteit. Het aantal minderjarige verdachten van fraudedelicten in de steekproef is te laag om zinnige uitspraken te doen over de verdere doorstroom in de strafrechtketen.

Resumé

In dit hoofdstuk zijn de in- en doorstroom van online criminaliteit in de strafrechtketen voor de jaren 2018-2020 geanalyseerd. Daartoe zijn BVH-registraties van de politie uit die periode als startpunt genomen. In het BVH-systeem registreert de politie incidenten, meldingen en aangiften en de aan de incidenten gekoppelde acties zoals processen-verbaal van verhoor van getuigen of verdachten. Omdat de verschillende vormen van online criminaliteit niet systematisch in de BVH-registraties kunnen worden geïdentificeerd aan de hand van bijvoorbeeld unieke maatschappelijke klassen, zijn *predictive textmining* modellen ontwikkeld die gebruikmaken van alle bij een BVH-registratie behorende registraties van *bevindingen*, *toelichtingen*, *verklaringen* en *MO-teksten.* Er zijn afzonderlijke modellen ontwikkeld om negen verschillende typen online criminaliteit te onderscheiden: vier vormen van cybercrime (hacking, malware, ransomware en DDoS-aanval) en vijf vormen van gedigitaliseerde criminaliteit (online bedreiging, online stalking, online smaad/laster/belediging, online oplichting en *money muling*), waarbij we online oplichting nog uitsplitsen naar phishing, online identiteitsfraude, online aan- en verkoopfraude, VIN-fraude, helpdeskfraude en overige online oplichting. De *predictive textmining* modellen hadden niet voor alle vormen van online criminaliteit een voldoende goede *performance* om ermee de afzonderlijke vormen van online criminaliteit in BVH-registraties te identificeren. Voor de algemene labels cybercrime en gedigitaliseerde criminaliteit als ook voor de afzonderlijke labels hacking, online oplichting, phishing, online identiteitsfraude, online aan- en verkoopfraude, VIN-fraude en helpdeskfraude was de *performance* goed en voor die vormen konden daarmee beschrijvende analyses van de in- en doorstroom in de strafrechtketen worden gepresenteerd.

Door de modellen met een goede *performance* toe te passen op een grote steekproef (n=300.000) van BVH-registraties kon de in- en doorstroom van online criminaliteit in de periode 2018-2020 worden bestudeerd. BVH-registraties met een aangifte vormen een duidelijk startpunt van de strafrechtketen en BVH-registraties die geclassificeerd zijn als online criminaliteit en waarbij tenminste 1 aangifte is geregistreerd markeren dan ook wat we in dit hoofdstuk de *instroom* van online criminaliteit in de strafrechtketen hebben genoemd. Voor alle BVH-registraties van online criminaliteit waarbij tenminste 1 aangifte was geregistreerd, is nagegaan in hoeverre er ook verdachten aan waren gekoppeld en door de BVH-registraties te koppelen aan gegevens uit het systeem Betere Opsporing door Sturing op Zaken

(BOSZ) kon per geregistreerde verdachte worden nagegaan of deze al vroeg in de strafrechtketen een afdoening kreeg (reprimande, politiestrafbeschikking, HALT) of door de politie werd ingezonden naar het OM. Voor het vaststellen van de doorstroom richting OM en rechtspraak zijn de registraties vervolgens gekoppeld aan gegevens ontleend aan het Geïntegreerd Processysteem Strafrecht (GPS). Op basis van de GPS-gegevens konden we per verdachte vaststellen of deze bij het OM een afdoening kreeg (strafbeschikking of transactie) of dat de verdachte werd gedagvaard en voor de rechter moest verschijnen.

De belangrijkste bevinding uit de kwantitatieve analyse van in- en doorstroom van online criminaliteit in de strafrechtketen is gelegen in de lage aantallen. We startten de analyse met een relatief grote steekproef van BVH-registraties (n=300.000) om vervolgens vast te stellen dat de meeste vormen van online criminaliteit in minder dan 1% (met maximum van 4% voor alle gedigitaliseerde criminaliteit tezamen) van de registraties voorkwam. Van de hoge prevalentie die wordt vastgesteld in slachtofferenquêtes (Akkermans *et al.*, 2022) zien we in BVH-registraties dus maar weinig terug. Vervolgens bleek in ongeveer 25% van de registraties geen sprake te zijn van een aangifte en van alle registraties met een aangifte werd maar in ongeveer 10% van de gevallen ook een verdachte gekoppeld. De belangrijkste conclusie moet dan ook luiden: we vinden zelfs met de toepassing van geavanceerde *predictive textmining* modellen maar weinig registraties van online criminaliteit in de strafrechtketen. De instroom in de vorm van aangiften is al niet groot, maar omdat er maar in ongeveer 10% van de gevallen en verdachte wordt gekoppeld, is de doorstroom nog veel geringer.

Verder laten de resultaten van de grootschalige kwantitatieve analyses zien dat BVH-registraties die als gedigitaliseerde criminaliteit zijn geclassificeerd aanzienlijk meer voorkomen dan registraties van cybercrime. De 25% van de BVH-registraties die geclassificeerd zijn als cybercrime of gedigitaliseerde criminaliteit waarbij geen sprake was van een aangifte wijst erop dat er in het BVH-systeem ook best vaak mutaties over online criminaliteit worden gemaakt zonder dat er sprake is van een aangifte. Wanneer we deze cijfers echter vergelijken met die voor andere vormen van criminaliteit, dan valt op dat dit helemaal niet uniek is voor online criminaliteit. Bij misdrijven tegen de lichamelijke integriteit (32%) en fraudedelicten (51%) liggen de percentages zelfs nog aanzienlijk hoger, terwijl het percentage bij vermogensdelicten (11%) juist lager is. Het maken van een BVH-mutatie zonder een aangifte op te nemen lijkt dus niet uniek voor online criminaliteit.

Het lage percentage BVH-registraties van online criminaliteit met een aangifte waarbij ook tenminste 1 verdachte staat geregistreerd (8% voor cybercrime en 10% voor gedigitaliseerde criminaliteit) blijkt flink te variëren tussen afzonderlijke vormen van online criminaliteit, van slechts 2% bij online aan- en

verkoopfraude tot 18% bij helpdeskfraude. Daarbij blijkt bovendien dat bij de vormen van online criminaliteit die relatief veel voorkomen juist relatief weinig verdachten worden geregistreerd.

88% van de verdachten van cybercrime en 85% van de verdachten van gedigitaliseerde criminaliteit was meerderjarig, al valt op dat het aandeel minderjarige verdachten wat hoger is bij helpdeskfraude (21%) en juist wat lager bij VIN-fraude (8%), online identiteitsfraude (8%) en online oplichting (9%).

Voor een aanzienlijk deel van de meerderjarige verdachten van online criminaliteit zien we een overige of onbekende afdoening geregistreerd staan bij politie of OM (samen goed voor 43%), terwijl dit bij minderjarige verdachten ook maar in mindere mate voorkomt (33%). Het percentage verdachten van online criminaliteit die helemaal doorstromen naar de rechtbank verschilt weinig tussen meerderjarige en minderjarige verdachten, en ligt rond eenderde. Minderjarige verdachten krijgen vaker een afdoening bij de politie (6%) dan meerderjarigen verdachten (1%).

Om de in- en doorstroom van online criminaliteit in perspectief te plaatsen, zijn dezelfde analyses gedaan voor drie andere vormen van criminaliteit, te weten *vermogenscriminaliteit*, *misdrijven gericht tegen de lichamelijke integriteit*, en *fraudedelicten*. We zien aanzienlijk meer BVH-registraties van vermogenscriminaliteit dan van online criminaliteit. De aantallen voor misdrijven gericht tegen de lichamelijke integriteit liggen juist net iets lager en voor fraudedelicten zien we nog veel minder registraties. Het percentage BVH-registraties waarbij ook tenminste 1 aangifte was geregistreerd lag hoger bij vermogenscriminaliteit dan bij online criminaliteit, maar bij de andere vormen van criminaliteit lag het juist lager. Bij vermogenscriminaliteit zien we ongeveer even vaak een verdachte geregistreerd staan (in 12% van de gevallen) als bij online criminaliteit (10%). Bij fraudedelicten ligt het percentage BVH-registraties met aangifte waarbij tenminste 1 verdachte is geregistreerd aanzienlijk hoger (31%), terwijl dit bij misdrijven gericht tegen de lichamelijke integriteit nog veel hoger (59%) ligt. De ophelderingspercentages liggen bij deze laatste twee vormen van criminaliteit dus aanzienlijk hoger dan bij online criminaliteit en vermogenscriminaliteit. Voor misdrijven tegen de lichamelijke integriteit is dit niet zo verwonderlijk, aangezien dader en slachtoffer vrijwel altijd direct met elkaar in contact zullen zijn geweest en er dan ook vaak sprake is van daderindicatie, terwijl bij online criminaliteit en vermogenscriminaliteit de verdachte vaak niet direct in beeld zal zijn. Dit verklaart echter niet het verschil in ophelderingspercentages bij online en offline fraudedelicten.

Zodra er een verdachte in beeld is, zien we ook bij vermogenscriminaliteit en misdrijven tegen de lichamelijke integriteit dat minderjarige verdachten vaker een afdoening bij de politie krijgen dan meerderjarige verdachten. Verder valt op dat een hoog percentage meerderjarige verdachten van vermogenscriminaliteit helemaal doorstroomt tot de rechtbank (55%). Ook bij misdrijven tegen de

lichamelijke integriteit (46%) en fraudedelicten (43%) ligt dit percentage aanzienlijk hoger dan bij online criminaliteit (32%).

5. Knelpunten volgens de literatuur en volgens actoren binnen de strafrechtketen

Inleiding

In dit hoofdstuk staan de knelpunten binnen de in- en doorstroom van online criminaliteit in de strafrechtketen centraal. We putten daarvoor uit zowel de literatuur als de interviews met respondenten die werkzaam zijn binnen de strafrechtketen in Nederland. Omdat deze interviews plaatsvonden voordat de resultaten uit de kwantitatieve analyses beschikbaar waren, kunnen geen directe links worden gelegd tussen de in- en doorstroomcijfers uit het vorige hoofdstuk en de door de respondenten genoemde knelpunten.

In totaal interviewden we 34 actoren binnen de strafrechtketen in Nederland, waarvan 26 werkzaam waren bij de politie (P1 t/m P26), 6 bij het OM (OM1 t/m OM6) en 2 bij de zittende magistratuur (R1 en R2). Verder interviewden we 5 internationale experts en bediscussieerden we de resultaten van de literatuurstudie, kwantitatieve analyses en interviews zijn met vijf experts van binnen en buiten politie/justitie (zie hoofdstuk 2 voor een uitgebreidere beschrijving van de gebruikte methoden).

We beschrijven de knelpunten per stap in het proces van in- en doorstroom (zie hoofdstuk 3 en 4). We beschrijven steeds eerst wat we weten uit de literatuur waarna de resultaten uit de interviews volgen. Het hoofdstuk eindigt met een resumé waar we de belangrijkste bevindingen samenvatten. In dit resumé voegen we ook de reflecties van internationale experts toe.

Intake

Literatuur

Uit de literatuur blijkt dat de politie niet altijd een aangifte opneemt wanneer slachtoffers van online criminaliteit contact opnemen met de politie (Toutenhoofd-Visser *et al.*, 2009; Leukfeldt *et al.*, 2012; Domenie *et al.*, 2013; Yar & Steinmetz, 2019; Button *et al.*, 2020; De Paoli *et al.*, 2020). Zo lieten Domenie *et al.* (2013) zien dat bij online delicten gericht op het geld van het slachtoffer, de politie in 56,9% van de gevallen daadwerkelijk een aangifte opnam. In 17,2% van de gevallen werd een melding opgenomen of advies gegeven en in 25,9% van de gevallen volgde geen strafrechtelijke actie. Bij online delicten gericht op de persoon of privésfeer van het slachtoffer lag het percentage opgenomen aangiften met 28,6% een stuk lager. Hier werd in 52,4% van de gevallen een melding opgenomen of advies gegeven en in 19% van de gevallen geen strafrechtelijke actie ondernomen. In sommige gevallen wordt een aangifte ten onrechte niet opgenomen door de politie (Toutenhoofd-Visser *et al.*,

2009; Leukfeldt *et al.*, 2012; Button *et al.*, 2020). Zo laten Button *et al.* (2020) bijvoorbeeld zien dat in het Verenigd Koninkrijk sommige hacking slachtoffers door intakemedewerkers van de politie onterecht wordt geadviseerd dat de gebeurtenissen geen criminaliteit betreffen. Ook in Nederland werden slachtoffers van online fraude soms ten onrechte weggestuurd met de mededeling dat het een civiele zaak betrof in plaats van een strafrechtelijke aangelegenheid (Toutenhoofd-Visser *et al.*, 2009; Leukfeldt *et al.*, 2012). Het succesvol opnemen van een aangifte van online criminaliteit is afhankelijk van het begrip en de kennis van de intakemedewerker (Toutenhoofd-Visser *et al.*, 2009; De Paoli *et al.*, 2020). Deze kennis is echter niet altijd (voldoende) aanwezig bij intakemedewerkers (Leukfeldt *et al.*, 2012; Boekhoorn, 2019). Ook wordt gesuggereerd dat de ernst van online criminaliteit als laag wordt geïnterpreteerd door politiemedewerkers en aangiften daardoor niet altijd worden opgenomen (Yar & Steinmetz, 2019). In lijn met deze bevindingen laat de studie van Van de Weijer *et al.* (2020) zien dat bijna de helft van de slachtoffers (erg) ontevreden is over de wijze waarop de politie hun aangifte online criminaliteit behandelde, omdat de politie onverschillig reageerde of omdat het probleem niet was opgelost.

Interviews

De kwaliteit van de aangifte

Respondenten geven aan dat met name een kwalitatief hoogstaande aangifte voor een succesvolle doorstroom in de strafrechtketen zorgt. Hiervan is volgens een deel van de respondenten (n=13) echter niet altijd sprake. Zij wijzen dit niet toe aan het feit dat steeds meer aangiften via het internet worden gedaan. Het geautomatiseerde aangifteproces via de website van de politie maakt het volgens P12 juist mogelijk om goed door te vragen op onderzoeksmogelijkheden (waaronder bankrekeningnummers). Wel wordt een gebrek aan kennis van online criminaliteit onder intakemedewerkers als knelpunt genoemd, hetgeen juist van belang is wanneer aangiften in persoon worden opgenomen. Een oorzaak die wordt genoemd is dat over het algemeen de "*laag betaalde en slecht opgeleide medewerker*" als intakemedewerker aan de balie wordt gezet (P1, P10, P21) en dat intakemedewerkers die het goed doen vaak snel doorstromen naar andere functies (P21). Een uitspraak van P10 geeft dit goed weer:

> *"Ik moet het doen met medewerkers op [niveau x] [schaal x]. Die zitten mij met grote vraagtekens aan te kijken. Zij kunnen amper een mobiele telefoon bedienen, laat ik het zo zeggen. Die vragen je nog om een app op hun telefoon te installeren. En die nemen dan een aangifte cybercrime op, dat gaan we dus niet doen. Die aangiftes haal ik altijd bij hen weg. Die ga ik zelf opnemen. Ik vind het namelijk ook niet leuk voor die andere partij, als er iemand*

tegenover je komt zitten die geen verstand van zaken heeft. Dat is onzin, je moet hen daar niet mee belasten."

Het is volgens zes respondenten belangrijk om bij het opnemen van een aangifte de juiste vragen te stellen, zodat de aangifte opsporing-technisch iets waard is. Noodzakelijke kennis heeft allereerst te maken met technische details, zoals hoe een IP-adres genoteerd dient te worden. *"Als de puntjes worden weggelaten, wat wel eens gebeurt, dan is de zaak mogelijk al uitgescreend*[8] *voordat de aangever opnieuw kan worden gebeld"*, zo stelt P1. In de tweede plaats is kennis van de modus operandi belangrijk. Hiervan geeft P5 een voorbeeld:

> *"Bij een betaling via iDeal gaat het geld altijd eerst naar een tussenrekening. Dat is bij veel I&S-medewerkers niet bekend, met als gevolg dat vaak de tussenrekening in de aangifte is opgenomen, waar niets op kan worden gevorderd. Dit is namelijk de rekening van een bank of Payment-serviceprovider en niet van een bedrijf of particulier. Het kost veel tijd om hier achteraan te gaan en moet dus aan de voorkant goed worden uitgevraagd."*[9]

Online criminaliteit vraagt volgens respondenten bij uitstek om bijscholing en kennis van actuele gebeurtenissen vanwege de snelheid waarmee deze criminaliteitsvorm verandert (P6, P13). Momenteel komt het voor dat aangevers met '*pakken bewijsmateriaal naar buiten worden gestuurd*' omdat intakemedewerkers niet goed weten wat ze er mee moeten (P6). Respondenten zijn van mening dat het gedurende het hele opsporingsproces zijn vruchten zal afwerpen als er meer wordt geïnvesteerd in de kwaliteit aan de voorkant van het proces. Er zijn wel hulpmiddelen beschikbaar waarmee intakemedewerkers op basis van de criminaliteitsvorm kunnen opzoeken welke informatie uitgevraagd dient te worden, maar daarvoor is vereist dat medewerkers deze hulpmiddelen weten te vinden en dat zij weten op welke criminaliteitsvorm de casus betrekking heeft.

Een niet eerder in de literatuur genoemd knelpunt is volgens respondenten dat de kwaliteit van de aangifte ook afhankelijk is van (de kennis van) de aangever. Zo benoemt P7 dat het 'verhaal' van de aangever lang niet altijd helder is en zo kan worden ingevoerd. Er zijn volgens deze respondent ook burgers die zelf niet precies weten wat er is gebeurd of hoe het heeft kunnen gebeuren. Des te belangrijker is het voor intakemedewerkers om de juiste vragen te stellen. Indien belangrijke informatie ontbreekt levert dit onvoldoende aanknopingspunten en daarmee opsporingsindicatie op

[8] Als een aangifte/melding wordt ingescreend, wordt een onderzoeksdossier van het misdrijf aangemaakt. Als een aangifte/melding wordt uitgescreend, wordt deze afgewezen.

[9] De beschrijving van dit proces is een letterlijke weergave van het antwoord van de respondent. Voor de goede orde melden we hier dat het proces van betalen via iDeal door de tijd heen kan veranderen. Op iDEAL | Online betalen via uw eigen bank staat informatie meer informatie over deze manier van betalen.

(zie de volgende paragraaf over 'screening'). P22 beschrijft wat volgens hem de oorzaak is van de gebrekkige kennis onder aangevers:

> *"Vooral met AnyDesk [de respondent heeft het hier over de fraudevariant bankhelpdeskfraude] en zo, dan beginnen ze te vertellen: 'ik word gebeld', ze weten de naam vaak nog en dan ineens blokkeren ze, dan is het gewoon klaar. Daarbij komt dat die mensen emotioneel niet helemaal stabiel zijn, die schamen zich dood dat het hun overkomen is. Ik had er gisteren ook weer een die zei van 'ik snap er niks van, ik word overal gewaarschuwd en ik was hartstikke wantrouwend, maar toch heb ik het gedaan.'" (P22)*

Zoals eerder benoemd, zou een ander knelpunt voor de instroom van online criminaliteitszaken kunnen zijn dat van online criminaliteit niet altijd aangifte wordt opgenomen. Hoewel dit in de interviews niet vaak werd genoemd, gaf een van de respondenten hiervan wel een concreet voorbeeld. P22 kiest er in het geval van *sextortion*, hetgeen verwijst naar afpersing met seksueel getint beeldmateriaal, in de regel voor om geen aangifte op te nemen en daarmee niet te vragen om een opsporingsonderzoek op te starten. De reden die hij hiervoor noemt is dat de opsporingskansen bij deze criminaliteitsvorm volgens hem erg laag zijn. Dit blijkt uit het volgende citaat:

> *"Als je vooraf al weet dat een aangifte niets gaat opleveren dan is het beter om alleen een mutatie in het systeem te zetten. […] Ik maak een mutatie op en geef ze [slachtoffers] handvaten waar ze naar toe kunnen. Er zijn genoeg sites waar men daar dan over kan praten. Ook zou een stopgesprek met de verdachte kunnen worden gehouden. Vaak is dat wel voldoende. Natuurlijk heb je uitzonderingen, maar de ervaring leert wel dat dat meer oplevert dan een aangifte."*

Casescreening

Literatuur

Enkele onderzoeken geven inzicht in knelpunten die bestaan rondom de casescreening van (traditionele) zaken. Zo liet de Algemene Rekenkamer in 2012 zien dat zaken uit werden gescreend ondanks dat deze volgens de *Aanwijzing voor de opsporing* opvolging zouden moeten krijgen. Dit was met name het geval bij veelvoorkomende criminaliteit (VVC). Oorzaken hiervoor werden later door Felix (2013) geïdentificeerd. Zo bleek bijvoorbeeld dat de *Aanwijzing voor de opsporing* onvoldoende rekening houdt met de beschikbare capaciteit en met het strafrecht als ultimum remedium. Ook zouden er grote verschillen zijn in de ervaring van casescreeners en het screeningsproces was niet eenduidig georganiseerd. Inmiddels is er een vernieuwde *Aanwijzing voor de opsporing* (geldig vanaf 2014), waarin een deel van deze problemen is geadresseerd. Een rapport van de Inspectie Justitie en Veiligheid (2019a) over de selectie en toewijzing in de opsporing geeft inzicht in meer recente

knelpunten. Ten aanzien van de selectie wordt onder andere benoemd dat er door capaciteitsoverwegingen relevante en/of kansrijke zaken afvallen (die complexer/arbeidsintensiever zijn of minder impact hebben), dat sommige zaken onnodig lang of intensief worden behandeld en dat de politie onvoldoende zicht heeft op zaken die niet worden geselecteerd, vroegtijdig worden beëindigd of stil komen te liggen. Ook wordt de rol van de casescreener soms uitgevoerd door medewerkers die ook andere rollen vervullen en mede daardoor niet alle richtlijnen (zoals de *Aanwijzing voor de opsporing*) goed kennen. Ten aanzien van de sturing blijkt dat door capaciteitsoverwegingen zaken worden toegewezen aan onderdelen op een te laag niveau – en ook aan individuele medewerkers – die niet altijd de expertise of gelegenheid hebben om de zaken op te pakken.

Er is relatief weinig onderzoek dat zich richt op de casescreening van zaken online criminaliteit door de politie. In 2012 gaven Leukfeldt *et al.* in een onderzoek naar de strafrechtelijke afhandeling van online criminaliteit meer inzicht in deze fase. Uit het onderzoek bleek dat online criminaliteitszaken minder snel opgepakt werden dan traditionele zaken. Verklaringen hiervoor waren dat de afhandeling van dergelijke zaken veel tijd kost, terwijl er weinig capaciteit voorhanden is. Daarnaast vraagt het (inter)nationale karakter van online criminaliteit niet zelden om samenwerking tussen eenheden of met politiediensten uit andere landen. Verder werd geconstateerd dat er tijdens de intake- en casescreening een gebrek aan kennis was over het opnemen van een aangifte online criminaliteit, waardoor de kwaliteit van opgenomen aangiften onvoldoende is. Zo bleek dat het verrijken van aangiften online criminaliteit als lastiger werd ervaren door politiemedewerkers dan de verrijking van reguliere zaken (Leukfeldt *et al.*, 2012). Dit kwam enerzijds door het gebrek aan kennis en ervaring met de afhandeling van aangiften online criminaliteit en anderzijds door de afhankelijkheid van derden voor het verzamelen van bewijs. Zo dienden IP-adressen en bankrekeningnummers vaak opgevraagd te worden bij internetserviceproviders en banken, wat meer inspanningen en ervaring vereist. Een ander knelpunt tijdens de casescreening was het gebrek aan zicht vanuit het OM op de uitstroom van zaken online criminaliteit, terwijl het OM hier destijds volgens de *Aanwijzing voor de opsporing* formeel bij betrokken diende te zijn. Een recenter onderzoek van Boekhoorn (2019) laat zien dat soortgelijke problemen rondom de intake en casescreening nog niet zijn opgelost. Zo blijkt dat onbekendheid met online criminaliteit bij intake- en servicemedewerkers – ondanks voorlichting en beschikbare tools – nog steeds als een knelpunt wordt ervaren door betrokken politiemedewerkers. De resulterende lage kwaliteit van aangiften heeft tot gevolg dat belangrijke informatie in de aangifte ontbreekt en tijdens de casescreening bepaalde zaken al niet in behandeling worden genomen (Boekhoorn, 2019).

Interviews

In hoofdstuk 3 kwam aan bod dat er verschillende redenen zijn om een zaak al dan niet in te screenen. Binnen sommige eenheden zijn hierover afspraken gemaakt met het OM, maar uit de interviews blijkt dat wat dit betreft aanzienlijke verschillen bestaan tussen eenheden, districten en basisteams. In deze paragraaf wordt aandacht besteed aan de meest genoemde redenen waarom aangiften binnen het screeningsproces uitvallen. Het gaat daarbij in de regel specifiek om de casescreening van online criminaliteit. In het geval dat deze volgens de respondenten tevens van toepassing is op traditionele criminaliteitsvormen wordt dit erbij vermeld.

Onvoldoende opsporingsindicatie

Een gebrek aan opsporingsindicatie vormt veruit de meest genoemde reden van respondenten (n=16) om een zaak niet op te pakken. Hiermee wordt bedoeld dat er gedurende het screenen nog geen dader in beeld is. Voor voldoende opsporingsindicatie is bepalend welke informatie de aangifte bevat die te koppelen is aan de identiteit van de verdachte(n), beschikbaar is en veilig gesteld kan worden (P14, P21) en met welke snelheid deze informatie gevorderd en verkregen kan worden (P10). Te denken valt aan camerabeelden, bankrekening- of telefoonnummers, logbestanden uit computers en telefoons. Dat een gebrek aan opsporingsindicatie een reden kan vormen om een zaak niet op te pakken, komt overeen met hetgeen gevonden werd in de literatuur. De casescreening vindt plaats op basis van de *Aanwijzing voor de opsporing* van het OM, welke onder meer voorschrijft dat delicten zonder opsporingsindicatie niet voor opsporing in aanmerking komen.

Hoewel dit bij traditionele delicten ook een rol kan spelen, zijn respondenten van mening dat dit met name bij online criminaliteit een probleem is. Allereerst omdat internet veel afschermmogelijkheden biedt waardoor het moeilijker is om een verdachte in beeld te krijgen. Voorbeelden die worden genoemd, zijn de mogelijkheid tot encryptie (een vorm van gegevens-beveiliging, bijvoorbeeld middels een *Virtual Private Network* (VPN)) (P15), *sim-swapping*, ofwel het switchen van simkaarten (P10), *spoofing* (waarbij daders via internet – en dus niet via een zendmast – bellen of sms-en met een willekeurig telefoonnummer zoals dat van een bank) (P16) of het gebruik van een IP-adres dat duizenden mensen per dag benutten, denk aan het IP-adres van een restaurant of universiteit (P10). Ook is het mogelijk het geldspoor zodanig te verhullen dat er weinig tot geen zicht op een verdachte is. P5 legt uit dat daders van online criminaliteit van de illegaal verkregen opbrengsten vaak tegoedkaarten kopen en online verhandelen. De besteding van de tegoedkaart is vaak niet naar de daadwerkelijke dader(s) herleidbaar, met als gevolg dat een dergelijke zaak niet wordt opgepakt.

Ten tweede geven vier respondenten aan dat het bij online criminaliteit – in vergelijking met traditionele criminaliteit – lastiger is om op voorhand in te schatten of een zaak voldoende

opsporingsindicatie bevat. Volgens P9 en P13 kent een aangifte van traditionele criminaliteit vaak meer tactische opsporingsmogelijkheden omdat het delict ergens fysiek plaatsvindt (bijvoorbeeld camerabeelden en getuigenverklaringen). Hierdoor is minder 'door-rechercheren' vereist. Andere respondenten (P18 en P20) stellen dat dit ook het geval kan zijn door een gebrek aan ervaring in het opsporingsteam: "*Je moet echt wel in het werkveld zitten om daar een goede afweging in te kunnen maken*" (P18). Volgens P20 is dit nog steeds een actueel vraagstuk, ondanks dat er binnen zijn eenheid een pilot is gedraaid om hierachter te komen:

> *"Als er heel veel aangiftes op je af komen van een type delict waar je eigenlijk geen ervaring mee hebt, dan is het heel erg lastig om aan de voorkant in te schatten welke zaken je... je kan ze niet allemaal oppakken, dus je moet kiezen. Hoe ga je slim kiezen? Welke zaken zijn kansrijk en welke niet? Bij online criminaliteit wordt bijna nooit aan de voorkant al een verdachte genoemd, dus je zult in elke zaak die je kiest moeten investeren om bij een verdachte uit te komen. In cyberzaken moet je heel vaak veel werk doen en je komt niet eens altijd bij een verdachte uit."*

Schadebedrag

Een andere veelgenoemde reden (n=10) om een zaak niet op te pakken, heeft betrekking op de hoogte van de geleden financiële schade. Opvallend is dat de genoemde bedragen uiteen lopen van 500 euro (P14, P20, P21 en P22) tot 1.000 euro (P9, P10 en P22), 2.000 euro (P3 en P4), 5.000 euro (P24) en 10.000 euro (P15, P23). Wat betreft gemaakte afspraken rapporteren respondenten ook verschillend. Enkele respondenten benoemen dat specifieke afspraken met het OM zijn gemaakt over het schadebedrag waarbij een zaak niet opgepakt mag of hoeft te worden (bijvoorbeeld P14, P20, P21 en P22). Anderen (P15 en P16) leggen uit dat dit meer de praktische gang van zaken is. Zo stelt P15:

> *"Over het algemeen als een zaak wordt opgepakt, wordt gekeken van waar is nou veel schade gemaakt, omdat dat dan een zaak is die ogenschijnlijk veel vlees op het bot heeft."*

Door drie respondenten (P14, P16 en P21) – die alle drie benoemen dat de grens op 500 euro ligt - wordt een specifieke reden gegeven, namelijk dat een dergelijk bedrag niet opweegt tegen de kosten van een zogenaamde BOB-aanvraag (bijzonder opsporingsbevoegdheid) die gedaan zal moeten worden indien de zaak wordt opgepakt.

> *"We hebben een beleidsregel dat in principe onder de 500 euro geen BOB-aanvragen worden gedaan, omdat een gemiddelde BOB-aanvraag zo 200-300 euro kan kosten. Dat is best wel prijzig." (P21)*

Verder veronderstellen enkele respondenten (P3, P4, P10) dat het screenen op schadebedrag uit één enkele aangifte – zeker bij online criminaliteit – eigenlijk onjuist is, omdat daders van online criminaliteit vaak meerdere slachtoffers maken en het schadebedrag in werkelijkheid dus hoger ligt dan in een oogopslag zichtbaar is. P3:

> *"Het is van belang dat aangiften los van elkaar behandeld worden. Het schadebedrag is in een individueel geval wellicht onder de 2.000 euro, maar in samenhang met andere zaken (met dezelfde dader) een stuk hoger."*

Het wordt daarnaast als onterecht verondersteld omdat het verliezen van een bepaald bedrag voor elk individu een andere betekenis heeft.

> *"Omdat het alle lagen van de bevolking raakt, zijn er hier en daar ook mensen die relatief weinig geld verliezen maar nog steeds geraakt worden. […] Neem een student van twintig, als diegene 2.000 euro verliest, is dat economisch veel zwaarder dan iemand die een ton op de bank heeft en 10.000 euro kwijt is. Ik vind dat af en toe wel lastig." (P15).*

Ten slotte benoemen enkele respondenten (P1, P9, P11 en P12) het feit dat zaken in de regel ook uitgescreend worden wanneer de financiële schade van een slachtoffer al vergoed is, bijvoorbeeld door de bank, verzekeraar of webshop.

Opsporing

Literatuur

Er kunnen verschillende redenen zijn waardoor zaken uitstromen tijdens de opsporing: zaken kunnen uitvallen op wettelijke gronden (de gedraging is geen misdrijf of het misdrijf kan niet worden bewezen), door een gebrek aan publieke interesse of door de geringe ernst van het misdrijf (Harrendorf, 2018). In onderzoek van de Algemene Rekenkamer (2012) worden enkele ongewenste vormen van uitstroom tijdens de opsporing in Nederland benoemd. Ten eerste waren er destijds zaken die als 'afgerond onderzoek zonder verdachte' uitstroomden, waarvan een deel ongewenst was. Een deel van deze uitstroom had namelijk eerder plaats kunnen vinden, waardoor capaciteit beschikbaar was voor andere onderzoeken. Een ander deel had juist wel kunnen doorstromen wanneer de kwaliteit van het opsporingswerk beter was of er tijdig capaciteit beschikbaar was. Aanvullende verklaringen voor deze ongewenste uitstroom zonder verdachte zijn een gebrekkige kwaliteit van de aangiften, een gebrek aan sturing en een gebrek aan kennis van digitale en financiële zaken (Felix, 2013). Een tweede vorm van ongewenste uitstroom werd gevonden in politiesepots. Formeel gezien is de politie niet bevoegd om zaken te seponeren zonder toestemming van het OM (art. 152 Sv), maar in de praktijk bleek dit

wel voor te komen (Algemene Rekenkamer, 2012). Recenter onderzoek van de Inspectie Justitie en Veiligheid (2019b) heeft verschillende knelpunten geïdentificeerd in het functioneren van de opsporing door de Nationale Politie. Ten eerste bleek dat de opsporing binnen de politie nog niet voldoende functioneert als één organisatie, omdat er nog onvoldoende wordt samengewerkt tussen verschillende onderdelen zoals de recherche, informatiepositie en Politieacademie. Een tweede knelpunt is dat de politie nog onvoldoende heeft geïnvesteerd op het gebied van politieonderwijs. De meeste opleidingen – en met name het curriculum intelligence – voldoen volgens de inspectie niet aan de behoefte. Tot slot is de besluitvorming over de opsporingscapaciteit in de stuurgroepen ondoorzichtig en verbrokkeld, waardoor de opsporingscapaciteit niet optimaal wordt benut (Inspectie Justitie en Veiligheid, 2019b).

Uit de literatuur komen vier factoren naar voren die de opsporing van online criminaliteit door de politie tegenhouden of vertragen: (1) een gebrek aan prioriteit, (2) een gebrek aan kennis, (3) een gebrek aan capaciteit, en (4) de complexiteit van online criminaliteitszaken.

Onderzoek laat zien dat er een gebrek aan prioriteit is binnen politieorganisaties (zowel nationaal als internationaal) voor de opsporing van online criminaliteit (Goodman, 1997; Struiksma *et al.*, 2012; Leukfeldt *et al.*, 2012; Leukfeldt *et al.*, 2013; Harkin *et al.*, 2018; De Paoli *et al.*, 2020). Redenen die worden genoemd voor dit gebrek aan prioriteit zijn een beperkt bewustzijn van de risico's van online criminaliteit, zowel binnen de politiecultuur als onder burgers (Goodman, 1997; De Paoli *et al.*, 2020), een gepercipieerde lagere (sociale) impact van online criminaliteit (Leukfeldt *et al.*, 2013), een gebrek aan kennis en ervaring onder rechercheurs (Leukfeldt *et al.*, 2013), de complexiteit van opsporingsonderzoeken (Goodman, 1997) en de onzichtbaarheid van online criminaliteit (Goodman, 1997). Het gebrek aan commitment en prioriteit voor online criminaliteit leidt bijvoorbeeld ook tot onvoldoende training van medewerkers binnen de politieorganisatie (Harkin *et al.*, 2018).

Een gebrek aan kennis wordt ook aangemerkt als factor die de opsporing van online criminaliteit hindert. Uit onderzoek blijkt namelijk dat er te weinig kennis en vaardigheden zijn onder politiemedewerkers om opsporingsonderzoeken inzake online criminaliteit (effectief) op te pakken (Leukfeldt *et al.*, 2012; Leukfeldt *et al.*, 2013; Hadlington *et al.*, 2018; Holt *et al.*, 2019; De Paoli *et al.*, 2020). Zo wordt er een gebrek aan (effectieve en consistente) trainingen voor huidige en nieuwe eerstelijnsmedewerkers geconstateerd (Brown, 2015; Hadlington *et al.*, 2018; De Paoli *et al.*, 2020). Ook worden politiemedewerkers en aanklagers in het Verenigd Koninkrijk volgens de onderzoekers (ten tijde van het onderzoek) niet voorzien van continue training over de modus operandi van cyberdaders en andere onderwerpen gerelateerd aan de opsporing van online criminaliteit (Brown, 2018). In Nederland wordt verder geconstateerd dat het ontbreekt aan verspreiding van kennis en

kunde binnen verschillende lagen van de politie-eenheden (Boekhoorn, 2019). Brown (2015) constateert zelfs dat de gezondheid van werknemers in de opsporing van online criminaliteit in het Verenigd Koninkrijk onder druk staat door een gebrek aan ervaring en een hoge werkdruk (Brown, 2015). Bovendien wordt opgemerkt dat er in Nederland geen landelijke aansturing is om de informatiepositie te versterken (Boekhoorn, 2019) en dat er geen centraal punt is waar kennis over online criminaliteit wordt verzameld en ontsloten (Struiksma *et al.*, 2012). Hierdoor wordt soms meerdere keren dezelfde kennis ontwikkeld binnen verschillende onderdelen van de politieorganisatie.

Ten aanzien van de capaciteit in de opsporing worden ook enkele knelpunten genoemd. Zo constateren Leukfeldt *et al.* (2013) personeelsuitdagingen omtrent de opsporing van online criminaliteit. Kennis over online criminaliteit is namelijk moeilijker te verkrijgen, de kennis heeft een kortere levensduur, politiemedewerkers met kennis worden weggetrokken door private partijen en carrièrevoortgang binnen specialistische politieteams is een probleem. Maar ook technische middelen en geld ontbreken om informatie te ontsluiten tijdens de opsporing (Brown, 2015).

Verder blijkt de opsporing van daders van online criminaliteit complex te zijn (Boekhoorn, 2019) door de aard van online criminaliteit. Ten eerste is het moeilijker om daders te identificeren die informatiesystemen en apparaten gebruiken (Brown, 2015). Opsporingsinstanties dienen bijvoorbeeld te bewijzen dat personen ten tijde van het delict gebruik maakten van een apparaat of systeem. Een tweede factor die de opsporing complex maakt, is het internationale karakter (Brown, 2015; Boekhoorn, 2019). Online criminaliteit gaat over de grenzen van regio's, eenheden en landen heen. Slachtoffers en daders kunnen zich daardoor in verschillende jurisdicties bevinden, wat (formele) samenwerking vereist die niet altijd aanwezig is (De Paoli *et al.*, 2020). Wanneer er wel samenwerking is, kunnen bijvoorbeeld internationale rechtshulpverzoeken erg tijdrovend zijn (Odinot *et al.*, 2017; Custers, 2018; Van den Eeden *et al.*, 2021). Ten derde worden er problemen geconstateerd rondom wet- en regelgeving. Zo is het bijvoorbeeld lastig voor wetgevers om de ontwikkeling van technologie bij te houden (De Paoli *et al.*, 2020), is er een gebrek aan materieel en formeel recht (De Paoli *et al.*, 2020) en verschilt wet- en regelgeving tussen landen waardoor mogelijkheden ontstaan voor daders om online criminaliteit te plegen (Brown, 2015). Ook is het verkrijgen en behouden van digitaal bewijs lastig door de vluchtigheid van digitale gegevens (Brown, 2015; Karie & Venter, 2015), zijn er problemen rondom de ontvankelijkheid en rechtvaardigheid van bewijsvoering (Brown, 2015) en is er door privacywetgeving een gebrek aan toegang tot digitale gegevens voor opsporingsdiensten (Brown, 2015; Van den Eeden *et al.*, 2021).

Interviews

Gedurende de interviews werd ook gesproken over mogelijke knelpunten in het opsporingsproces die ervoor kunnen zorgen dat zaken uitstromen. Deze komen overeen met de factoren waarvan op grond van de literatuur aangenomen kan worden dat deze de opsporing van online criminaliteit door de politie tegenhouden of vertragen, te weten een gebrek aan prioriteit, een gebrek aan kennis, een gebrek aan capaciteit en de complexiteit van online criminaliteitszaken. In het vervolg van deze paragraaf zullen deze punten op basis van de interviews verder worden uitgewerkt, waarna tot slot aandacht wordt besteed aan een ander punt dat uit de interviews naar voren kwam, namelijk een gebrek aan eigenaarschap over aangiften van online criminaliteit.

Gebrek aan prioriteit

In de literatuur werden verschillende redenen genoemd voor een gebrek aan prioriteit voor de opsporing van online criminaliteit, waaronder een beperkt bewustzijn van de risico's van online criminaliteit, een gepercipieerde lagere (sociale) impact van online criminaliteit, een gebrek aan kennis en ervaring onder rechercheurs, de complexiteit van opsporingsonderzoeken en de onzichtbaarheid van online criminaliteit. Waar het laatstgenoemde al aan bod is gekomen in hoofdstuk 4 en de complexiteit van opsporingsonderzoeken verder in deze paragraaf wordt uitgewerkt, werd in lijn met een gebrek aan prioriteit door respondenten hoofdzakelijk gesproken over een gepercipieerde lagere (sociale) impact.

Achttien respondenten benoemen dat traditionele delicten in de praktijk voorrang hebben op online delicten. Zoals eerder benoemd is, worden hiervan concrete voorbeelden gegeven, waaronder onderstaande:

> *"Hoe is het mogelijk dat mensen urenlang bezig zijn met een winkeldief die twee droge worsten uit de winkel heeft gehaald en dat we op dezelfde dag doodleuk van een aangifte van diefstal van cryptomunten waarbij iemand 60.000 euro heeft verloren, zeggen 'ja, dat is wel een beetje dom, dat je in die phishing-mail bent getrapt. Nee, daar hebben we geen tijd voor.' Hoe is dat mogelijk? Ik en mijn collega's snappen dat niet, en toch zien we het elke dag weer gebeuren. Allebei. Die winkeldief wordt weer opgehaald, wij gaan weer uren binnen zitten en horen en dossiers maken en weet ik veel wat allemaal. En die aangifte wordt ook weer aan de kant geschoven. Dat gaat niet goed." (P20)*

En ook:

> *“Onze coördinator is wegens een steekincident met dodelijke afloop wekenlang van het [cyber]project weggehaald. Dat is problematisch. Cyber is leuk als het uitkomt. Maar als het niet zo handig is, liever niet.” (P5)*

Respondenten spreken over ‘bloed = spoed’ (P3 en P4) en wijzen in meer algemene zin op de voorrang die traditionele criminaliteit nog steeds lijkt te hebben omdat die een grotere maatschappelijke impact zou hebben (P2, P9), meer ‘gevoeld’ wordt (P10, P16), bijvoorbeeld omdat de afstand tussen dader en slachtoffer kleiner lijkt (P13, P15) en online criminaliteit daardoor juist als ‘minder tastbaar’ wordt gezien (P6 en P7). Meerdere respondenten benadrukken dat deze gepercipieerde lagere (sociale) impact volgens hen onterecht is. Zo ook P16 en P18:

> *"Dat vind ik het ergste. Als je ziet, iemand krijgt een klap op z'n oog. 'Oh, zo erg, verschrikkelijk.' Maar het beeld, en dat mist compleet in Nederland, van wat het met die mensen [slachtoffers van online criminaliteit] doet, dat is zo sneu. Ik ben daar meerdere keren geweest, die mensen staan door een kier naar buiten te kijken. Als ik ze bel dan hangen ze op. Ze zijn zo angstig. Daar is helemaal geen zicht op. Maar als jij een klap op je neus krijgt, 'oh nou, dat is traumatisch.' Maar díe mensen [slachtoffers van online criminaliteit] hebben een trauma." (P16)*

> *"Want er zit geen direct leed in. Terwijl als je soms hoort hoeveel leed die slachtoffers hebben, dat al hun spaargeld weg is, dat ze hun hele leven hebben verzameld, dat veroorzaakt heel veel leed, alleen het is minder direct zichtbaar." (P18)*

Vier andere respondenten (P3, P4, P24, P26) zijn van mening dat traditionele criminaliteit in de praktijk vaak boven online criminaliteit geprioriteerd wordt doordat de werkprocessen binnen de politieorganisatie daar nou eenmaal zo op ingericht zijn. Heterdaadzaken (waarbij verdachten zijn aangehouden) gaan voor op niet-heterdaadzaken (niet-aangehouden verdachten), zo blijkt uit onder meer het volgende citaat:

> *“Bij gedigitaliseerde criminaliteit is vaak (nog) geen verdachte in beeld. Dit heeft dus betrekking op de niet-vaste werkstroom. Gechargeerd gezegd heeft vaste proces voorrang op het niet-vaste proces. Dit werkt belemmerend voor het oppakken van online criminaliteit. Het gevolg hiervan is dat de winkeldief die een blikje steelt voorrang krijgt op een VIN-fraude waar duizenden euro’s zijn buit gemaakt.” (P3)*

Politieteams hebben in de praktijk lang niet altijd zelf de keuze tussen het oppakken van een traditioneel delict en een online delict. In het geval van een aanhouding (bijvoorbeeld bij een

winkeldiefstal), moet die verdachte simpelweg 'afgehandeld' worden. De tijd die daar in gaat zitten kan vervolgens niet besteed worden aan de andere zaken die liggen te wachten.

Hoewel traditionele criminaliteit het volgens respondenten in de prioritering van de praktijk vaak wint van online criminaliteit, geeft wel de meerderheid van de respondenten (n=19) aan dat er wat betreft de prioritering van online criminaliteit een verbetering zichtbaar is. Dit uit zich volgens hen in de opzet en ontwikkeling van gespecialiseerde teams (waaronder het LMIO en de cybercrimeteams op eenheidsniveau), op online criminaliteit gerichte 'projecten' zoals Operatie Centurion[10] (P3, P4, P5, P6, P7, P9 en P14), een toename in vacatures die tevens toegankelijk zijn voor externen (P1, P9), een groter bewustzijn binnen de politieorganisatie van de noodzaak om online criminaliteit aan te pakken, meer sturing op het thema (P8, P9, P14, P18) en meer ruimte voor opleidingen en trainingen (P2, P6, P7). P14 merkt op dat hij eerst *"moest trekken aan een dood paard"* maar dat teams nu gemakkelijker mee te krijgen zijn omdat zij zien dat *"zij niet meer kunnen weglopen voor cyber"*, hetgeen P1 beaamt. Het thema begint meer te leven (P13, P14) en er komt meer begrip voor. Zo stelt P15:

> *"Je ziet dat gaandeweg de tijd bepaalde fenomenen meer voorkomen, bekendheid krijgen, duidelijker in beeld worden gebracht en daarmee ook de prioritering meer vorm krijgt."*

Volgens respondenten (P10, P11, P12 en P20) valt online criminaliteit inmiddels officieel onder zogenaamde 'prio 1'-delicten en staat het tegenwoordig hoog op zowel regionale als landelijke Veiligheidsagenda's (P15, P16 en P17). P15:

> *"Dat is het manifest om te zeggen van 'kijk, het is belangrijk!' En het feit dat we meer capaciteit hebben gekregen heeft hier zeker mee te maken. We hadden nooit een team van deze expertises kunnen krijgen als het niet op enig punt geprioriteerd was."*

Volgens P25 heeft het prio-1 label echter enkel betrekking op gedigitaliseerde criminaliteit en dus niet op online criminaliteit in brede zin. Bovendien, zolang online criminaliteitszaken ondanks het prio-1 label in de praktijk nog altijd vroegtijdig worden beëindigd, is een groter urgentiebesef en erkenning door middel van Veiligheidsagenda's volgens respondenten niet voldoende voor een succesvolle aanpak van online criminaliteit. P14:

> *"Dat is de eerste winst. De volgende stap en onze doelstelling is echter dat elke cyberzaak serieus bekeken wordt."*

[10] Operatie Centurion is een landelijk opererend politieteam dat zich net zoals het LMIO bezighoudt met het clusteren van online criminaliteitszaken. Centurion richt zich in tegenstelling tot het LMIO niet alleen op aan- en verkoopfraude, maar daarnaast ook op vriend-in-nood-fraude (VIN-fraude), (bank)helpdeskfraude en phishing.

Gebrek aan kennis

De literatuur laat zien dat een gebrek aan kennis en vaardigheden onder politiemedewerkers een succesvolle aanpak van opsporingsonderzoeken inzake online criminaliteit in de weg staat. Dit beeld wordt bevestigd tijdens de interviews. Verschillende respondenten bevestigen dat sprake is van onvoldoende kennis van online criminaliteitszaken onder politiemedewerkers en dat dat inderdaad de doorstroom in de weg kan staan. Drie respondenten (P1, P6, P13) zijn van mening dat vooral de oudere opsporingsambtenaren niet echt digitaal onderlegd zijn omdat deze niet met ICT zijn opgegroeid. P13 stelt dat de wat oudere collega's hierdoor ook minder open staan voor aanpassingen in het werkproces en dat zij deze houding soms ook overbrengen op nieuwe, jongere collega's (aangezien zij zich vaak meten aan de meer ervaren collega's). Daarnaast wordt genoemd dat vooral op basisteam- en districtsniveau sprake is van onvoldoende kennis (P11, P12, P13, P16, P17, P18 en P19). Specialisten werken hoofdzakelijk bij de cybercrimeteams die zich enkel op online criminaliteit focussen, maar basisteams en districtsrecherches beschikken vanwege het aanbod aan ander soort zaken niet over voldoende tijd om ervaring op te doen en een geschikt netwerk op te bouwen.

Het soort kennis dat volgens deze respondenten ontbreekt maar voor een goede aanpak wel noodzakelijk is, betreft enerzijds (basale) technische kennis (zoals wat een URL of IP-adres inhoudt) (P9, P14) en anderzijds welke vorderingen gedaan kunnen worden om de juiste informatie boven water te halen (P11, P12, P13). Een van de respondenten (P22) – werkzaam in een basisteam – benoemt zelf ook dat hij deze twee zaken soms lastig vindt. Zo zegt hij dat IP-adressen voor hem soms nog "abracadabra" zijn en vertelt hij over (het zicht op) opsporingsmogelijkheden:

> *"Je hebt online heel veel mogelijkheden tot opsporing. Ik zal ze niet allemaal weten, maar volgens mij kun je overal wel iets weghalen zeg maar. Dat is voor mij soms nog een grijs gebied, wat wel en wat niet."*

Het bovenstaande wordt bevestigd door andere intakemedewerkers. Zo stelt P19: "*Ik ben echt a-technisch wat dat betreft. Ik snap er gewoon ook niets van. […] Als het over computers gaat dan haak ik af."* Een deel van de respondenten (n=7) is echter van mening dat het opsporen van online criminaliteit helemaal geen hoogwaardige (technische) kennis vereist. De volgende quotes ondersteunen deze constatering:

> *"Digitaal is voor een hoop mensen nog moeilijk, er hangt een soort stigma aan: 'je moet een computernerd zijn.' We moeten eerst de boodschap overdragen dat dat niet nodig is. We moeten juist de kleine dingen, de successen laten zien en voelen zodat men ziet dat het ook anders kan. Iedereen stuurt een appje, kijkt z'n Facebook, deelt een foto op Instagram. Dat moet in je werk precies zo zijn." (P13)*

> *"Het woord 'cyber' zorgt er voor dat mensen dit als een complexe criminaliteitsvorm zien. Dan zien ze meteen zo'n matrix-velden met allemaal 1-en en 0-en. Terwijl de realiteit is dat een deel hiervan gewoon oplichting is met een stekker eraan, een financieel gemotiveerd delict met een gedigitaliseerd randje." (P15)*

Volgens respondenten (n=8) is sprake van "*koudwatervrees*". Online criminaliteit wordt vaak gezien als iets ingewikkelds. Onder de noemer "*onbekend maakt onbemind*" wordt dit veelal toegeschreven aan een gebrek aan opsporingservaring met dergelijke zaken (P9, P10, P25). Meerdere respondenten geven dan ook aan dat het van groot belang is dat opsporingsteams ervaring opdoen met dit soort zaken. "*Als een zaak maar vooruit geschoven blijft worden, is dat heel hardnekkig. Dat vertraagt de leercirkel enorm." (P20).* Hetzelfde wordt gezegd door P3: *"Met tactische vaardigheden kom je al heel ver. Het is vooral belangrijk dat mensen ervaring opdoen, uren maken"*. P14 zegt hierover:

> *"Alles valt en staat met het doen. Je kunt zo veel opleidingen en initiatieven geven, maar als collega's er niet mee gaan werken, dan zijn ze het een week later kwijt. Er moet meer tijd en capaciteit worden vrijgemaakt zodat collega's die het willen doen, het ook mogen doen."*

Waar in de literatuur wordt gesteld dat er te weinig effectieve trainingen bestaan, komt dit in de interviews niet echt aan de orde. Wel wordt gesteld dat online criminaliteit op de Politieacademie onvoldoende wordt meegenomen. P10 vindt dit zorgelijk: "*Zolang je politiemannen en -vrouwen niet voedt of ondervoedt, krijg je beperkingen."* Er is volgens respondenten echter voldoende ruimte voor mensen die zich willen specialiseren, zij het door het volgen van een opleiding, cursus of vakdagen (P6, P7, P13, P23) of door (tijdelijk) mee te draaien in een team waar meerdere specialisten werkzaam zijn (P1, P8, P14, P16). P17 is van mening dat er op grond van de huidige bezetting te weinig ruimte is om een opleiding te volgen indien collega's dat zouden willen. Daarnaast wordt benoemd dat de keuze om een opleiding te volgen volledig bij de medewerker zelf ligt en dus afhankelijk is van de interesse en motivatie van individuele medewerkers, hetgeen een ander knelpunt betreft. Een grote uitdaging wordt namelijk gezien in het enthousiast maken van politiemedewerkers, aangezien niet iedereen affiniteit met dit thema heeft (P9, P10, P11, P13, P15, P20, P23). In vergelijking met traditionele criminaliteit wordt online criminaliteit door de gemiddelde politieambtenaar als *"minder sexy"* gezien (P20, P24, P26) en mensen die wel in online criminaliteit geïnteresseerd zijn, vertrekken volgens P11 vaak naar de specialistische teams, waardoor de kennis binnen de politie ontzettend fluctueert.

Gebrek aan capaciteit

De bevindingen uit de interviews bevestigen de constatering uit de literatuur dat een gebrek aan capaciteit in opsporingsteams een knelpunt vormt voor een goede doorstroom van onderzoeken inzake online criminaliteit. Ondanks dat er zoals eerder aangegeven in ieder geval op papier een

verbetering zichtbaar is in de mate waarin er prioriteit wordt gegeven aan online criminaliteitszaken, geven tenminste 26 respondenten, ofwel een grote meerderheid aan dat zowel de basisteams, de districtsrecherches als de cybercrimeteams kampen met een capaciteitsgebrek. Binnen de eenheid waar P11 werkt zijn de laatste tijd zo'n 250 medewerkers weggegaan. *"Het piept en kraakt in de basisteams en ook de crimeteams gaan van tien naar zes man of zoals in [stad], naar drie man."* Volgens hem en andere respondenten staat dit de opsporing in de weg. Zo vertelt P21:*"Het ligt vaak aan capaciteit dat een hoop zaken tussen de mazen van het net doorglippen."* P6 is van mening dat het gebrek aan opsporingscapaciteit ertoe leidt dat zelfs zaken met een goede opsporingsindicatie *"gewoon op de plank liggen te wachten tot er capaciteit vrij is om deze op te pakken."*

Volgens respondenten (waaronder P8, P9, P15) speelt een rol dat veelal wordt gewerkt met tijdelijke tewerkstellingen (ook wel TTW's genoemd). P8 wijst het succes in een specifiek opsporingsonderzoek toe aan een zij-instromer die middels een TTW binnen het basisteam is aangesteld en de tijd had om zich fulltime met online criminaliteitszaken bezig te houden. Tegelijkertijd vreest hij voor het moment dat deze zij-instromer het team weer moet verlaten: *"Als dat wordt gestopt, dan valt de mogelijkheid op nog zo'n succes per definitie weg. Ik vind dit [experiment met de TTW] fantastisch, maar ik zie met angst en beven het einde ervan tegemoet."* Bovendien heeft dit – zoals ook uit de literatuur bleek – gevolgen voor het waarborgen van relevante kennis binnen de politieorganisatie. Zo kost het volgens P9 enige tijd voor een team *"qua kennis up to speed is"*, maar worden medewerkers wanneer de kennis in een team op niveau is weer overgezet naar een andere afdeling. In dat geval begin je volgens haar weer van vooraf aan, hetgeen P10 en P11 bevestigen.

Verder wordt in de interviews ook bevestigd dat politiemedewerkers met kennis van online criminaliteit soms vertrekken naar private partijen of de overstap maken naar de meer specialistische politieteams. Genoemd wordt dat het zowel lastig is om IT-specialisten binnen te krijgen als binnen te houden omdat zij in het bedrijfsleven veel meer zouden kunnen verdienen (P9, P13, P17). P13 is zelf IT-specialist en is bekend met de beweging dat IT-specialisten de politieorganisatie over het algemeen snel verlaten. Hij vertelt dat het een andere motivatie vergt om voor de politie te (blijven) werken, maar dat niet iedereen die motivatie heeft:

> *"Ik heb ook wel eens de opmerking gehad van waarom ga je niet voor jezelf beginnen of bij [cybersecuritybedrijf] werken? Natuurlijk, er is vraag naar en je kan er veel meer verdienen, maar ik heb ooit bij de politie gesolliciteerd omdat ik ergens voor stond, omdat ik iets wil uitdragen en dat vind ik belangrijk. Voor mij is het dan niet het geld dat telt, ik wil ook betekenis geven aan mijn werk. En ik voel me dan hier meer op mijn plek dan bij een extern bedrijf." (P13)*

De complexiteit van online criminaliteitszaken

Ten vierde wordt tijdens de interviews genoemd dat de opsporing van online criminaliteit complex in elkaar steekt en dat dit een knelpunt kan vormen voor een goede doorstroom hiervan. Alle factoren die online criminaliteit complex (kunnen) maken en in de literatuurstudie werden genoemd, werden ook tijdens de interviews gevonden. Veruit het meest genoemd betreft het mogelijke internationale karakter van online criminaliteit en de constatering dat het verkrijgen en behouden van digitaal bewijs lastig is door de vluchtigheid van gegevens in de online wereld. In het vervolg van deze paragraaf wordt verder uitgewerkt waarom dit volgens de respondenten knelpunten vormen in de doorstroom van online criminaliteit.

Allereerst wordt de aanname dat online criminaliteit niet aan (lands)grenzen gebonden is gezien als belemmerend punt bij het oppakken van dergelijke zaken. Dit wordt door meerdere (tenminste 12) respondenten aangekaart. Respondenten geven bijvoorbeeld aan dat het voorkomt dat het doen van een rechtshulpverzoek op voorhand niet haalbaar wordt geacht en zaken daardoor vroegtijdig worden beëindigd, bijvoorbeeld wanneer een provider in het buitenland wordt gehost of geld via een buitenlands rekeningnummer gaat. Dit komt enerzijds doordat het doen van een rechtshulpverzoek volgens respondenten (n=7) ontzettend veel tijd kost en doordat partijen niet altijd meewerken en/of de gevraagde informatie tijdig delen (P9, P15). Volgens P15 speelt het internationale aspect vooral een rol bij cybercrime en minder bij gedigitaliseerde criminaliteit, maar dit speelt ook een rol bij bijvoorbeeld de VIN-fraude netwerken die hun berichten vertalen en op die manier slachtoffers in of vanuit het buitenland maken. Ook in het geval van gedigitaliseerde criminaliteit wordt informatie uit het buitenland meestal niet opgevraagd. Zo stelt P15: *"Voordat we informatie van de Duitsers terug hebben, ligt het dossier over het algemeen al bij justitie."* Sommige respondenten vermoeden dat criminelen inmiddels wel weten dat een buitenlands component de opsporing voor de politie veel lastiger zo niet onmogelijk maakt.

Er is slechts één respondent die van mening is dat problemen ten aanzien van internationale rechtshulpverzoeken door collega's vaak worden overdreven. Hij vindt sporen die uitlopen in het buitenland dan ook geen goed argument om bij voorbaat te stoppen met een opsporingsonderzoek.

> *"Er zijn veel indianenverhalen. Ik hoor veel collega's klagen, zo van 'die reageren niet.' Op een gegeven moment dacht ik, ik ga gewoon uitvogelen of dat echt zo is. Ik ben dat hele spoor gaan uitlopen en dan blijkt dat zo'n provider dezelfde dag heeft geantwoord, maar dat het ergens in het proces fout is gegaan of dat er interne miscommunicatie is. In sommige gevallen hebben de collega's een verdiepingsvraag gekregen die zij niet hebben beantwoord, dus dan ligt het gewoon aan de collega's zelf." (P18)*

Hij vervolgt:

> *"Er zijn afspraken gemaakt met het IRC (Internationaal Rechtshulp Centrum)." Er bestaat een Landelijk IRC (LIRC) en alle eenheden beschikken over een IRC. "Uitgaande rechtshulpverzoeken worden gewoon gedaan. Als we een Google-account willen hebben, dan doen we gewoon een rechtshulpverzoek naar Google of een crypto-exchange. Dat is voor ons [team] géén belemmering waardoor we ons laten stoppen."*

Wel onderschrijft ook P18 dat het doen van een rechtshulpverzoek complex kan zijn. Onder meer het type land speelt een rol en daar hangt het zogenoemde 'wederkerigheidsbeginsel' mee samen. Zo verstuurt Nederland geen rechtshulpverzoeken naar China of Iran omdat we niet bereid zijn een wedervraag te beantwoorden. Daarnaast speelt het type bedrijf een rol. Grotere bedrijven – zoals Google en Microsoft – hebben dit vaak goed ingericht, bijvoorbeeld door middel van *Compliance Officers* of eigen advocatenkantoren. Bij kleinere bedrijven wordt het lastiger of kan het langer duren, zo legt P18 uit.

Met P18 zijn er anderen (P11, P12, P16) die het rechtshulpverzoek-probleem relativeren door te benadrukken dat een buitenlands rekeningnummer, een buitenlandse cryptobeurs of een buitenlandse server niet per definitie betekent dat een dader zich in het buitenland begeeft. Vaak wordt er met buitenlandse rekeningnummers ook gewoon in Nederland gepind of leidt het postadres naar een Nederlands adres (P11, P12). Tevens ligt een oplossing volgens P9 en P15 in het gegeven dat veel van dit soort daders zowel slachtoffers in Nederland als het buitenland maken. In zo'n geval kan er ook voor worden gekozen om de verdachte(n) enkel op basis van de aangiften van Nederlandse slachtoffers in te sturen naar het OM.

Behalve het internationale karakter vormt zoals gezegd de 'vluchtigheid van gegevens op internet' een knelpunt die de doorstroom van online criminaliteit bemoeilijkt. Een grote inhaalslag is volgens respondenten (P19) dan ook te maken bij aanvang van het opsporingsproces. P13:

> *"De aangifte is natuurlijk het allerbelangrijkste. Niet alleen qua inhoudelijke informatie, maar ook wat betreft de snelheid waarmee het opgepakt wordt. Dat is cruciaal omdat we met vluchtige gegevens werken."*

Of een aangifte na een week wordt opgenomen (P15), na twee weken (P13) of na vier weken (P10), respondenten zijn het er over eens dat informatie inzake online criminaliteit vaak te snel verloren gaat en dat vorderingen om die reden snel moeten worden uitgevoerd.

> *"Vanuit digitaal oogpunt is een week een eeuwigheid! Het zijn vluchtige gegevens, dat is zeker in cyberzaken heel belangrijk. Voordat een aangifte is opgenomen, gewogen, aan een*

opsporingsteam is toegevoegd... dan ben je al zo'n bulk aan informatie kwijt. Tenzij de burger toevallig weet wat hij veilig moet stellen..." (P15)

De processen binnen de huidige strafrechtketen zijn volgens P6 niet goed genoeg ingericht om deze vluchtige informatie tijdig veilig te stellen. Er worden verschillende voorbeelden van vluchtige data genoemd, waaronder camerabeelden van pinautomaten (P5, P9, P17), IP-adressen (P9, P13, P19), informatie op servers (P6), printlijsten van telecomproviders die aantonen wanneer telefoongesprekken hebben plaatsgevonden en mastgegevens die laten zien waar iemand zich tijdens een telefoongesprek bevond (P13) of log-gegevens van het programma AnyDesk, een remote desktop applicatie die wordt gebruikt bij verschillende helpdesk-fraudes. AnyDesk-data dienen volgens respondenten zelfs al binnen 48 uur na de fraude veiliggesteld te worden omdat deze data anders verloren gaan (P11, P12).

In lijn met het bovenstaande is ook van belang op te merken dat sommige informatie niet eens te bevragen is. Te denken valt aan een niet-bevraagbare links, waaronder een valse URL of vals betaalverzoek. Zo stelt P16:

"Je hebt de echte link van Tikkie, die is via de ABN AMRO bevraagbaar. Dan krijg je bepaalde gegevens om op te sporen. Maar je hebt ook fake links. Stuk moeilijker. Dan stoppen we omdat we dit niet bij een partij kunnen vorderen."

P5 gaat in op de oorzaak van de lange tijdsduur van vorderingen (ofwel BOB-aanvragen). Volgens deze respondent zijn te veel actoren bij dit proces betrokken, te weten een officier van justitie (die toestemming moet geven), de BOB-kamer en mensen bij de organisatie waar de informatie wordt opgevraagd (zoals een bank of provider).

"Alleen om te weten waar iemand heeft gepind. Dan denk ik jongens, kom op. Daar kan echt mijn bloed van gaan koken. Hoe bureaucratisch zijn we? […] Het kost enorm veel capaciteit, terwijl het wat mij betreft middels een telefoontje op te lossen is. Dat scheelt vijf mensen werk, voor zoiets simpels." (P5)

Voorts spelen de hoge kosten van een BOB-aanvraag een rol, zo stelt P21. Het betreft een kosten-baten-afweging die door het OM wordt gemaakt:

"*Ik heb rekeningen gezien van 300 euro voor één BOB-aanvraag. Soms moet je in een onderzoek zeven BOB-aanvragen doen, dan zit je al op 2.100 euro. Ik heb onderzoeken gehad waarbij je uiteindelijk niet eens tot een dader komt, dus dat is een hoop geld en energie en dan heb ik het nog niet eens over de personeelskosten." (P21).*

Volgens deze respondent kan de afweging die het OM hierin maakt ook leiden tot de conclusie dat een dergelijke zaak vroegtijdig beëindigd moet worden en dus niet succesvol doorstroomt.

Wanneer vorderingen niet of niet tijdig zorgen voor nieuwe informatie tijdens een opsporingsonderzoek, wordt het volgens P13 lastiger om een zaak rond te krijgen. *"Je ziet dat de benodigde data allemaal slinkt en dat het steeds lastiger wordt om iets bewijsbaar te krijgen."* Dit komt overeen met hetgeen in de literatuur is gevonden, namelijk dat de vluchtigheid van gegevens het verkrijgen en behouden van digitaal bewijs bemoeilijkt. Twee respondenten (P2, P10) ondersteunen ook de bevinding uit de literatuur dat problemen rondom de ontvankelijkheid en rechtmatigheid van de bewijsvoering bij online criminaliteit een rol spelen. De bewijslast is volgens hen complexer. Het is bijvoorbeeld niet alleen noodzakelijk om te bewijzen dat het delict via een bepaald apparaat heeft plaatsgevonden, maar ook dient te worden bewezen dat de verdachte degene was die op dat moment *"achter de knoppen zat"* (P10). Dat is volgens deze twee respondenten vaak lastig hard te maken.

Daarnaast benoemen respondenten (P5, P13) dat de politie als gevolg van wet- en regelgeving (met name omtrent privacy) vaak over onvoldoende opsporingsmogelijkheden beschikt om digitaal bewijs veilig te kunnen stellen. Dit komt ook overeen met de literatuur. P5 geeft het voorbeeld van een stalkings-zaak waarbij het Google-systeem in het huis van het slachtoffer was gehackt. Waar de politie tegen allerlei wettelijke struikelblokken aanliep, leidde het inschakelen van een televisieprogramma wel tot de oplossing van de zaak. Volgens de respondent komt dat omdat journalisten niet aan dezelfde regels gebonden zijn. P13 benadrukt dat privacybelangen steeds zwaarder wegen:

> *"Als ik bijvoorbeeld een printlijst wil opvragen, daar nam voorheen de officier van justitie een beslissing over. Op Europees niveau is daar nu een uitspraak over geweest waarin gesteld werd dat dat privacygevoelig is en dat dat via een rechter-commissaris moet, dus dan ga je weer een stapje hoger. Daar zitten steeds meer en grotere schakels tussen en de bezwaren worden ook steeds groter. Privacy is echt een ding wat voor ons werk een hoop belemmeringen oplevert."*

De bevindingen uit de literatuur worden in de interviews dus bevestigd. Respondenten wijzen echter ook nog op andere factoren die online criminaliteit in vergelijking met traditionele delicten complex maakt. In de eerste plaats wijzen zes respondenten (P1, P11, P12, P15, P20 en P24) op het grote aantal slachtoffers dat met online criminaliteit gepaard gaat en de ervaring dat slachtoffers vaak niet binnen dezelfde eenheid woonachtig zijn. Dit levert volgens hen meer werk op dan het geval is bij traditionele delicten, waar per delict vaak minder slachtoffers aangifte van doen.

Ten tweede wordt gewezen op de snelheid waarmee de verschijningsvormen van online criminaliteit veranderen (P6, P7, P11, P12, P15, P19, P20, P21, P22, P24). *"Waar je vandaag denkt helemaal bij te zijn, word je morgen alweer door de realiteit ingehaald. […] Het is vijf over twaalf. Tegen de tijd dat wij*

nieuwe oplichtingstrucs hebben uitgevonden, hebben zij [oplichters] alweer wat nieuws", aldus P19. Daders van online criminaliteit ontwikkelen volgens respondenten veelvuldig nieuwe modus operandi, hetgeen een wendbare politieorganisatie vereist. Ook vergt het volgens respondenten de bereidheid om deze nieuwe werkwijzen te ontrafelen en deze kennis organisatiebreed te delen zodat niet iedereen zelf het wiel hoeft uit te vinden. P21 benadrukt dat behalve binnen de politieorganisatie ook in de samenleving tijdig moet worden gecommuniceerd over (nieuwe) vormen van online criminaliteit. De media berichten volgens haar vaak over online criminaliteitsvormen op het moment dat deze helemaal niet meer actueel zijn, hetgeen een succesvolle preventieve aanpak in de weg zou staan. Ook P26 benadrukt de preventieve rol van de media door over actuele vormen van online criminaliteit te berichten.

Gebrek aan eigenaarschap

Tot slot merken respondenten (n=8) een ander knelpunt op die gelinkt kan worden aan de bevinding dat online criminaliteit niet aan grenzen gebonden is en dat aangiften van online criminaliteit – die mogelijk tot dezelfde verdachte leiden – hierdoor vaak bij verschillende politie-eenheden in het land binnenkomen. Het is bij online criminaliteit namelijk op voorhand niet altijd evident 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. Opsporingsteams zijn volgens respondenten veelal lokaal georiënteerd, wat op gespannen voet staat met de onbegrensdheid van online criminaliteit. Het gevolg hiervan is dat het eigenaarschap niet altijd duidelijk is.

Wanneer niet duidelijk is aan welk opsporingsteam een zaak toebehoort, kan dit er in de eerste plaats toe leiden dat een zaak helemaal niet wordt opgepakt. Respondenten beschrijven dat zaken *"over de schutting worden gegooid*" (P10), zonder te weten of en door welk opsporingsteam deze uiteindelijk wordt opgepakt. P21 benoemt dat dit bijvoorbeeld het geval was in een helpdesk-fraudezaak die bij het basisteam in haar district binnenkwam. Hierbij deed iemand aangifte omdat zij als geldezel gebruikt was. Gedurende het onderzoek ontving het basisteam een aangifte uit een andere eenheid

met daarbij het verzoek om deze op te pakken, aangezien het rekeningnummer van de ontvanger van het geld overeenkwam met het rekeningnummer van degene die als geldezel werd gebruikt.

> *"Uit verder onderzoek bleek dat er ook een dader in [stad] woonde én er was zelfs 25.000 euro naar iemand in [stad] overgemaakt. […] Dus ik zit naar die zaak te kijken van waarom krijgen wij hem? […] Zo heb je drie versnipperde dingen, terwijl je als totaal onderzoek een heel andere strafmaat krijgt. Die zaak bleef maar heen en weer gestuiterd worden." (P21)*

Ook komt het voor dat een zaak door meerdere teams tegelijkertijd wordt opgepakt, zonder dat zij dat van elkaar weten. Zo stelt P12: *"Als je het niet bundelt aan de voorkant, kan het voorkomen dat je in elkaars vaarwater zit. Met het horen van verdachten en het uitzetten van vorderingen bijvoorbeeld."* Deze respondent geeft tevens een concreet voorbeeld van een zaak waarin dit het geval was. In deze zaak werd aangifte gedaan door vier personen uit drie verschillende woonplaatsen. Alle vier de aangevers gaven hetzelfde bankrekeningnummer op. Vervolgens is de verdachte door twee verschillende teams gehoord.

> *"In [plaats] was de verdachte in beeld gekomen doordat ze een tap hadden lopen op de hoofddaders uit die zaak. [Eenheid] was met de zaak bezig omdat zij een VIN-fraude-pakketje hadden ontvangen uit [eenheid]. Dat is jammer, want je hebt dagen zitten typen en het kan zo de prullenbak in." (P12)*

Mogelijke oorzaken voor dit probleem worden door respondenten toegewezen aan werkprocessen en dan met name aan het feit dat opsporingsteams in verschillende registratiesystemen werken die niet altijd even goed op elkaar aansluiten (P11, P12, P18, P21). Zo werkt het ene team in BVH en het andere in Summ-IT. Ook wordt uitgelegd dat de overdracht van een zaak in principe in BOSZ dient te worden gedaan, maar dat dit enkel mogelijk is voor de overdracht naar een team binnen dezelfde eenheid. Ook binnen BVH is het niet mogelijk om zaken gemakkelijk door te zetten naar een andere eenheid. Hierbij wordt benadrukt dat dossiers fysiek worden overgedragen en dat deze overdracht soms wel weken in beslag kan nemen. Zo stelt P18:

> *"Bijlagen is echt een hot issue. We hebben een verschrikkelijk systeem, BVH. Ik was heel blij dat BVH zou komen, maar ook dit systeem kan geen bijlagen handelen. Je maakt het aangifteformulier op, dat staat in BVH, maar de aangever komt altijd met een heleboel bijlagen waar het bewijs in zit. Dat kan niet in BVH worden geüpload. Momenteel vormt het doorzetten van een zaak naar een andere eenheid een hele papieren stroom, daar kan echt weken overheen gaan voordat we de fysieke stukken in bezit hebben." (P18)*

Tot slot wordt benoemd (P9, P11, P12, P18) dat dit niet alleen gevolgen heeft voor de doorstroom van dit soort zaken, maar ook voor de registratiecijfers:

"Als ik een zaak overdraag naar [eenheid], dat gaat niet. Dat betekent dat ik de zaak hier moet afboeken. Die eenheid moet de zaak opnieuw in BVH pro forma zetten. Dan staat er dus een nieuwe zaak in BOSZ en die kunnen ze dan intern routeren naar de juiste afdeling. […] Als we een onderzoek hebben waarin we bijvoorbeeld twintig aangiftes hebben, dan zijn er misschien wel tien of meer afkomstig uit een andere eenheid. Dus dat zijn allemaal nieuwe aangiftes die we pro forma moeten aanmaken in ons systeem, wat een gigantisch vertekend beeld veroorzaakt." (P18)

OM en ZM

Literatuur

Uit de meest recente cijfers van de Strafrechtketenmonitor (Directie Strafrechtketen, 2020) blijkt dat 91% van de misdrijven vanuit de politie wordt ingezonden naar het OM[11]. Van de misdrijven die in 2020 bij het OM instroomden, werd in de initiële stroom[12] bij 42,3% van de misdrijven overgegaan tot dagvaarding. Verder werd 31,3% afgedaan als onvoorwaardelijk sepot en 6,9% als voorwaardelijk sepot. In de berechtingsfase werd in 2020 volgens de Strafrechtketenmonitor bij 79,2% van de zaken in de initiële stroom besloten tot schuldigverklaring met en zonder straf. In 6,4% van de gevallen werd besloten tot vrijspraak.

Bij de doorstroom van zaken bij het OM worden door de Algemene Rekenkamer (2012) twee mogelijke vormen van ongewenste uitstroom benoemd: (1) technische sepots en (2) onvoorwaardelijke beleidssepots. Technische sepots zijn vaak het gevolg van een gebrek aan bewijs. Deze sepots kunnen ongewenst zijn indien de politie onnodig werk verricht (terwijl voor het OM al duidelijk was dat een zaak onvoldoende bewijs bevat) óf als een zaak wel kansrijk zou zijn geweest indien meer tijd was besteed aan de zaak of de kwaliteit beter was geweest. Onvoorwaardelijke beleidssepots komen vaak voor als gevolg van een oud feit, doordat er een lange tijd is verstreken nadat een feit is gepleegd. De volgende onderliggende verklaringen worden hiervoor genoemd: (1) gebrekkige sturing op doorlooptijden in de gehele strafrechtketen, (2) capaciteitsgebrek bij de rechtbank, (3) relatief veel dagvaardingen en (4) lang traject in de strafrechtketen (Felix, 2013). Verklaringen voor het niet

[11] Het percentage misdrijven dat in 2020 werd ingezonden naar het OM is een stuk hoger dan in eerdere jaren, omdat sinds 2019 is besloten om alle onvoorwaardelijke sepots in het primaire systeem van het OM vast te leggen. De sepots worden in de opsporingsfase daarom vanaf 2019 geregistreerd als 'inzenden naar het OM'.

[12] Dit betreft dus geen zaken die instromen doordat bijvoorbeeld een verdachte gebruik maakt van de mogelijkheid om in beroep te gaan tegen de eerste inhoudelijke beslissing.

uitstromen van zaken bij het OM kunnen liggen in zaakinhoudelijke aspecten, procesmatige redenen, technische problemen en organisatorische redenen (zie Reitsma & Heijmen, 2015 voor meer context).

Inhoudelijke knelpunten die de Algemene Rekenkamer identificeerde in de berechtingsfase waren (1) de intrekking van beroeps- en cassatiezaken en (2) niet-ontvankelijkheid van het OM. Dat veel beroeps- en cassatiezaken worden ingetrokken voordat berechting plaatsvindt, is onder andere een strategie om tijd te winnen door de verdediging of vindt plaats omdat er behoefte is aan een uitgewerkt vonnis (Felix, 2013). Niet-ontvankelijkheid van het OM werd ook als ongewenst gezien door de Algemene Rekenkamer (2012). Onderliggende oorzaken zijn verjaring, gebrek aan kwaliteitsmanagement of niet-ontvankelijkverklaring als instrument voor de administratieve beëindiging van zaken.

Studies naar de afhandeling van online delicten door OM en ZM zijn er in mindere mate. In de studie van Leukfeldt *et al.* (2012) is van 647 politiedossiers uit de *Verkenning Cybercrime in Nederland 2009* (Leukfeldt *et al.*, 2010) achterhaald hoe de zaken door de politie zijn afgehandeld. Hieruit bleek dat 43,6% van de zaken was afgedaan door de politie, 30,1% doorgestuurd werd naar het OM en dat van 26,3% van de zaken onbekend was op welke wijze deze waren afgedaan. Het percentage dat destijds werd doorgestuurd naar het OM ligt daarmee beduidend lager dan bij traditionele criminaliteitszaken.

Meer inzicht in de wijze waarop online criminaliteitszaken vervolgens door het OM en de ZM worden afgedaan kan worden ontleend aan de studie van Boekhoorn (2019). Van het aantal zaken dat instroomt doet het OM de meeste zaken zelf af (58,2% in 2018), de rest wordt doorgestuurd naar de ZM (39,5% in 2018). Het blijkt dat het OM – bij beoordeling van de zaken in BOSZ – zaken online criminaliteit relatief vaak afdoet met een sepot (50,2% van de totale instroom bij het OM in 2018). Dit betreft meestal een technisch sepot (56,4% van de sepots), wat betekent dat het OM niet overgaat tot vervolging van een strafbaar feit omdat men verwacht dat vervolging niet tot een veroordeling zal leiden (CBS, 2021). Onvoldoende bewijs of niet-strafbaarheid van het feit of de verdachte kunnen bijvoorbeeld tot deze beslissing leiden. Verder is te zien dat de toename in het aantal online criminaliteitszaken bij het OM in 2018 meer dan verdubbeld is ten opzichte van 2015.

Ook het Centraal Bureau voor de Statistiek (CBS) beschikt over gegevens omtrent beslissingen die het OM en de ZM nemen inzake online criminaliteit, specifiek met betrekking tot het delict computervredebreuk[13] (CBS, 2017). Ook uit deze cijfers blijkt dat het OM een relatief hoog percentage

[13] Het CBS bevat slechts gegevens over het delict computervredebreuk en geen gegevens over (meerdere typen) online criminaliteit. Een mogelijke verklaring hiervoor zijn registratieverschillen tussen het OM en de politie. Zo bleek dat er in 2012 verschillen bestonden in de definities inzake cybercrime tussen de politie en het OM. Volgens het OM was cybercriminaliteit in ruime zin geen cybercrime (Leukfeldt *et al.*, 2012).

zaken afdoet met een sepot (49%), waarvan 46% van de sepots bestond uit een technisch sepot. Rechters besluiten in het gros van de 120 zaken die zij hebben behandeld tot schuldverklaring met straf (70,8%). Ook wordt er geregeld tot vrijspraak besloten (25%).

Er is verder weinig onderzoek dat dieper ingaat op de knelpunten in de doorstroom van zaken binnen het OM of de ZM. Het onderzoek van Leukfeldt *et al.* concludeerde in 2012 dat gespecialiseerde officieren van justitie op het gebied van online criminaliteit weinig of geen online criminaliteitszaken krijgen. Dit kwam enerzijds doordat het merendeel van de cyberzaken door de politie zelf werd afgehandeld en anderzijds doordat OM medewerkers gedigitaliseerde criminaliteit beoordeelden als klassieke delicten. Uit het onderzoek van Leukfeldt *et al.* (2012) bleek verder dat rechters geen knelpunten ervaarden in de afhandeling van online criminaliteitszaken. Wel kostten deze zaken meer tijd omdat de materie moet worden doorgrond, er weinig tot geen jurisprudentie is voor rechters en er beperkte richtlijnen zijn voor straftoemeting voor dergelijke delicten. Leukfeldt *et al.* (2012) merken op dat het de vraag is in hoeverre rechters onafhankelijke toetsing van bewijsvoering optimaal kunnen waarborgen, gezien de complexiteit en specialistische kennis die nodig is bij online bewijsvoering. Andere knelpunten omtrent de vervolging van online criminaliteit hebben te maken met wet- en regelgeving, bewijsvoering en de complexiteit van online criminaliteitszaken (Brown, 2015), zoals deze ook gelden voor de opsporing van online criminaliteit.

Interviews

Wanneer medewerkers bij het OM gevraagd wordt naar de doorstroom van online criminaliteitszaken, wijzen zij voornamelijk op knelpunten in de opsporing en dus bij de politie (deze knelpunten kwamen eerder al aan bod). Veel van de genoemde knelpunten – bijvoorbeeld een gebrek aan capaciteit of prioriteit – spelen volgens hen in de fase van vervolging geen rol meer. OM1 stelt dat sinds 2018 meer aandacht voor online criminaliteit bij het OM is gekomen. Ook is er volgens OM2 voor personele versterking op dit thema binnen het OM steeds meer geld beschikbaar. *"Dat is niet eens meer een prikkel te noemen, dat is gewoon plat gezegd 'je moet geld gaan uitgeven.' [..] Elk parket krijgt heel veel geld op jaarbasis, structureel, om het been bij te trekken"*, aldus OM2. Binnen een andere eenheid wordt gesteld dat zij momenteel nog te weinig zaken hebben om meer mensen op dit thema aan te hoeven nemen. Zij (OM3, OM4) verwachten wel dat zij indien nodig de parketleiding hierin mee zouden krijgen. OM3 is echter ook van mening dat nog te weinig mensen binnen het OM zich met online criminaliteit bezighouden. Zo stelt zij:

> *"Binnen [deze eenheid van] het OM zijn wij de enige drie die deze portefeuille hebben. Ik denk echt: hoe kan dat nou? Á la 2022, waarin zoveel strafbare feiten middels de digitale weg*

plaatsvinden? […] Het wordt echt als specialisme gezien, bijvoorbeeld net zoals 'afpakken', terwijl het eigenlijk van iedereen is. Ik vind dat het meer mensen eigen moet worden."

Een knelpunt dat volgens respondenten net als bij de politie wel bij het OM optreedt, is het bestaan van koudwatervrees. Zo zegt OM1: *"Dat zit hem gedeeltelijk in het onbekend zijn met de materie, het spannend vinden en terecht of onterecht ingewikkeld vinden. Maar als je je er niet in verdiept, dan kun je helemaal niet spreken van ingewikkeld."* Ook OM5 stelt dat hiervan sprake is en dat men bij het OM vooral met dit soort zaken aan de slag moet gaan om hier een beter begrip van te krijgen. *"Je kunt daar nog zoveel presentaties over krijgen, maar tachtig procent van die zaal gaat de volgende dag iets anders doen en een week later zit het nog ergens daar… Je moet het in de praktijk gaan brengen."* OM5 is bovendien van mening dat de huidige opleiding voor officieren "*op de schop moet*", omdat deze te diep gaat en erg specialistisch is. *"We moeten echt een soort basis voor de hele organisatie modulair gaan opbouwen."*

De geïnterviewde officieren benoemen verder dat zaken in de vervolgingsfase ongewenst kunnen uitstromen als gevolg van een gebrek aan strafrechtelijke haalbaarheid. Dit komt overeen met bevindingen uit de literatuur en heeft volgens respondenten deels te maken met de wijze waarop online criminaliteit (juridisch) gedefinieerd wordt. OM1 beschrijft dat het voor de *"gewone collega"* nog wel eens moeilijk is om onderscheid te maken tussen online criminaliteit in enge en brede zin. OM5 onderschrijft dit en geeft hiervan een concreet voorbeeld:

"VIN-fraude valt niet onder cybercrime [in enge zin], zoals ze in het Wetboek van Strafrecht staan. En dat is natuurlijk waar je op wordt afgerekend. Je wordt afgerekend op een 138ab of iets dergelijks. Dan heb je nog mensen die zeggen van 'ik heb hier een VIN-fraude', terwijl het een 1-cent-fraude blijkt te zijn, wat eigenlijk weer phishing is. Daarbij zie je dan vervolgens weer dat de credentials gebruikt worden om in te loggen, dan zit je weer bij de 138ab [strafbaarstelling computervredebreuk ofwel cybercrime in enge zin]. Dit soort dingen maken het erg lastig."

Hoewel enkel hier beschreven, vormt het op een bepaalde manier labelen en conceptualiseren van online criminaliteit een knelpunt dat ook door veel geïnterviewde medewerkers van de politie (n=12) is genoemd. Het knelpunt wordt gevormd doordat medewerkers binnen dezelfde organisatie (politie) of verschillende organisaties (politie en OM) niet op één lijn zitten. Politiemedewerkers zijn teleurgesteld als het OM een verdachte voor een ander feit vervolgd dan dat de politie voor ogen had en vice versa zijn OM'ers van mening dat feiten bij de politie niet altijd juist gelabeld worden, met gevolgen voor de doorstroom.

Tevens kunnen zaken uitstromen omdat het OM in plaats van dagvaarden kiest voor een alternatieve afdoeningswijze. OM1, OM4, P24 en P26 wijzen in dit verband om de "*knock-and-talk*"- of *"stop-*

gesprekken" die de politie regelmatig uitvoert, al dan niet met inbegrip van een verzoek of civielrechtelijke vordering tot het terugbetalen van de financiële schade en bemiddeling daarbij. Dergelijke interventies zijn volgens OM1 niet terug te zien in de gebruikelijke statistieken. Het wordt wel geregistreerd, namelijk in het systeem Landelijk Zicht Op Zaken (LZOZ), maar dit telt bijvoorbeeld niet mee in het aantal zaken dat het OM op jaarbasis dient af te ronden.

Deze *key performance indicators* (KPI's), ofwel streefdoelen omtrent het afronden van een bepaald aantal zaken, wordt tevens door de respondenten als knelpunt genoemd. Deze doelstellingen, vastgelegd in de Nationale Veiligheidsagenda, worden bepaald door de Minister van Justitie en Veiligheid na overleg tussen de politie- en OM-leiding en kunnen per eenheid verschillend zijn. Alle geïnterviewde officieren achten de gestelde doelen haalbaar, echter was dat lang niet altijd zo. OM2: *"Vier jaar geleden was dat echt een hoofdpijn-nummer. Daar kwamen we niet aan. We hadden toen nog maar acht FTE in het CCT en een CCT moet af en toe ook langdurigere onderzoeken kunnen draaien."* Voorts is OM1 van mening dat de focus door de KPI's te veel op kwantiteit in plaats van kwaliteit komt te liggen. Zo stelt zij:

> *"Je kunt wel meer zaken oppakken, maar volgens mij moet je de juiste zaken oppakken. Als mijn baas blij wordt van twintig streepjes die ik moet zetten, dan zoek ik twintig goedkope, eenvoudige streepjes, scoor ik die en is de baas blij. Maar heb ik dan iets gedaan wat zinvol is? Ik denk het niet."*

Daarnaast waren deze doelstellingen tot nu toe enkel gericht op online criminaliteit in enge zin. OM2: "Wij kunnen 200 Marktplaats-verdachten voor de rechter brengen, maar dat betekent niets voor waar wij uiteindelijk op worden afgerekend." Door OM5 wordt benoemd dat hier echter verandering in komt. In de nieuwe Veiligheidsagenda is volgens hem namelijk ook een resultaatverplichting opgesteld ten aanzien van gedigitaliseerde criminaliteit. "In de praktijk zie je dat gedigitaliseerde criminaliteitsonderzoeken eerder het onderspit delven op het moment dat je een weging gaat maken, want niemand werd hierop afgerekend. Vanaf dit jaar wordt dat anders, want anders haal je de Veiligheidsagenda niet", zo stelt hij.

Verschillende respondenten (OM2, OM5, OM6) gaan in op de specifieke doelstellingen die op basis van de Veiligheidsagenda moeten worden behaald:

> *"Wij moeten 33 cybercrimeverdachten per jaar voor de rechter brengen. Dat klinkt niet als een hoog aantal, maar soms doe je onderzoek en kom je nergens op uit. […] Mochten we de 33 dit jaar niet aantikken, dan kunnen we nog een beroep doen op een soort hardheidsclausule dat je ook nog alternatieve interventies kan meetellen. Deze mogen voor 25 procent worden meegeteld." (OM2)*

OM5 en OM6 voegen daaraan toe dat daarnaast op jaarbasis zo'n 42 fenomeenonderzoeken door alle eenheden gezamenlijk gedraaid moeten worden. Hier ziet het Landelijk Operationeel Cybercrime Overleg (LOCO) op toe. Binnen het LOCO worden projectvoorstellen gedeeld, welke vervolgens weer over de eenheden worden verdeeld, afhankelijk van welk team hier de ruimte en expertise voor heeft. OM6 legt dit verder uit: *"Binnen het LOCO is de afspraak gemaakt dat elk CCT zestig procent van hun capaciteit moet besteden aan zaken die landelijk worden opgewerkt, vanuit het LOCO zelf. De overige veertig procent dient te worden besteed aan lokale zaken."*

Zoals benoemd, wordt over het algemeen elke online criminaliteitszaak die door het OM bij de ZM wordt aangebracht, door de ZM opgepakt. De in dit onderzoek geïnterviewde rechters ervaren weinig knelpunten in de afhandeling van deze zaken, hetgeen overeenkomt met bevindingen uit eerder onderzoek. Ook stellen beide rechters dat er (tegen verwachtingen in) relatief weinig online criminaliteitszaken bij de ZM worden aangebracht en dat deze hoeveelheid dan ook goed te behappen is. Volgens R1 is wel sprake van koudwatervrees onder rechters, zowel ten aanzien van online criminaliteit in brede als in enge zin. *"Er is een beperkt aantal mensen dat dit leuk en interessant vindt. […] Het is voor veel mensen de onbekendheid. De meeste rechters zijn geen bèta's, dus die vinden dit soort dingen te ver van hun bed."* Ook rechters die affiniteit met online criminaliteit hebben, geven soms aan deze liever niet te behandelen. R1: *"En terecht, want het kost je meer tijd om de zaak eigen te maken, om te doorgronden waar het over gaat."* Wat volgens R1 met name lastig wordt gevonden, zijn de bewijswaardering en strafbepaling. R2 verwacht dat rechters in de beoordeling van dit soort zaken weinig moeite hebben met het bepalen van de strafmaat, aangezien hiervoor richtlijnen vanuit het OM en de ZM zijn opgesteld. De waardering van bewijs levert volgens hem wel problemen op. Zo stelt hij: *"Het probleem zit hem vooral in de eerdere fase. Hoe zien we de tenlastelegging? Wat begrijpen we uit het proces-verbaal? Hoe interpreteren we de verklaringen van deskundigen?"* Een goede opname van de aangifte is hiervoor van belang (zo bleek al uit de genoemde knelpunten rond de intake), maar hetzelfde geldt volgens R2 voor de kwaliteit van het proces-verbaal. *"Soms staat er 'de bestanden zijn opgeslagen op een niet-benaderbare locatie, punt.' Nou, dat kan jij als politieagent wel vinden, maar wij moeten dat ook vaststellen en daar hebben wij concrete gegevens voor nodig."*

Hoewel daders van online criminaliteit vaak meerdere feiten tegelijk ten laste wordt gelegd, heeft R1 echter niet de ervaring dat de behandeling van online criminaliteitszaken op zitting veel meer tijd kost dan traditionele zaken. Vertraging ontstaat volgens haar eerder doordat aanvullend onderzoek (door de politie, het Pieter Baan Centrum (PBC) of het Nederlands Instituut voor Forensische Psychiatrie en Psychologie (NIFP)) nog niet is afgerond, maar dit gaat net zo goed op voor traditionele delicten. R2 is wel van mening dat het grote aantal slachtoffers dat met online criminaliteit gepaard gaat terug te zien is in de duur van de behandeling van deze zaken door de ZM. Hij spreekt in dit verband over

"megazaken" die – afhankelijk van het aantal aangevers dat op zitting verschijnt – zo'n vijftien werkdagen in beslag kunnen nemen. Phishing biedt hiervan een veelvoorkomend voorbeeld:

> *"Dat zijn zaken met veel slachtoffers. Dat is enorm bewerkelijk. Zo hadden we zaken met wel 200, 300 benadeelde partijen. […] Gelukkig komen ze niet allemaal op zitting, soms zelfs helemaal niemand, wat dan ook weer merkwaardig is. […] Maar qua verwerking, administratief is het een enorme opgave. Het moet allemaal worden ingevoerd in [systeem x] en per benadeelde partij moeten allerlei beslissingen worden genomen. Over de vordering, de schadevergoedingsmaatregel, de wettelijke rente, dus dat kost veel tijd […] en beperkt onze capaciteit wel." (R2)*

Een van de LMIO-medewerkers heeft eenzelfde ervaring, hetgeen blijkt uit zijn beschrijving van een lopende zaak waarin zo'n 350 tot 400 aangiften zijn gedaan wegens het bestaan van een malafide webwinkel:

> *"Je hebt maar één verdachte, maar de omvang van de zaak en de hoeveelheid dossiers en pagina's bepaalt dan of het een megazitting wordt. Slachtoffers hebben geen spreekrecht, maar ze kunnen zich wel voegen in het strafdossier. Dat betekent dat zij hun voeging mondeling moeten toelichten. Dus daar moet je als rechtbank rekening mee houden. […] Wij zijn er als politie, OM en rechtelijke macht niet ingericht op dergelijke zaken."*

Desondanks ziet R2 dit niet als knelpunt voor de doorstroom van online criminaliteitszaken: "Dan kom je toch weer terug op: capaciteit is op zich ons probleem niet. We zouden meer cyberzittingen kunnen doen en zijn al blij als we deze zittingen op kunnen vullen, eigenlijk."

Resumé

Intake

Uit de literatuur blijkt dat de politie niet altijd een aangifte opneemt wanneer slachtoffers van online criminaliteit contact opnemen met de politie. Dat kan komen doordat intakemedewerkers denken dat het niet om een strafbaar feit gaat (bijvoorbeeld in hacking zaken), dat het om een civiele zaak gaat (bijvoorbeeld bij online fraude) of meer algemeen dat intakemedewerkers de ernst van het slachtofferschap als laag inschatten. Indien er wel een aangifte wordt opgenomen, dan lijkt het succesvol opnemen van een aangifte afhankelijk te zijn van het begrip en de kennis van de intakemedewerker die de aangifte van online criminaliteit opneemt. Deze kennis is echter niet altijd (voldoende) aanwezig bij intakemedewerkers.

Respondenten geven aan dat ze een gebrek aan kennis van online criminaliteit zien onder intakemedewerkers, terwijl juist een kwalitatief hoogstaande aangifte voor een succesvolle

doorstroom in de strafrechtketen zorgt. Een knelpunt is verder dat de aangifte ook afhankelijk is van (de kennis van) de aangever. Het 'verhaal' van de aangever is lang niet altijd helder. Burgers weten zelf ook niet altijd precies wat er is gebeurd. Des te belangrijker is het voor intakemedewerkers om de juiste vragen te stellen. Wel zijn er hulpmiddelen beschikbaar waarmee intakemedewerkers op basis van de criminaliteitsvorm kunnen opzoeken welke informatie uitgevraagd dient te worden, maar daarvoor is vereist dat medewerkers deze hulpmiddelen weten te vinden en dat zij weten om welke criminaliteitsvorm het gaat. Ten slotte wijzen respondenten er op dat er steeds vaker aangifte via internet wordt gedaan. Het geautomatiseerde aangifteproces via de website van de politie maakt het mogelijk om goed door te vragen op onderzoeksmogelijkheden (waaronder bankrekeningnummers).

Zowel de experts die deelnamen aan de discussiesessies als de internationale respondenten die geïnterviewd zijn herkennen het beeld dat naar voren kwam uit de literatuur en interviews. Tijdens de expertsessies werd meermaals gewezen op de belangrijke rol die intakemedewerkers spelen bij het leggen van een goede basis voor verder opsporingsonderzoek. Zonder de juiste informatie is de kans op vroegtijdig uitval volgens de experts groter.

Casescreening

Er is relatief weinig onderzoek dat zich richt op de casescreening van zaken online criminaliteit door de politie. Uit het onderzoek dat wel is gedaan ontstaat het beeld dat online criminaliteit zaken minder snel worden opgepakt dan traditionele zaken. Verklaringen hiervoor zijn dat de afhandeling van dergelijke zaken veel tijd kost, een gebrek aan capaciteit, het internationale karakter van online criminaliteit en de kwaliteit van de opgenomen aangiften. Zaken waarin belangrijke informatie ontbreekt worden tijdens de casescreening minder snel in behandeling genomen.

Uit de interviews komen verschillende redenen naar voren waarom zaken van online criminaliteit binnen het screeningsproces uitvallen. De belangrijkste reden die door respondenten wordt genoemd is het gebrek aan opsporingsindicatie en meer concreet het ontbreken van een verdachte. Hoewel dit geen uniek probleem is, speelt dit volgens respondenten in het bijzonder bij online criminaliteit, omdat daders zichzelf en de illegaal verkregen inkomsten makkelijker en effectiever kunnen afschermen. Daarbij blijkt het voor online criminaliteit lastiger dan voor traditionele criminaliteit in te schatten of een zaak voldoende opsporingsindicatie bevat. Voor het al dan niet oppakken van een zaak speelt ook de financiële schade een rol. Is sprake van een 'gering' schadebedrag dan wordt een zaak niet opgepakt. Wat precies met 'geringe schade' wordt bedoeld verschilt volgens de respondenten echter tussen eenheden, maar ook tussen districten en basisteams. Het kan ook een reden zijn om een zaak uit te screenen, als blijkt dat de financiële schade van een slachtoffer al is vergoed, bijvoorbeeld door een bank.

Opsporing

Ook wanneer wordt besloten om een zaak op te pakken, kunnen er verschillende redenen zijn waarom een zaak tijdens de opsporing alsnog uitstroomt. Uit de literatuur komen vier factoren naar voren die de opsporing van online criminaliteit bemoeilijken. Ten eerste wordt het gebrek aan prioriteit binnen politieorganisaties genoemd, wat onder meer versterkt wordt door de complexiteit van deze opsporingszaken en het beperkte bewustzijn van de risico's van online criminaliteit. Ten tweede bestaat er te weinig kennis en vaardigheden onder politiemedewerkers om opsporingsonderzoeken inzake online criminaliteit (effectief) op te pakken. Ten derde komt uit de literatuur naar voren dat ook bij de opsporing te weinig capaciteit aanwezig om online criminaliteit op te pakken, waarbij politiemedewerkers met specialistische kennis moeilijker binnen de politieorganisatie te behouden zijn. Tot slot geldt dat de complexiteit van online criminaliteit de opsporing van daders verder bemoeilijkt. Dit komt bijvoorbeeld door het internationale karakter van online criminaliteit, maar ook door de vluchtigheid van digitale gegevens en het idee dat daders zich makkelijker via het internet en computerprogramma's kunnen verschuilen.

De knelpunten die in de literatuur worden benoemd, zijn op soortgelijke wijze teruggekomen tijdens de interviews en worden ook benoemd in de discussiesessie: een gebrek aan prioriteit, een gebrek aan kennis, een gebrek aan capaciteit en de complexiteit van online criminaliteitszaken. Voor wat betreft het gebrek aan prioriteit werd door respondenten vooral gesproken over de gepercipieerde lagere (sociale) impact van online criminaliteit, hoewel dit door een deel van de respondenten als onterecht wordt beschouwd. Algemeen gesteld lijken de werkprocessen van de politieorganisatie nog voornamelijk te zijn ingericht op traditionele vormen van criminaliteit. Heterdaadsituaties, bijvoorbeeld bij winkeldiefstallen, krijgen voorrang op online criminaliteit zaken. Tegelijkertijd dient te worden opgemerkt dat de afgelopen jaren een duidelijke kentering zichtbaar is, waarbij verschillende teams speciaal zijn ingericht op het opsporen van online criminaliteit. Voor wat betreft het gebrek aan kennis, wordt door respondenten gewezen op het idee dat met name (maar niet uitsluitend) de wat oudere collega's minder open staan voor het eigen maken van nieuwe kennis over online criminaliteit. Volgens respondenten wordt online criminaliteit door collega's nog vaak (onterecht) als iets ingewikkelds gezien. Op papier wordt in toenemende mate prioriteit gegeven aan het aanpakken van online criminaliteit. Dit komt in de praktijk onder andere tot uiting via het oprichten van verschillende specialistische cyberteams. Ondanks deze verbeteringen geeft het overgrote deel van de respondenten aan dat zowel de basisteams, de districtsrecherches als de cybercrimeteams, om verschillende redenen, kampen met een capaciteitsgebrek.

Tijdens de interviews wordt ook genoemd dat de opsporing van online criminaliteit complex is en dat deze complexiteit een knelpunt kan vormen voor de goede doorstroom hiervan. Alle factoren die online criminaliteit complex (kunnen) maken en in de literatuurstudie werden genoemd, werden ook tijdens de interviews genoemd. Veruit het meest genoemd was het internationale karakter van online criminaliteit en de perceptie dat het verkrijgen en behouden van digitaal bewijs lastig is door de vluchtigheid van gegevens in de online wereld, bijvoorbeeld wanneer het gaat om IP-adressen of informatie op servers. Daarnaast benoemen respondenten dat de politie als gevolg van wet- en regelgeving (met name omtrent privacy) vaak over onvoldoende opsporingsmogelijkheden beschikt om digitaal bewijs veilig te kunnen stellen. In aanvulling op de literatuur wijzen respondenten ook nog op het potentieel grote aantal slachtoffers dat met online criminaliteit gepaard gaat en de mogelijkheid dat slachtoffers vaak niet binnen dezelfde eenheid woonachtig zijn. Ook de snelheid waarmee nieuwe vormen van online criminaliteit ontstaan draagt bij aan de complexiteit ervan.

Tot slot is aan bod gekomen dat het internationale karakter van online criminaliteit en het feit dat er vaak veel verschillende slachtoffers in meerdere eenheden zijn een gebrek aan eigenaarschap in de hand kan werken. Wanneer niet duidelijk is aan welk opsporingsteam een zaak toebehoort, kan dit er toe leiden dat een zaak niet wordt opgepakt. Ook komt het voor dat een zaak door meerdere teams tegelijkertijd wordt opgepakt, zonder dat zij dat van elkaar weten.

De internationale respondenten schetsen eenzelfde beeld als de Nederlandse respondenten. Alhoewel het per land verschillend is, lijkt de situatie in zowel het VK, VS en Australië zelfs nog complexer door de veelheid van lokale politieregio's en de organisatie van de politie op federaal en statelijk niveau. Respondenten geven bijvoorbeeld aan dat het voor casescreeners lastig kan zijn om te bepalen waar een zaak 'gedraaid' moet worden omdat in veel gevallen lokale politiediensten zijn die een zaak kunnen oppakken, maar dat er ook landelijk opererende teams zijn die zich richten op georganiseerde misdaad en/of fraude en cybercrimes inmiddels ook in hun takenpakket hebben. Als een zaak dan naar een 'verkeerd' team gaat, dan is de kans volgens respondenten groot dat die nooit wordt opgepakt.

OM en ZM

Er bestaat weinig onderzoek dat ingaat op de knelpunten in de doorstroom van zaken binnen het OM of de ZM. In 2012 werd door Leukfeldt *et al.* nog geconcludeerd dat gespecialiseerde officieren van justitie op het gebied van online criminaliteit weinig of geen online criminaliteitszaken krijgen. Dit kwam enerzijds doordat het merendeel van de cyberzaken door de politie zelf werd afgehandeld en anderzijds doordat OM medewerkers cybercriminaliteit in ruime zin beoordeelden als klassieke delicten. Verder leken in dat onderzoek rechters geen knelpunten te ervaren in de afhandeling van online criminaliteitszaken, hoewel ze wel meer tijd kosten om goed te kunnen doorgronden. Andere

knelpunten omtrent de vervolging van online criminaliteit zijn hetzelfde als voor de opsporing, en hebben te maken met wet- en regelgeving, bewijsvoering en de complexiteit van online criminaliteitszaken.

Opvallend is dat alle respondenten aangeven dat het merendeel van de knelpunten bij de politie ligt en in mindere mate bij OM en ZM. Over het algemeen wordt ook gesteld dat er bij OM en ZM minder problemen zijn op het gebied van capaciteit als het gaat om de afhandeling van online criminaliteit. Ook is het duidelijk dat online criminaliteit prioriteit heeft. Dat wil overigens niet zeggen dat er – met name bij het OM – buiten de politie geen knelpunten benoemd zijn. Zo geven respondenten bijvoorbeeld wel aan dat ook bij het OM – en in mindere mate ook ZM – er sprake is van digitale koudwatervrees. De onbekendheid met online criminaliteit en de perceptie van technische ingewikkeldheid spelen hierbij volgens respondenten een rol. Een punt dat enkele malen tijdens de interviews aan bod kwam en ook door experts tijdens de discussiesessies werd benoemd is dat er wel knelpunten zijn door de gehanteerde definities van online criminaliteit. Streefdoelen van het OM met betrekking tot online criminaliteit zouden met name betrekking hebben op cybercrimes in enge zin. Vormen van gedigitaliseerde criminaliteit kunnen daardoor eerder buiten de boot vallen volgens respondenten en experts. Dit komt overeen met bevindingen uit de literatuur en heeft volgens respondenten deels te maken met de wijze waarop online criminaliteit (juridisch) gedefinieerd wordt. Tenslotte geven zowel respondenten als experts tijdens de discussiesessie aan dat zaken kunnen uitstromen omdat het OM in plaats van dagvaarden kiest voor een alternatieve afdoeningswijze zoals '*knock-and-talk'*- of 'stop'-gesprekken. Dergelijke interventies zijn volgens respondenten en experts niet terug te zien in de gebruikelijke statistieken.

6. Verbetermogelijkheden volgens de literatuur, actoren binnen de strafrechtketen en experts uit binnen- en buitenland

Inleiding

In dit hoofdstuk beschrijven we de verbetermogelijkheden binnen de in- en doorstroom van online criminaliteit binnen de strafrechtketen. Dat doen we op basis van een analyse van de literatuur, aangedragen oplossingen van de 34 door ons geïnterviewde respondenten die werkzaam zijn binnen de strafrechtketen in Nederland, interviews met vijf internationale experts en de discussiebijeenkomst met vijf experts waarmee we gereflecteerd hebben op de resultaten van dit onderzoek (meer over de gebruikte methoden in hoofdstuk 2). Omdat de interviews plaatsvonden voordat de resultaten uit de kwantitatieve analyses beschikbaar waren, kunnen geen directe links worden gelegd tussen de in- en doorstroomcijfers uit hoofdstuk 4 en de door de respondenten genoemde verbetermogelijkheden. We beschrijven de verbetermogelijkheden per stap in het proces van in- en doorstroom (zie hoofdstukken 3 en 4). Het hoofdstuk eindigt met een resumé waar we de belangrijkste bevindingen samenvatten en tevens de reflecties daarop van internationale experts toevoegen.

Geen instroom

Literatuur

In de literatuur worden enkele suggesties gedaan om de aangiftebereidheid onder slachtoffers van online criminaliteit te verhogen. Een eerste aanbeveling betreft het inzetten van publieke bewustwordingscampagnes waarin de noodzaak wordt benadrukt om online criminaliteit te melden bij de politie (Moitra, 2005; Bossler & Holt, 2012; Bidgoli & Grossklags, 2016). Dergelijke campagnes zouden meer kennis en bewustzijn moeten bijbrengen over mogelijkheden om aangifte te doen. Uit een eerdere studie bleek bijvoorbeeld dat studenten in de Verenigde Staten niet wisten hoe zij formeel aangifte moeten doen van online criminaliteit (Bidgoli *et al.*, 2016). Het is nog onduidelijk of campagnes voor online criminaliteit zich op een ander publiek dienen te richten dan campagnes om aangiften van traditionele criminaliteit te stimuleren, aangezien er nog geen consensus bestaat over de rol van demografische factoren in de meldingsbereidheid bij online criminaliteit (Van de Weijer *et al.*, 2019; Van de Weijer *et al.*, 2020).

Een andere suggestie is om uniforme en gedegen aangiftesystemen op te zetten (Brown, 2015), bijvoorbeeld in de vorm van online aangiftesystemen (Cross, 2018; Bidgoli *et al.*, 2019). Zo zouden online aangiftesystemen de aangiftebereidheid van gebruikers om aangifte te doen van online

criminaliteit verhogen (Bidgoli *et al.*, 2019). In Australië is bijvoorbeeld een online aangiftesysteem ontwikkeld speciaal voor online criminaliteit (Morgan *et al.*, 2016; Cross, 2018). Dit systeem – genaamd 'CyberReport' (voorheen ACORN) – dient het voor slachtoffers gemakkelijker en toegankelijker te maken om aangifte te doen van online criminaliteit. Een evaluatie van het systeem laat zien dat gebruikers grotendeels tevreden zijn over de gebruiksvriendelijkheid van het systeem, maar grotendeels ontevreden over de uitkomsten van de aangifte omdat deze niet altijd voldeed aan hun verwachtingen (Morgan *et al.*, 2016). Daarnaast heeft driekwart van de personen die aangifte deed preventieadvies gelezen dat werd aangeboden tijdens het doorlopen van het systeem. Dit advies werd door gebruikers beoordeeld als gemakkelijk te begrijpen en relevant. Verder leidde het systeem tot een toename in het aantal aangiften dat werd ontvangen en behandeld en tot een verbeterde intelligence positie bij de politie (Morgan *et al.*, 2016). Of het opzetten van een online aangiftesysteem daadwerkelijk tot een verhoogde aangiftebereidheid kan leiden blijft onduidelijk. Van de Weijer *et al.* (2020) laten namelijk zien dat het aantal aangiftemogelijkheden bij de politie geen invloed heeft op de intentie van personen om aangifte te doen van online criminaliteit.

Tenslotte wordt in de literatuur geopperd om de opportuniteitskosten (tijd, moeite en financiële kosten) voor het doen van aangifte te verminderen en de waargenomen voordelen van het aangifteproces te verhogen (Bidgoli & Grossklags, 2016; Kemp, 2020). Zo zouden slachtoffers tijdens het aangifteproces kunnen worden voorzien van cijfers over slachtofferschap van online criminaliteit, online preventie tips of informatie over stappen die de politie onderneemt tegen online criminaliteit (Bidgoli & Grossklags, 2016). Ook informatie met betrekking tot oplossingspercentages, aantal afgeronde zaken of de status van de desbetreffende zaak kunnen worden aangeboden aan slachtoffers (Kemp, 2020). Dergelijke informatie zou de perceptie van slachtoffers en hun omgeving omtrent het doen van aangifte positief kunnen beïnvloeden, waardoor toekomstige slachtoffers mogelijk eerder zijn geneigd om aangifte te doen.

Intake en casescreening

Literatuur

Om de eerdergenoemde knelpunten in de intake van aangiften online criminaliteit te kunnen verbeteren, wordt aanbevolen om training op maat te geven aan intake- en servicemedewerkers (De Paoli *et al.*, 2020). Het is belangrijk dat intakemedewerkers slachtoffers van online criminaliteit serieus nemen en niet onverschillig reageren wanneer zij melding doen bij de politie (Cross *et al.*, 2016; Leukfeldt *et al.*, 2018; Van de Weijer *et al.*, 2020). Verder adviseert Boekhoorn (2019) om het intakeproces te verbeteren door bijvoorbeeld (1) een technische aanpassing van de 'query' (in de vorm

van '*tekst mining*' en '*machine learning*') zodat meer aangiften online criminaliteit worden herkend, (2) door een aparte helpdesk in te stellen vanuit een regionaal cybercrimeteam voor intake- en servicemedewerkers en (3) door aanvullende scholing. Om de casescreening van aangiften online criminaliteit te verbeteren is in de politie-eenheid Noord-Holland een 'Cybercenter' ingericht binnen een regionaal cybercrimeteam (Boekhoorn, 2019). Dit is een 'hulploket' dat op basis van expertise de aangiften screent, veredelt en vervolgens 'panklaar' neerlegt voor basisteams. Verdere aanbevelingen omtrent de casescreening ontbreken in de literatuur.

Interviews

Zoals eerder beschreven, blijkt uit de interviews dat het aangifteproces als een belangrijke stap in het proces van in- en doorstroom van online criminaliteit wordt gezien. Zeker 11 respondenten bevelen dan ook aan online criminaliteitszaken niet enkelvoudig te benaderen (op basis van één aangifte), maar om aangiften te clusteren. Respondenten zijn van mening dat deze aangiften ten behoeve van een betere doorstroom het beste gecentraliseerd ofwel landelijk kunnen worden verzameld en gescreend. Hoewel wordt genoemd dat dit waarschijnlijk makkelijker zal zijn voor online criminaliteit in brede zin dan online criminaliteit in enge zin (P18, OM1), wordt door andere respondenten hier geen onderscheid in gemaakt.

Er worden verschillende redenen aangedragen voor het belang van clusteren in dit soort zaken. In de eerste plaats wordt genoemd dat een groter aantal aangiften meer data over bijvoorbeeld verdachten oplevert en om die reden de opsporingskansen vergroot (P15). Ook kan op deze manier worden ondervangen dat aangiften met een (te) laag schadebedrag niet worden opgepakt, omdat zo beter zichtbaar wordt dat dezelfde verdachten veel meer schade hebben berokkend dan op basis van afzonderlijke aangiften kan worden opgemerkt (P3, P4, OM1). Het kan volgens respondenten tevens de efficiëntie van het politiewerk vergroten (P15, OM1) en het mogelijk maken om trends te signaleren en op basis daarvan de prioriteit te bepalen (bijvoorbeeld welke aangiften als eerste moeten worden opgepakt) (P8). Daarbij werd ook het belang van geautomatiseerde dataverrijking en -analyse genoemd (OM1), met name omdat online criminaliteit minder tot de verbeelding spreekt. Waar het bij traditionele criminaliteit gemakkelijker is om zaken op basis van informatie te koppelen – denk aan overvallen waarbij steeds drie jongens worden gezien, waarbij een van hen altijd rode schoenen draagt – is dat bij online criminaliteit lastiger volgens respondenten. Zo stelt OM1: *"Er is niemand die denkt: 'oh, dat IP-adres heb ik al een keer eerder zien staan' of 'dat Mac-adres, telefoon- of bankrekeningnummer ken ik…' De analyse van aangiften moet dus op een heel andere manier worden aangevlogen."*

Een belangrijke reden die wordt gegeven voor het gecentraliseerd verzamelen en screenen van online criminaliteit, is dat volgens respondenten noodzakelijkerwijs iemand de regie moet nemen en dat dat momenteel niet gebeurt. Hoewel Nederland over een Nationale Politie beschikt, spreken respondenten (P5, P9, P14, P21, P23) over allerlei 'eilandjes' en 'compartimenten' die nog te veel afzonderlijk het wiel aan het uitvinden zijn. Een betere samenwerking en communicatie tussen opsporingsteams zou de doorstroom van online criminaliteit volgens hen bevorderen. Daarnaast wordt gesteld (P15) dat basisteams – aan wie dit soort zaken momenteel vaak worden toegewezen – simpelweg niet zijn ingericht om zaken te clusteren en complexe onderzoeken 'te draaien'. Hoewel niet genoemd, kan tevens verwacht worden dat een gecentraliseerde aanpak het probleem omtrent 'eigenaarschap' wordt opgelost. Indien een cluster van aangiften aan een specifiek team wordt toegewezen, wordt immers duidelijk wie verantwoordelijk is voor het oppakken van deze zaak, waardoor niet twee of meer teams zich met dezelfde zaak bezig zullen houden en het bovendien minder makkelijk wordt om een zaak aan een ander opsporingsteam toe te wijzen. Voorts zou een centrale screening betekenen dat elke zaak op basis van dezelfde indicatoren wordt gescreend, hetgeen bijdraagt aan een uniforme werkwijze.

In lijn met het centraal verzamelen en screenen van online criminaliteitszaken, wijzen meerdere respondenten op bestaande initiatieven zoals het LMIO, de ECTF en Operatie Centurion. Het is hierbij van belang te benoemen dat het LMIO zich zoals eerder benoemd slechts op één vorm van online criminaliteit in brede zin richt (online aan- en verkoopfraude), dat Operatie Centurion in de meeste eenheden nog een toekomstig initiatief betreft en dat de ECTF volgens enkele respondenten nog onvoldoende lijkt te worden benut. In het geval dat de clusters van aangiften uiteindelijk weer aan de basisteams of districtsrecherches worden toegewezen, komt daar bij voor dat de eindverantwoordelijkheid voor het oppakken van deze zaken bij de opsporingsteams ligt. Dit zal ertoe leiden dat zaken alsnog niet succesvol doorstromen, mits aandacht wordt besteed aan andere knelpunten in de doorstroom (waaronder het gebrek aan capaciteit en prioriteit).

De twee respondenten uit de eenheden waar Centurion al is geïnitieerd, zijn op het moment van interviewen erg positief. Zaken worden eerder opgepakt en de informatieverstrekking door andere partijen (zoals de ECTF) is verbeterd, zo stelt P14. Verwachtingen van respondenten uit andere eenheden zijn wisselend. Enerzijds is de verwachting positief: deze werkwijze zou de opsporing kunnen versnellen en het helpt bij het in kaart brengen van het 'lokale daderschap'. P17: "*Het lijkt mij prettig als je bij de start van een zaak al weet dat de verdachte in jouw werkgebied woont. […] Je weet dan wie zich daarmee bezighouden en het spreekt meer tot de verbeelding als je weet wie het zijn*." Anderen (P11, P12, P16, P17, P20) zijn ongerust over het vrijblijvende karakter van het oppakken van dergelijke zaken. Verplicht oppakken is volgens P11 ook niet te doen. Zo stelt hij:

“Wij hebben al gezegd dat hij [de projectleider] vist in de vijver van zaken die toch vroegtijdig beëindigd worden. Hoe wil je dat ooit aan de basisteams gaan verplichten? […] Die [zaken] komen allemaal in die lijst terecht van tachtig zaken en dan mag jij raden welke zaken vroegtijdig worden beëindigd. Cyberzaken. Ik geef het je op een briefje: ook al is het goed bedoeld, als de verplichting op het basisteam rust, dan worden er keuzes gemaakt om het niet op te pakken. Dat wordt een lastige en daar maak ik mij grote zorgen over." (P11)

P17 en P20 zijn van mening dat bovenstaande werkwijze – indien het oppakken aan de basisteams behouden blijft - in ieder geval meer sturing en gekwalificeerd personeel vereisen dan hier momenteel beschikbaar voor is. De nieuwe werkwijze van het LMIO, ‘LMIO 2.0’, betreft volgens LMIO-medewerkers een goed voorbeeld van een mogelijkheid om beter op dergelijke zaken te sturen. Waar voorheen de aangiftemodule in BVH-systeem van de Landelijke Eenheid nog niet was gekoppeld aan het registratieve systeem BOSZ, is dat inmiddels wel het geval. Het gevolg (P26): “*Het is mogelijk dat men de verantwoordelijk dan nog niet voelt, maar dan kun je er in ieder geval op sturen en op bevraagd worden, zo van ‘waarom doe je het wel of niet?’”*

In de derde plaats wordt aangegeven dat de komst van Centurion naar verwachting in ieder geval betere resultaten zal opleveren in vergelijking met de huidige aanpak (P16, P17, P20). Volgens P20 is het in ieder geval de moeite waard om te verkennen of het werkt. “Er moet iets veranderen, want dit [de huidige aanpak] werkt niet” (P20). P17 legt ook uit waarom:

"We zijn nu allemaal vaak individueel bezig. Terwijl er overal visjes uitgegooid worden. Wij hebben een slachtoffer, maar dat bankrekeningnummer wordt misschien wel tien keer bevraagd in heel Nederland. Uiteindelijk komen we uit bij een verdachte die in [stad] woont. Voor ons is het een enkelvoudige zaak, maar er hangen nog tien aangiftes aan. Dat is gewoon onwerkbaar en niet efficiënt. En ook zonde van alle inspanningen." (P17)

Tenslotte wordt het belang van informatie-uitwisseling met externe partijen zoals banken, telecombedrijven en webwinkels genoemd. Meerdere respondenten merken op dat deze partijen ook een grotere rol in het aangifteproces zouden kunnen spelen, bijvoorbeeld door slachtoffers meer te stimuleren aangifte te doen, informatie proactief te delen met de politie of met aangevers of door zelf aangifte te doen bij de politie (P2, P5, P10, P11, P12, P14, P15, P16, P17, P21, OM3). Dergelijke partijen zijn vaak namelijk zelf ook slachtoffer, bijvoorbeeld wanneer zij de schade aan het slachtoffer (dienen te) vergoeden.

Opsporing

Literatuur

Omtrent de opsporing van online criminaliteit kan het geven van trainingen aan rechercheurs zorgen voor meer commitment. Een studie van Lee *et al.* (2019) laat namelijk zien dat een training over online criminaliteit ervoor zorgde dat rechercheurs bewuster werden over de mogelijke ernst van deze vormen van criminaliteit en meer geneigd waren om een onderzoek in te stellen. Struiksma *et al.* merkten in 2012 op dat destijds de vereiste expertise op operationeel niveau niet complex was en dat kennis zich vooral diende te richten op het karakter van online criminaliteitsvormen en het aanreiken van routes naar andere afdelingen binnen de politieorganisatie die over specialistische kennis beschikken. Een andere aanbeveling is om opsporingsteams te versterken met mensen van buiten de politie (Harkin *et al.*, 2018; De Paoli *et al.*, 2020), aangezien sommige burgers over meer expertise beschikken op het gebied van online criminaliteit dan traditionele politiemedewerkers. Verder merken studies op dat er meer (inter-)nationale samenwerking nodig is tussen opsporingsinstanties zodat kennis over online criminaliteit, forensische methodes en opsporingstechnieken kunnen worden uitgewisseld (Brown, 2015; Boekhoorn, 2019). Op nationaal niveau is samenwerking tussen cybercrimeteams in Nederland nog beperkt en richten zij zich vooral op hun eigen werkgebied, terwijl men wellicht beter op een landelijk niveau deskundigheid kan opbouwen (Boekhoorn, 2019).

Interviews

Aangezien daders van online criminaliteit vaak meerdere slachtoffers tegelijkertijd maken, geven respondenten aan dat het soms lijkt alsof er eindeloos veel aangiften aan elkaar kunnen worden gekoppeld. Een eerste punt voor verbetering aangaande de fase van opsporing die door zowel respondenten bij de politie als het OM (n=7) wordt genoemd, houdt in dat het recherchewerk niet eindeloos door hoeft te gaan. P17 spreekt in dit geval van ‘slimmer opsporen’, waarmee de respondent doelt op het uitvragen van alleen het benodigde bewijsmateriaal – in plaats van ál het bewijsmateriaal. Volgens P14, P16 en P17 is dit bij online criminaliteit júist van belang, aangezien hier veel meer soorten bewijs kunnen worden verzameld dan het geval is bij traditionele delicten, waar dit zich meestal beperkt tot fysieke sporen op de plaats delict, getuigenverklaringen en camerabeelden. Ook moet de politie *“durven te stoppen”* op het moment dat een opsporingsonderzoek nergens op uit dreigt te lopen (P15).

Dergelijke keuzes betreffen volgens OM2 een kosten-baten-overweging: “Wat je er in stopt, aan tijd en capaciteit, versus de output, wat gaat het ons opleveren? Gaat iemand een wezenlijk hogere straf krijgen? Gaat het iets betekenen voor de aangevers?” Een andere respondent bij het OM stelt ook dat men vooral het doel voor ogen moet houden.

> *Op een gegeven moment moet je gewoon keuzes maken. We gaan tot zover, punt. Komt er weer iets nieuws, dan maken we daar weer een nieuw onderzoek van. Ik denk dat het anders eigenlijk ook z'n doel voorbij schiet. Voordat je dan eens een keer zo'n zaak op zitting krijgt, heb je weer veel meer tijd nodig. Dan krijg je advocaten met allerlei onderzoekswensen. Hoe overzichtelijker je het houdt, hoe effectiever je dan op kan treden." (OM3)*

Tot slot benadrukt P15 dat niet gedacht hoeft te worden dat het uitgevoerde werk voor niets is geweest: *"Als iets in de koelkast gaat, wil dat niet zeggen dat het er nooit meer uit kan komen."*

Een ander punt van verbetering dat door de respondenten genoemd wordt, is dat een meer proactieve aanpak gewenst is. Respondenten benoemen dat opsporingsinstanties momenteel vooral reactief te werk gaan en omschrijven dit als *'pleisters plakken'* (P10) en *'mosterd na de maaltijd'* (P15). In plaats van te wachten op aangiften, zou de 'blauwe politiemedewerker', ofwel de politieambtenaar in de operatie alerter kunnen zijn op signalen die duiden op online criminaliteit. Hierbij worden verschillende voorbeelden genoemd. Vijf respondenten (P3, P4, P11, P12, P13) benadrukken dat jongeren die meerdere telefoons en/of bankpassen bezitten een mogelijk signaal zou kunnen afgeven. Volgens P13 wordt in dit geval onterecht meestal aan drugscriminaliteit gedacht. In het geval van online criminaliteit in brede zin komt het bovendien regelmatig voor dat daders fysiek op pad gaan, bijvoorbeeld om bij een slachtoffer geld of een bankpas op te halen, een pakketje te onderscheppen of op te halen op een afhaalpunt of om geld op te nemen bij een pinautomaat. Dit soort situaties verhogen de kans op heterdaad-situaties, zo stelt P16.

In dit verband wordt ook gewezen op de rol van andere actoren, zoals bedrijven die beschikken over een openbaar wifi-netwerk (P14) (zij kunnen opmerken wanneer iemand op regelmatige momenten van dit netwerk gebruik komt maken) en vakantieparken (P16) (wanneer een grote hoeveelheid telefonische apparatuur wordt aangetroffen). Hoewel 'het blauw' volgens respondenten (P9, P17, P20, P21) minder geïnteresseerd is in online criminaliteit, toont een voorbeeld dat P16 geeft aan dat de opsporing van deze feiten niet saai hoeft te zijn en ook ergens in de fysieke wereld plaatsvindt:

> *"Daar waren de hoofddaders live bezig. Zij zaten met acht man in een vakantiehuisje. We vielen dat hok binnen, iedereen rennen, maar allemaal vastgepakt! Er was echt een rolverdeling, dat kun je gewoon een criminele organisatie noemen. ABN-sprekende meisjes die de hele dag aan het bellen zijn, AnyDesk stond open en de bad guys zaten hun geld te tellen. Dat was net een film."*

Ook wijzen respondenten (n=7) op de rol van financiële instellingen. Banken zijn er volgens respondenten het snelste bij, want zij kunnen op het moment van de transactie zien hoeveel er wordt overgeboekt, naar wie het bedrag wordt overgemaakt, bij welke pinautomaat het geld wordt

opgenomen en zelfs via welk apparaat er op de bankrekening wordt ingelogd. Enkele respondenten (P5, P12, P17) zijn van mening dat banken (nog) vaker rekeningen blokkeren in het geval van een opmerkelijke transactie. P17 benadrukt hierbij ook de keuze van banken om in onderlinge samenwerking directe overboekingen mogelijk te maken. In 2016 was het volgens deze respondent nog mogelijk om bij een fraudemelding direct beslag te leggen op de tussenrekening, waardoor het geld terug kon worden geboekt wanneer inderdaad sprake was van een frauduleuze overboeking. Tegenwoordig kunnen mensen binnen één minuut geld naar elkaar overmaken, met als het gevolg dat het geld vaak allang is weggesluisd wanneer de politie hier achteraan gaat.

Daarnaast wordt ook bij deze stap binnen het proces door respondenten het belang van informatie-uitwisseling met externe partijen benadrukt. Behalve banken kan gedacht worden aan gemeenten, cybersecuritybedrijven, telecombedrijven, advertentiewebsites (zoals Marktplaats), webwinkels (waaronder Bol.com en Wehkamp) en online betaaldiensten (denk aan Klarna en Afterpay). Dergelijke partijen beschikken volgens respondenten over relevante informatie die binnen zowel het aangifteproces als de opsporing ten goede zouden komen wanneer deze vaker met de politie gedeeld zou worden. Er wordt door respondenten gesteld dat dergelijke partijen momenteel weinig of geen belang hebben in een meer proactieve rol of betere informatie-uitwisseling. Respondenten zijn van mening dat zij niet of nauwelijks getroffen worden. Zo stelt P16:

> *"Wat mij enorm verbaast, is dat op geen enkele politieke agenda staat en dat mega veel schadebedragen gewoon door de bank vergoed worden. […] De kosten wegen niet op tegen de baten. Het raakt ze gewoon niet. Ze maken de betaalpas gewoon een euro duurder."*

Volgens een andere respondent hebben banken zelfs baat bij een niet-proactieve houding aangezien zij zoals eerder beschreven geld ontvangen voor elke vordering die de politie bij hen doet. *"Wij spekken de kas",* aldus P21. P17 bevestigt het laatstgenoemde met de volgende uitspraak: *"Ik weet dat ze 300 euro per vordering krijgen dus ik snap dat ze dat in stand willen houden. Het is gewoon een verdienmodel voor banken. Zij verdienen er flink op, maar het zou juist andersom moeten werken."*

OM en ZM

Literatuur

Door het beperkte aantal studies omtrent de in- en doorstroom van online criminaliteit bij het OM en de ZM, ontbreken aanbevelingen omtrent deze fasen in de strafrechtketen. Wel adviseert Brown (2015) om aanklagers nauw samen te laten werken met medewerkers op de plaats delict, zodat rechtbanken kunnen worden voorzien van uitgebreide en nauwkeurige aanklachten.

Sommige aanbevelingen die in de literatuur worden genoemd om de in- en doorstroom van online criminaliteit te verbeteren hebben betrekking op meerdere fasen in de strafrechtketen of zelfs de gehele strafrechtketen. Zo wordt aanbevolen om lange termijnplannen te maken om vaardigheden van medewerkers te verbeteren, aangezien kennis van online criminaliteit snel veroudert (Harkin *et al.*, 2018). Daarnaast kan de effectiviteit van trainingen worden verbeterd door trainingen interactief en meer 'to the point' te laten zijn (Hadlington *et al.*, 2018). Een andere suggestie is om duidelijke en uniforme definities te creëren binnen de strafrechtketen – maar ook internationaal – omtrent (slachtofferschap van) online criminaliteit (Moitra, 2005; Brown, 2015; Bidgoli & Grossklags, 2016; De Paoli *et al.*, 2020). Ten slotte wordt aanbevolen aan strafrechtsketenorganisaties om actief samen te werken met andere relevante publieke en private organisaties, zoals banken, online marktplaatsen, helpdesks en creditcard organisaties (Van de Weijer *et al.*, 2020). Slachtoffers melden hun delicten namelijk relatief vaak bij andere organisaties, wat betekent dat deze organisaties een goede of zelfs betere kennispositie hebben dan de politie op het gebied van verschillende vormen van online criminaliteit.

Interviews

In de gesprekken met officieren werden zoals gezegd niet veel knelpunten omtrent de vervolging van online criminaliteit genoemd. Hetzelfde kan worden gezegd over verbeterpunten omtrent de vervolging. Daarnaast bestaat verdeeldheid over de verbeterpunten die wél genoemd werden. Zo oordelen enkele officieren dat er een portefeuille 'gedigitaliseerde criminaliteit' (brede zin) aan officieren zou moeten worden toegekend, terwijl momenteel alleen portefeuillehouders 'cybercrime' (enge zin) zijn aangesteld. Een andere officier (OM5) is juist van mening dat dit niet noodzakelijk is omdat elke officier met dergelijke zaken aan de slag zou moeten kunnen en hiermee ervaring op zou moeten doen.

Met betrekking tot de rechtspraak wordt als verbeterpunt genoemd om zogenoemde 'gelabelde' zittingen te organiseren. Hiermee wordt gedoeld op zittingen waarop in principe alleen online criminaliteitszaken worden behandeld. Volgens R1 gebeurt dat momenteel ook voor andere thema's, waaronder terrorisme. Wanneer dagen voor deze gelabelde zittingen worden gereserveerd, heeft dat volgens R1 het voordeel dat je zeker weet dat deze zaken worden behandeld door rechters die gespecialiseerd zijn op dit thema (namelijk rechters uit het cybercluster). *"Zo kun je zaken beter plannen en loop je niet het risico dat een voorzitter hem doorschuift naar een later moment. Ook weet het OM dan waar ze naar toe moeten werken."*

Volgens R2 wordt er binnen de ZM verschillend gedacht over het belang van een gespecialiseerde groep rechters op dit thema, ofwel een zogenoemd cybercluster. Hij stelt dan ook dat als gevolg van

"*rechterlijke onafhankelijkheid"* niet elke regio over een cybercluster beschikt en dat de cyberclusters die bestaan, verschillen in mate van volwassenheid en formalisatie. Enerzijds wordt volgens R2 gesteld dat iedere rechter een online criminaliteitszaak moet (kunnen) behandelen. Zelf acht R2 dit niet haalbaar. *"Dat betekent dat als je het aantal cyberzaken dat ieder jaar wordt gedaan, een paar honderd, verdeelt, dat iedere rechter dan minder dan één cyberzaak per jaar doet. Nou, daar leer je het niet van."* R2 is wel voorstander van specialisatie onder een kleiner aantal rechters, zodat zij hier meer ervaring over opdoen.

Ook R1 stelt dat het zinvol zou zijn om een 'cyberkamer' in te richten of een samenwerkingsverband tussen bijvoorbeeld drie rechtbanken op te zetten, waarbij dan enkel dit soort zaken worden aangebracht. Volgens haar leidt dat tot *"meer eenheid in de rechtspraak*" en kan "*een selecte groep meer expertise opbouwen."* Wat betreft het laatste is R1 wel van mening dat dat enkel van belang is bij de meer geavanceerde vormen van online criminaliteit. Zaken omtrent gedigitaliseerde criminaliteit zouden volgens haar in het takenpakket van iedere rechter moeten zitten en dus door iedere rechter behandeld moeten kunnen worden.

Ook zou de koudwatervrees onder rechters weggehaald kunnen worden door hen op opleidings- of trainingsdagen met online criminaliteitszaken te laten oefenen. R1: *"Door het regelmatig te herhalen gaan mensen het makkelijker doen. Sommige aspecten moet je gewoon een aantal keer horen voordat je precies snapt hoe het zit."* Momenteel wordt de kennis van rechters op dit gebied bijgespijkerd door het Kenniscentrum Cybercrime van het Gerechtshof Den Haag, welke het cursusaanbod van opleidingsinstituut Stichting Studiecentrum Rechtspleging (SSR) verzorgt. Voor het cybercluster worden tevens bijeenkomsten georganiseerd om de bestaande kennis op peil te houden (R1), kennis te delen en ervaringen uit te wisselen (R2).

Indien het aantal 'megazaken' toeneemt en de werkdruk bij het OM en/of de ZM tóch onder druk komt te staan, is het volgens R2 in een beperkt aantal gevallen mogelijk om slechts een selectie van het aantal aangiften in de tenlastelegging op te nemen. Dit zou gevolgen hebben voor de doorstroom want, zo stelt R2, aangevers die niet in de tenlastelegging zijn meegenomen, dienen in dat geval de geleden schade via het civiele recht terug te vorderen. Voor de strafmaat hoeft dit (indien aannemelijk is dat het feit meerdere keren heeft plaatsgevonden) echter geen verschil te maken: *"Het OM kan zeggen 'de verdachte heeft meer feiten begaan dan in de tenlastelegging zijn opgenomen, die gaan wij niet allemaal noemen maar […] we eisen wel dat u dit betrekt bij uw strafmaat'"* (R2).

Resumé

Geen instroom

In de literatuur worden enkele suggesties gedaan om de aangiftebereidheid onder slachtoffers van online criminaliteit te verhogen. Een eerste aanbeveling betreft het inzetten van publieke bewustwordingscampagnes waarin de noodzaak wordt benadrukt om online criminaliteit te melden bij de politie. Een andere suggestie is om uniforme en gedegen aangiftesystemen op te zetten, bijvoorbeeld in de vorm van online aangiftesystemen. Zo zouden online aangiftesystemen de aangiftebereidheid van gebruikers om aangifte te doen van online criminaliteit verhogen. In Australië is bijvoorbeeld een online aangiftesysteem ontwikkeld speciaal voor online criminaliteit. Ten slotte wordt in de literatuur geopperd om de opportuniteitskosten (tijd, moeite en financiële kosten) voor het doen van aangifte te verminderen en de waargenomen voordelen van het aangifteproces te verhogen.

Intake en case screening

Uit de interviews blijkt dat het aangifteproces een belangrijke stap is in het proces van in- en doorstroom van online criminaliteit. Om de eerdergenoemde knelpunten in de intake van aangiften online criminaliteit te kunnen verbeteren, wordt in de literatuur aanbevolen om training op maat te geven aan intake- en servicemedewerkers. Ook respondenten en experts gaven tijdens de discussiesessie aan dat het goed opleiden van intake medewerkers en/of casescreeners van groot belang is om de kwaliteit van aangiften te verbeteren.

Een door respondenten veelgenoemde verbetering zit dan ook in het landelijke clusteren en screenen van aangiften. De experts die deelnamen aan de discussiesessies bevestigen dit. Een belangrijke reden die hiervoor wordt gegeven is dat volgens respondenten noodzakelijkerwijs iemand de regie moet nemen en dat dat momenteel niet gebeurt. Centralisatie zou ervoor moeten zorgen dat meer aangiften relevante informatie over verdachten bevatten en daarmee de opsporingskansen worden vergroot. Tevens zou dit er volgens respondenten voor kunnen zorgen dat er beter zicht komt op de samenhang tussen aangiften die individueel wellicht een (te) laag schadebedrag hebben en daardoor nu niet worden opgepakt, maar eigenlijk samenhangen omdat ze door dezelfde verdachte(n) zijn gepleegd. Daarnaast kan het volgens respondenten tevens de efficiëntie van het politiewerk vergroten en het mogelijk maken om trends te signaleren en op basis daarvan de prioriteit te bepalen (bijvoorbeeld welke aangiften als eerste moeten worden opgepakt). Daarbij benadrukken respondenten het belang van geautomatiseerde dataverrijking en -analyse, met name omdat online criminaliteit minder tot de verbeelding zou spreken.

We merken graag op dat in lijn met het centraal verzamelen en screenen van online criminaliteitszaken, meerdere respondenten wijzen op bestaande initiatieven zoals het LMIO, de ECTF en Operatie Centurion.

Buitenlandse respondenten geven aan dat in zowel het VK, de VS en Australië op eenzelfde manier wordt gezocht om problemen met betrekking tot intake en case screening op te lossen. Het meest kunnen we leren van de situatie in het VK en Australië. In het VK is er sprake van een gecentraliseerde intake van fraudezaken. Zowel online als offline fraudes. In Australië zijn er voor verschillende vormen van criminaliteit centrale meldpunten waar burgers en bedrijven aangifte kunnen doen waarna de aangifte naar het juiste politieteam wordt gestuurd. Sinds enkele jaren is er ook een landelijk meldpunt voor online criminaliteit. Het voert te ver om deze initiatieven hier tot in detail te beschrijven. Een belangrijke les die we volgens respondenten van beide initiatieven kunnen leren is dat de centrale afhandeling van aangiften zorgt voor een veel betere registratie van aangiften en dat daarmee het totale aantal aangiften simpelweg snel omhoog zal gaan. Dat zegt echter niets over de verdere doorloop binnen de strafrechtketen. Respondenten geven aan dat ook verderop in de keten (van opsporingsteams tot OM en ZM) de capaciteit moet worden vergroot omdat er anders wel meer aangiften zijn die binnenstromen, maar er bij toename van de instroom gebrek aan capaciteit ontstaat om zaken op te pakken. De respondenten uit het VK geven daarbij aan dat ze zien dat er relatief veel aangiften alsnog meteen uitstromen, maar dat de aangiften die gebundeld en verrijkt zijn met informatie over de verdachte(n) er wel voor zorgen dat de zaken die ze doorsturen naar teams vaker succesvol worden opgepakt. De respondent uit Australië geeft aan dat er een ander positief neveneffect te zien is van het centraal opnemen van aangiften, namelijk dat de tevredenheid van aangevers de afgelopen jaren is gestegen. Ondanks dat lang niet alle aangiften succesvol worden opgepakt voorziet in dit geval het centraal opnemen van aangiften toch in een belangrijke behoefte van slachtoffers.

Opsporing

In de literatuur worden met name suggesties gedaan om het proces van de opsporing van online criminaliteit te verbeteren die gericht zijn op het wegnemen van koudwatervrees. Zo zouden trainingen ervoor kunnen zorgen dat rechercheurs bewuster worden over de mogelijke ernst van deze vormen van criminaliteit en zien dat onderzoeken lang niet altijd complex zijn. Daarnaast wordt genoemd dat opsporingsteams kunnen worden versterkt met mensen van buiten de politie omdat bijvoorbeeld sommige burgers over meer expertise beschikken op het gebied van online criminaliteit dan traditionele politiemedewerkers. Ten slotte wijzen studies er op dat er meer (inter-)nationale samenwerking nodig is tussen opsporingsinstanties zodat kennis over online criminaliteit, forensische methodes en opsporingstechnieken kunnen worden gedeeld.

Een punt voor verbetering aangaande de fase van opsporing die door zowel respondenten bij de politie als het OM wordt genoemd, houdt in dat het recherchewerk niet eindeloos door hoeft te gaan. Respondenten merken op dat daders van online criminaliteit meerdere slachtoffers tegelijkertijd kunnen maken en dat het soms lijkt alsof er eindeloos veel aangiften aan elkaar kunnen worden gekoppeld. Er moet volgens sommige respondenten dan ook 'slimmer worden opgespoord'. Het is niet altijd nodig om ál het bewijsmateriaal te verzamelen. Er kunnen ook vaker kosten-baten-overwegingen worden en worden bekeken wat de investering (in tijd en menskracht) op gaat leveren (een hogere straf?).

OM en ZM

Door het beperkte aantal studies omtrent de in- en doorstroom van online criminaliteit bij het OM en de ZM, ontbreken aanbevelingen omtrent deze fasen in de strafrechtketen. Sommige aanbevelingen die in de literatuur worden genoemd om de in- en doorstroom van online criminaliteit te verbeteren hebben betrekking op meerdere fasen in de strafrechtketen of zelfs de gehele strafrechtketen. Zo wordt aanbevolen om lange termijnplannen te maken om vaardigheden van medewerkers te verbeteren, moet de effectiviteit van bestaande trainingen worden verbeterd en wordt aanbevolen aan strafrechtketenorganisaties om actief samen te werken met andere relevante publieke en private organisaties, zoals banken, online marktplaatsen, helpdesks en creditcard organisaties.

Tijdens de interviews werden er niet heel veel knelpunten omtrent de vervolging van online criminaliteit genoemd. Datzelfde geldt dan ook voor de mogelijke verbeterpunten. Een punt dat respondenten noemen en dat door experts tijdens de discussiesessies werd aangedragen is het organiseren van geschikte cursussen voor zowel OM als ZM om de koudwatervrees weg te nemen. Over andere verbeterpunten die genoemd werden bestaat verdeeldheid. Zo oordelen enkele officieren dat er een portefeuille 'gedigitaliseerde criminaliteit' (brede zin) aan officieren zou moeten worden toegekend, terwijl momenteel alleen portefeuillehouders 'cybercrime' (enge zin) zijn aangesteld. Anderen geven juist aan dat elke officier met dergelijke zaken aan de slag zou moeten kunnen en hiermee ervaring op zou moeten doen. Met betrekking tot de rechtspraak wordt als verbeterpunt genoemd om zogenoemde 'gelabelde' zittingen te organiseren. Hiermee wordt gedoeld op zittingen waarop in principe alleen online criminaliteitszaken worden behandeld. Op die manier behandelen rechters die gespecialiseerd zijn op dit thema deze zaken. De interviews laten wel zien dat er verschillend wordt gedacht over het belang van een gespecialiseerde groep rechters op dit thema. En als gevolg van "rechterlijke onafhankelijkheid" zou momenteel ook niet elke regio over een cybercluster beschikken en zijn de cyberclusters die wel bestaan verschillend in mate van volwassenheid en formalisatie.

7. Slotbeschouwingen

Alle vorige hoofdstukken bevatten uitgebreide resumés en er zijn twee aparte hoofdstukken gewijd aan knelpunten en verbetermogelijkheden. Om die reden zullen we in dit hoofdstuk niet nog eens de belangrijkste resultaten uit de afzonderlijke hoofdstukken herhalen, maar gaan we kort in op wat de belangrijkste conclusies zijn wanneer we de resultaten van de verschillende onderzoeksmethoden in samenhang bezien. Daarnaast gaan we in op enkele belangrijke beperkingen van het onderhavige onderzoek en geven we suggesties voor vervolgonderzoek.

Conclusies op hoofdlijnen

Hoewel online criminaliteit volgens onderzoek gebaseerd op slachtofferenquêtes tegenwoordig tot de grootste vorm van criminaliteit behoort, blijken de meeste vormen van online criminaliteit door de wijze waarop het in de strafrechtketen wordt geregistreerd vaak niet als zodanig herkenbaar. Dit belemmert het zicht op de in- en doorstroom van online criminaliteit in de strafrechtketen als ook de mogelijkheden voor een gerichte aanpak van de knelpunten in de strafrechtketen. Om de in- en doorstroom van online criminaliteit in de strafrechtketen toch te kunnen bestuderen hebben we onze toevlucht moeten nemen tot het ontwikkelen van *predictive textmining* modellen om BVH-registraties te kunnen classificeren. Dit bleek niet voor alle vormen van online criminaliteit mogelijk, waarmee we voor malware, ransomware, DDoS-aanval, online bedreiging, online stalking, online smaad/laster/belediging, overige online oplichting en money muling geen in- en doorstroomanalyses konden doen. Het zou enorm helpen wanneer bij de registratie van criminaliteit een uitgebreidere en ook regelmatig geactualiseerde lijst specifieke delicttypen zou worden gehanteerd, waardoor de verschillende verschijningsvormen op systematische wijze in kaart kunnen worden gebracht. Dit verbetert het informatiebeeld, maakt een gerichtere aanpak van de knelpunten in de strafrechtketen mogelijk en voorkomt dat een volgende studie wederom complexe methoden moet gebruiken in een poging om de in- en doorstroom in beeld te brengen.

Uit het onderzoek komt naar voren dat er zowel obstakels zijn bij de instroom als ook bij de doorstroom van online criminaliteit in de strafrechtketen. Waar de prevalentie van online criminaliteit op basis van slachtofferenquêtes juist erg hoog wordt geschat, vallen in de kwantitatieve analyses van BVH-registraties met name de lage instroomcijfers op. Gedigitaliseerde criminaliteit komt ongeveer 4 keer vaker voor dan cybercrime, maar de meeste vormen van online criminaliteit komen in minder dan 1% (het maximum ligt op 4% voor alle gedigitaliseerde criminaliteit tezamen) van de BVH-registraties voor. Dit beeld past bij wat bekend is over de lagere aangiftebereidheid bij online criminaliteit in vergelijking

met die bij traditionele criminaliteit: veel gevallen van online criminaliteit stromen dus simpelweg nooit de strafrechtketen in.

De geïnterviewde experts zien de grootste uitdagingen aan de voorkant van de strafrechtketen, bij de politie. Met name de intake van online criminaliteit zou te wensen overlaten omdat kennis en expertise ontbreken. Dit zou ertoe leiden dat bij online criminaliteit er niet altijd een aangifte wordt opgenomen en soms alleen een melding wordt geregistreerd, waarmee de grootste bron van instroom (aangiften door burgers en bedrijven) stokt. Enerzijds klopt dit beeld met onze bevindingen. We constateerden immers dat waar de prevalentie van online criminaliteit op basis van slachtofferenquêtes erg hoog wordt geschat, in onze kwantitatieve analyses van BVH-registraties juist de lage instroomcijfers opvallen. Er is dus een groot verschil tussen door burgers ervaren – en in slachtofferenquêtes gerapporteerd – slachtofferschap en door de politie geregistreerd slachtofferschap. Verder troffen we in de kwantitatieve analyses inderdaad BVH-registraties van online criminaliteit zonder aangifte aan. Dit betrof ongeveer een kwart van de registraties. Dit is echter niet uniek voor online criminaliteit, want bij andere vormen van criminaliteit zagen we zelfs nog hogere percentages BVH-registraties zonder aangifte. Het is om die reden aan te raden om in vervolgonderzoek te kijken naar de discrepantie tussen ervaren slachtofferschap door burgers en door de politie geregistreerd slachtofferschap. Verder is het van belang om voor verschillende vormen van criminaliteit een nadere analyse te maken van de situaties waarin de politie een melding registreert in plaats van een aangifte opneemt. Volgens de geïnterviewde experts zou het gebrek aan kennis en expertise bij de intake van de politie daarnaast leiden tot een lage kwaliteit van de processen-verbaal van aangifte, hetgeen in alle vervolgstappen in de strafrechtketen tot problemen kan leiden.

Als slachtoffers van online criminaliteit wel aangifte hebben gedaan, dan blijkt dat er in 90% van de gevallen geen verdachte wordt geïdentificeerd. Dit lage percentage in combinatie met de al zeer beperkte instroom leidt ertoe dat maar weinig zaken doorstromen in de strafrechtketen. Het percentage BVH-registraties met een aangifte waarbij tenminste één verdachte wordt geïdentificeerd verschilt overigens weinig tussen cybercrime en gedigitaliseerde criminaliteit, al valt op dat de percentages registraties met verdachte(n) juist laag zijn bij die vormen van online criminaliteit die het meest geregistreerd worden. Blijkbaar lukt het bij die zaken die het grootste deel van het werkaanbod van de politie bepalen het minst goed om er verdachten aan te koppelen. Met name het lage percentage bij online aan- en verkoopfraude (2%) is opvallend, aangezien er bij die vorm toch vaak bankrekeninggegevens beschikbaar zouden moeten zijn.

Hoewel de respondenten verschillende redenen noemden waarom opsporing bij online criminaliteit lastig is en dat er koudwatervrees bestaat, zijn lage ophelderingspercentages niet uniek voor online

criminaliteit. Ook bij vermogenscriminaliteit zien we lage percentages (bij 12% van de BVH-registraties met een aangifte zagen we ook tenminste 1 verdachte geregistreerd staan), terwijl deze juist aanzienlijk hoger liggen bij fraudedelicten (31%) en al helemaal bij misdrijven tegen de lichamelijke integriteit (59%). Het verschil met misdrijven tegen de lichamelijke integriteit is wellicht niet zo verwonderlijk, omdat in die gevallen er vaak sprake zal zijn geweest van direct contact tussen dader en slachtoffer, waardoor er daderindicatie zal zijn. Het grote verschil tussen offline en online fraudedelicten is echter niet op deze wijze te verklaren. Hoewel we in deze studie niet kunnen uitsluiten dat de waargenomen verschillen samenhangen met verschillen in opsporingsinzet, komt uit de interviews naar voren dat de aanwezigheid van dader- of opsporingsindicatie een grote rol speelt bij de keuze om zaken op te pakken. Respondenten gaven aan dat dit bij online criminaliteit vaker ontbreekt waardoor zaken al sneuvelen bij de casescreening of verder niet succesvol worden opgepakt. Het ontbreken van dader- of opsporingsindicatie is echter niet uniek voor online criminaliteit, want dit speelt ook vaak bij vermogensdelicten.

Wanneer het de politie lukt om verdachten te identificeren, dan blijken dat voor het overgrote deel meerderjarige verdachten te zijn. De verhouding tussen meerderjarige en minderjarige verdachten verschilt daarbij nauwelijks tussen cybercrime en gedigitaliseerde criminaliteit. Ongeveer eenderde van zowel de meerderjarige als de minderjarige verdachten van online criminaliteit stroomt helemaal door naar de rechtbank. We zagen verder bij een aanzienlijk deel van de meerderjarige verdachten een overige of onbekende afdoening bij politie of OM (43%), terwijl dit bij minderjarige verdachten ook maar in mindere mate voorkwam (33%). Minderjarige verdachten kregen vaker dan meerderjarige verdachten al een afdoening bij de politie.

Hoewel onder de respondenten consensus lijkt te bestaan dat de grootste uitdagingen in de in- en doorstroom van online criminaliteit binnen de strafrechtketen liggen binnen de politie, laten de kwantitatieve analyses zien dat er voor een aanzienlijk deel van de naar het OM ingestuurde verdachten sepots worden geregistreerd. Dat beeld zien we overigens ook voor de drie andere typen delicten waarmee we online criminaliteit vergeleken hebben. De redenen voor de sepots hebben we niet onderzocht, maar het beeld is dus niet uniek voor online criminaliteit. Daarmee lijkt het voor het verbeteren van de in- en doorstroom van online criminaliteit binnen de strafrechtketen inderdaad verstandig om vooral de aandacht te richten op de knelpunten en uitdagingen binnen de politie.

Beperkingen van het onderzoek

In deze studie is gebruik gemaakt van literatuuronderzoek, grootschalige kwantitatieve analyse van registratiegegevens en interviews om zicht te bieden op de in- en doorstroom van online criminaliteit

in de strafrechtketen en tevens knelpunten en verbetermogelijkheden te identificeren. Hoewel op basis van de literatuurstudie en interviews is ingegaan op de relatief lage instroom doordat slachtoffers zich simpelweg niet melden bij de politie, valt dit buiten de scope van de kwantitatieve analyse omdat daarvoor juist politieregistraties als startpunt hebben gediend. De literatuurstudie liet echter zien dat er op basis van slachtofferenquêtes al het nodige over bekend is. De aangiftebereidheid blijkt lager te liggen bij online criminaliteit dan bij traditionele vormen van criminaliteit. Deze studie geeft ook geen kwantitatieve analyse van rechterlijke uitspraken in online criminaliteitszaken, waarmee de in- en doorstroom van online criminaliteit in de strafrechtketen is geanalyseerd vanaf aangifte tot dagvaarding.

We menen op basis van de verschillende onderzoeksmethoden een rijk beeld te hebben gegeven over de in- en doorstroom van online criminaliteit in de strafrechtketen, maar elke afzonderlijke methode heeft uiteraard eigen beperkingen. We noemen hier de belangrijkste die betrekking hebben op de gehanteerde empirische onderzoeksdesigns.

Om een kwantitatieve analyse van de in- en doorstroom van online criminaliteit in de strafrechtketen mogelijk te maken, zijn *predictive textmining* modellen ontwikkeld. Daarbij is gebruik gemaakt van LASSO logistische classificatiemodellen, een relatief eenvoudig *supervised machine learning* model. Nader onderzoek zou moeten uitwijzen of meer geavanceerde *machine learning* modellen beter hadden gepresteerd. Zo is in deze studie ervoor gekozen om 17 afzonderlijke zogenaamde *binary classification* (wel/niet) modellen te ontwikkelen voor cybercrime en gedigitaliseerde criminaliteit alsmede voor elke vorm van online criminaliteit apart, terwijl sommige BVH-registraties betrekking hebben op meerdere vormen tegelijk. Zogenaamde *multilabel classification* modellen zijn in dat geval mogelijk meer geschikt (Tollenaar *et al.*, 2019), maar ze zijn veel minder gangbaar en vragen om specialistische software terwijl in deze studie gebruik is gemaakt van het binnen de *machine learning* in R gangbare `tidymodels` *framework*.

Voor de ontwikkeling van de modellen zijn 7.500 BVH-registraties uit een selectieve steekproef met relatief veel online criminaliteit handmatig geannoteerd. Hoewel de *performance* van veel modellen goed was, bleek het voor sommige afzonderlijke vormen van online criminaliteit niet mogelijk modellen te ontwikkelen waarmee goede classificaties konden worden gedaan, met name voor vormen die maar weinig voorkwamen in de selectieve steekproef. Daarmee werd het onmogelijk om voor malware, ransomware, DDoS-aanvallen, online bedreigingen, online stalking, online smaad/laster/belediging, overige online oplichting en *money muling* afzonderlijke in- en doorstroomanalyses te doen. Omdat voor de ontwikkeling van goed-presterende *machine learning* modellen in de regel veel gegevens nodig zijn, had het annoteren van een nog grotere steekproef

mogelijk tot betere *performance* van de modellen geleid. Dit vraagt echter om een nog grotere inspanning waarbij het maar de vraag is of de kosten opwegen tegen de baten, terwijl het uiteindelijk veel beter zou zijn als reeds bij de registratie van criminaliteit een uitgebreidere en ook regelmatig geactualiseerde lijst van specifieke delicttypen zou worden gehanteerd. Overigens kan het daarbij heel nuttig zijn om verder te investeren in de ontwikkeling van *predictive textmining* modellen voor de classificatie van verschillende delicttypen zodat intakemedewerkers van de politie tijdens het maken van een nieuwe registratie geassisteerd kunnen worden door een *predictive user interface* die aan de medewerker suggesties doet over het specifieke type delict waarop de registratie betrekking heeft, zoals nu ook al gebruik wordt gemaakt van een 'slimme keuzehulp' bij online aangiftes (Landman, 2023).

Een belangrijke beperking van de kwantitatieve in- en doorstroomanalyses is dat aangiften geregistreerd in het BVH-systeem van de politie als startpunt zijn genomen. Alle instroom die op een andere manier dan middels een aangifte heeft plaatsgevonden, viel daarmee buiten de scope van de kwantitatieve analyse. Naar de omvang van die andere instroom kunnen we alleen maar gissen. Ondanks dat respondenten in de interviews juist aangaven dat online criminaliteitszaken ook vaak anders instromen dan via een aangifte, vermoeden we dat voornamelijk uitzonderlijke zaken buiten beeld zijn gebleven terwijl de meeste gevallen wel degelijk in het BVH-systeem geregistreerd zullen zijn geweest.

Een belangrijke beperking van de interviews is dat ze zijn gehouden met een selectieve groep van personen die zich binnen de strafrechtketen met online criminaliteit bezighouden (op enkele intakemedewerkers en casescreeners na). Dat had als voordeel dat ze goed geïnformeerd waren over de huidige stand van zaken en ook knelpunten en verbetermogelijkheden konden identificeren. De selectie van respondenten die zich veel met online criminaliteit bezighouden heeft echter wel als risico dat zij vooral het belang van meer aandacht voor online criminaliteit benadrukken en knelpunten identificeren die eigenlijk helemaal niet specifiek zijn voor online criminaliteit. Dit risico is vooral groot wanneer respondenten benoemen dat anderen binnen de politie, het OM of de rechtspraak het belang van online criminaliteit te weinig onderkennen. Met de selectie van respondenten weten we immers niet of zij die zich minder met online criminaliteit bezighouden daadwerkelijk het belang minder zien, of dat dit alleen in de perceptie van deze respondenten te weinig is.

Summary

Our current society is highly digitalized. With the digitization of society, crime has also been digitized and the workload of the police and the judiciary has therefore changed. The criminal justice system is increasingly confronted with crimes with a digital component, also known as online crime. On the one hand, there are new crimes, for example hacking a database with personal data or shutting down websites or networks. These are examples of cybercrime-dependent crimes. On the other hand, there are traditional forms of crime in which ICT plays an increasingly important role. Examples include committing fraud via the Internet and online stalking. These are examples of cyber-enabled crimes.

Victimization surveys show that nowadays more citizens fall victim to hacking, online scams and online fraud than to bicycle theft. Citizens and companies also fall victim to many more forms of online crime: from malware or ransomware to phishing, cyberstalking and cyber threats. Although it is now clear that online crime is a growing problem and that many people get victimized, the inflow and throughput of online crime in the criminal justice system appears to be lagging behind the development of victimization of online crime as reported in the Safety Monitor from Statistics Netherlands. While there are apparently many victims, the number of offenders convicted of online crime is small.

Previous research shows that there are at least three reasons for the large difference in the number of victims and the number of convictions: a low willingness to report online crimes, the organization of the police and the judiciary that is not yet sufficiently equipped to effectively deal with such cases, and the complexity of cases. In addition to these causes for a low inflow and throughput of online crime in the criminal justice system, there is also the problem that many forms of online crime - especially forms of cyber-enabled crimes - are not recognizable as such in the police and judicial records. This means that not only may the actual inflow and throughput be small, but there is also limited insight into the inflow and throughput that does exist.

This research is aimed at providing more insight into the inflow and throughput of online crime in the criminal justice system. In addition to insight into the current inflow and throughput, the research also provides insight into possible bottlenecks within the criminal justice system, good practices and opportunities for improvement.

The research answers the following research questions:

1. According to the literature, are there forms of online crime in which suspects do not or hardly enter the criminal justice system? If yes, which one? What explanations are given in the literature for this low inflow?

2. What are the most recent figures for 2018-2020 regarding the inflow and throughput of online crime in the criminal justice system?
3. Which bottlenecks can be identified within the inflow and throughput of online crime in the criminal justice system?
4. To what extent do other countries also have to deal with the bottlenecks identified under question 3? What experiences do other countries have with solving these bottlenecks?
5. What improvements can be made per link of the criminal justice system?

Research methods

To answer the research questions we used various research methods.

We conducted an international literature review to gain insight into which forms of online crime do not or hardly enter the criminal justice system, what explanations exist for this, which bottlenecks within the criminal justice system can lead to limited inflow and throughput of cases and what possible points for improvement are within the various links of the criminal justice system to promote the throughput of cases.

For the quantitative analysis of the inflow and throughput of online crime in the criminal justice system, we took BVH registrations from the police as a starting point. Because many forms of online crime are not registered as such in the police registration system, we developed predictive text mining models. Such models can automatically classify documents with large amounts of text based on relevant text features. For the present study, this meant that BVH registrations with text fields - which, for example, included findings from reporting officers and statements from victims, suspects or witnesses - could be assigned one or more forms of online crime as a label. We used supervised machine learning. With this technique, a model is trained using sampled documents for which the label they should have has been manually determined in advance. After training, it is assumed that the model can provide new documents with the correct label itself. We developed the models based on a selective sample (n=7,500) in which relatively many registrations of online crime occurred and then applied the models to a large random sample (n=300,000) of unique BVH registrations from the years 2018-2020. For the registrations from the large sample, we checked to what extent there had been a crime report and whether suspects had been linked. To determine the throughput in the criminal justice system, we linked the BVH data to data derived from the BOSZ system. This link made it possible to check for each registered suspect whether he or she received a settlement early in the criminal justice system (reprimand, police penalty order, HALT) or was sent by the police to the Public Prosecution Service. To

determine the throughput to the Public Prosecution Service and the court, we then linked the data on suspects submitted to the Public Prosecution Service to data taken from the GPS system of the Public Prosecution Service. Based on the GPS data, we were able to determine for each suspect whether the case was dismissed, whether the suspect received a settlement from the Public Prosecution Service (penal order or transaction) or whether the suspect was summoned and had to appear in court. To determine to what extent the inflow and throughput of online crime differs from other types of crime, we repeated the same analyses for three other forms of crime (property crimes, violent crimes and offline fraud).

In addition to the literature research and the large-scale quantitative analysis of police and judicial data, we conducted interviews with people working within the various organizations of the criminal justice system, interviews with national and foreign experts, and we organized two discussion sessions with experts from within and outside the police and justice system. The purpose of the interviews with people working within the criminal justice system was to gain insight into general bottlenecks in the inflow and throughput of online crime in the criminal justice system. We interviewed a total of 34 people within the criminal justice system, of which 26 worked for the police, 6 for the Public Prosecution Service and 2 judges. The aim was to at least speak to people within the police organization who have a role in both the inflow and throughput of cases: service & intake staff, case screeners and a team leader who is involved in the case weighing process. Discussions were held with employees from various teams, including frontline teams (BT), the district criminal investigation team (DR) and the Regional Criminal Investigation Division (DRR) within the following 5 police units: The Hague, North Holland, Northern Netherlands, Central Netherlands and Zeeland-West Brabant. Within the Public Prosecution Service, public prosecutors who have online crime in their portfolio have been interviewed. Here the public prosecutor's offices have been selected that collaborate with the selected police units. Two judges were interviewed who had handled cases with an online component.

To gain insight into possible good practices in other countries that could also be applicable in the Netherlands, we interviewed 5 international experts. The purpose of these interviews was to gain insight into the extent to which other countries also face the bottlenecks that we heard in the interviews with people working within the criminal justice system and what experiences there are in solving these bottlenecks in those countries. Interviews were conducted with 3 academic researchers and 2 practitioners from the United Kingdom (UK), the United States (US) and Australia.

Finally, the results of the literature review, quantitative analyses and interviews were discussed with experts from within and outside the police and justice system. The discussion meetings were also used

to identify possible solutions to improve the identified bottlenecks. A total of 5 experts participated in the discussion sessions.

Victimization, no inflow

Previous research shows that the willingness to report crimes among victims of online crime is generally lower than among victims of traditional crimes. Dutch studies show that approximately 13% of victims of online crime report it to the police. The willingness of victims to report to the police differs for different forms of online crime. For crimes where IT is not only the means but also the target (cyber-dependent crimes), the willingness to report crimes appears to be lower than for crimes where IT is only used as a tool (cyber-enabled crimes). Previous studies show that – just like for traditional crime – the type of online crime is an important predictor of the willingness to report online crime. Furthermore, again just as with traditional crime, the (perceived) seriousness of a crime is an important predictor: the more serious the crime, the more likely it is reported.

Various explanations are given in the literature as to why victims of online crime do not report crime. For example, individuals and companies do not always know that they are victims or victims do not see online incidents such as malware infections as crime. In cases where victims are aware of their victimization, various factors can lead to them not reporting the crime. A frequently mentioned explanation is that individuals experience the severity and impact of online crimes as low and are therefore less likely to report them. In other cases there is no or little (financial) damage or the damage has already been reimbursed by, for example, insurance companies or financial institutions. Furthermore, shame can play a role in not reporting victimhood. Finally, victims may have a lack of confidence in the police to track down and arrest perpetrators of online crime.

Inflow and throughput in figures

The inflow and throughput of online crime in the criminal justice system has been analyzed for the years 2018-2020. To this end, police BVH registrations from that period were taken as a starting point. In the BVH system, the police register incidents, reports and the actions linked to the incidents, such as reports of interrogations of witnesses or suspects. Because the various forms of online crime cannot be systematically identified in the BVH registrations on the basis of, for example, unique crime classes, predictive text mining models have been developed that use all textual information recorded in registrations of findings, explanations, statements and modus operandi associated with a BVH registration. Separate models have been developed to distinguish nine different types of online crime: four forms of cyber-dependent crimes (hacking, malware, ransomware and DDoS attack) and five forms of cyber-enabled crimes (online threat, online stalking, online libel/slander/insult, online fraud

and money muling), where we further divide online fraud into phishing, online identity fraud, online purchase and sales fraud, Whatsapp-fraud, helpdesk fraud, and other online fraud. The predictive text mining models did not perform sufficiently well for all forms of online crime to identify the individual forms of online crime in BVH registrations. The performance was good for the general labels of cyber-dependent and cyber-enabled crime as well as for the individual labels of hacking, online fraud, phishing, online identity fraud, online purchase and sales fraud, Whatsapp-fraud and helpdesk fraud, and descriptive analyses of the inflow and throughput in the criminal justice system of those cases are presented.

By applying the models with good performance to a large sample (n=300,000) of BVH registrations, the inflow and throughput of online crime in the period 2018-2020 could be studied. BVH registrations with a crime report form a clear starting point of the criminal justice system and BVH registrations that are classified as online crime and in which at least 1 report has been registered therefore mark what we have called in quantitative analysis the inflow of online crime into the criminal law system. For all BVH registrations of online crime in which at least 1 report had been registered, it was examined to what extent suspects were also linked to them and by linking the BVH registrations to data from the BOSZ-system, for each registered suspect, it is checked whether he received a settlement early in the criminal justice system (reprimand, police penalty order, HALT) or was sent by the police to the Public Prosecution Service. To determine the throughput to the Public Prosecution Service and court, the registrations are then linked to data derived from the GPS-system used by the Public Prosecution Service. Based on the GPS data, we were able to determine for each suspect whether he or she received a settlement from the Public Prosecution Service (penalty order or transaction) or whether the suspect was summoned and had to appear in court.

The most important finding from the quantitative analysis of the inflow and throughput of online crime in the criminal justice system lies in the low numbers. We started the analysis with a relatively large sample of BVH registrations (n=300,000) and subsequently established that most forms of online crime occurred in less than 1% (with a maximum of 4% for all cyber-enabled crime together) of the registrations. We therefore see little of the high prevalence found in victimization surveys in BVH registrations. Subsequently, it turned out that in approximately 25% of the registrations there was no crime report and of all registrations with a report, a suspect was only linked in approximately 10% of the cases. The most important conclusion must therefore be: even with the application of advanced predictive text mining models, we find few registrations of online crime in the criminal justice system. The inflow in the form of crime reports is not large, but because a suspect is only linked in approximately 10% of the cases, the throughput is much smaller.

Furthermore, the results of the large-scale quantitative analyses show that BVH registrations classified as cyber-enabled crime are significantly more common than registrations of cyber-dependent crime. The 25% of BVH registrations that are classified as cyber-dependent or cyber-enabled crime where no crime report was made indicates that apparently quite often registrations are made in the BVH system regarding online crime without anyone reporting victimization. However, when we compare these figures with those for other forms of crime, we see that this is not unique to online crime. For violent crimes (32%) and fraud (51%), the percentages are even considerably higher, while the percentage for property crimes (11%) is actually lower. Making a BVH registration without recording a crime report therefore does not seem unique to online crime.

The low percentage of BVH registrations of online crime with a crime report for which at least 1 suspect is registered (8% for cyber-dependent crime and 10% for cyber-enabled crime) appears to vary considerably between different forms of online crime, from only 2% for online purchase and sales fraud up to 18% in helpdesk fraud. It also appears that relatively few suspects are registered for forms of online crime that occur relatively frequently.

88% of suspects of cyber-dependent and 85% of suspects of cyber-enabled crime were adults, although it is striking that the share of underage suspects is somewhat higher in helpdesk fraud (21%) and somewhat lower in Whatsapp-fraud (8%), online identity fraud (8%) and online scams (9%).

For a significant proportion of adult suspects of online crime, we see other or unknown settlements registered with the police or Public Prosecution Service (together accounting for 43%), while this also occurs to a lesser extent among minor suspects (33%). The percentage of suspects of online crime who go all the way to court differs little between adult and underage suspects, and is around one third. Underage suspects are more likely to receive a settlement with the police (6%) than adult suspects (1%).

To put the inflow and throughput of online crime into perspective, the same analyses have been done for three other forms of crime, namely property crime, violent crime, and offline fraud. We see significantly more BVH registrations of property crime than of online crime. The numbers for violent crimes are slightly lower and we see much fewer registrations for offline fraud. The percentage of BVH registrations in which at least 1 crime report was registered was higher for property crime than for online crime, but it was lower for other forms of crime. In property crime we see a suspect registered approximately as often (in 12% of cases) as in online crime (10%). For offline fraud, the percentage of BVH registrations with a report in which at least 1 suspect is registered is considerably higher (31%), while for violent crimes this is much higher (59%). The clearance rates for these last two forms of crime are therefore considerably higher than for online crime and property crime. This is not surprising for

violent crimes, since the perpetrator and victim will almost always have been in direct contact with each other and there is therefore often offender information, while in online crime and property crime the suspect will often not be immediately known. However, this does not explain the difference in clearance rates for online and offline fraud.

As soon as a suspect is in the picture, we also see that underage suspects are more likely to be dealt with by the police in property crime and violent crimes than adult suspects. It is also striking that a high percentage of adult suspects of property crime progress all the way to court (55%). This percentage is also considerably higher for violent crimes (46%) and offline fraud (43%) than for online crime (32%).

Bottlenecks according to the literature and according to actors within the criminal justice chain

Intake

The literature shows that the police do not always file a report when victims of online crime contact the police. This may be because intake employees think that it is not a criminal offense (for example in hacking cases), that it is a civil case (for example in online fraud) or more generally that intake employees estimate the seriousness of the victimization as low. If a report is recorded, the successful recording of a report appears to depend on the understanding and knowledge of the intake employee who records the report of online crime. However, this knowledge is not always (sufficiently) available among intake staff.

Respondents indicate that they see a lack of knowledge of online crime among intake staff, while a high-quality report ensures a successful throughput through the criminal justice system. A further bottleneck is that the statement of the victim also depends on (the knowledge of) the victim. The victim's 'story' is not always clear. Citizens themselves do not always know exactly what happened. It is all the more important for intake staff to ask the right questions. There are tools available that allow intake employees to look up which information needs to be requested based on the type of crime, but this requires that employees know where to find these tools and that they know which type of crime it concerns. Finally, respondents point out that reports are increasingly being filed via the internet. The automated reporting process via the police website makes it possible to properly inquire about relevant information for criminal investigation (including bank account numbers).

Both the experts who participated in the discussion sessions and the international respondents who were interviewed recognize the picture that emerged from the literature and interviews. During the expert sessions, the important role that intake staff play in laying a good foundation for further

investigations was repeatedly pointed out. Without the right information, the risk of premature failure is greater, according to the experts.

Case screening

There is relatively little research that focuses on case screening of online crime cases by the police. The research that has been done gives the impression that online crime cases are less likely to be processed than traditional cases. Explanations for this are that handling such cases takes a lot of time, a lack of capacity, the international nature of online crime and the quality of the crime reports. Cases in which important information is missing are less likely to be processed during the case screening.

The interviews reveal various reasons why online crime cases are not included in the screening process. The most important reason mentioned by respondents is the lack of investigative leads and, more specifically, the lack of suspect information. Although this is not a unique problem, according to respondents it is particularly prevalent for online crime, because perpetrators can protect themselves and illegally obtained income more easily and effectively. In addition, it appears to be more difficult for online crime than for traditional crime to estimate whether a case contains sufficient investigative leads. The financial damage also plays a role in whether or not a case is taken up. If there is a 'small' amount of damage, the case will not be taken up. However, what exactly is meant by 'minor damage' differs according to the respondents between police units, but also between districts and frontline teams. It can also be a reason to screen out a case if it turns out that a victim's financial damage has already been compensated, for example by a bank.

Investigation

Even when it is decided to take up a case, there may be various reasons why a case still flows out during the investigation. Four factors emerge from the literature that complicate the detection of online crime. Firstly, the lack of priority within police organizations is mentioned, which is reinforced by, among other things, the complexity of these investigations and the limited awareness of the risks of online crime. Secondly, there is insufficient knowledge and skills among police officers to (effectively) conduct investigations into online crime. Thirdly, the literature shows that the investigation also has insufficient capacity to tackle online crime, making it more difficult to retain police officers with specialist knowledge within the police organization. Finally, the complexity of online crime further complicates the detection of perpetrators. This is due, for example, to the international nature of online crime, but also to the volatility of digital data and the idea that perpetrators can more easily hide via the internet and computer programs.

The bottlenecks mentioned in the literature were similarly mentioned during the interviews and are also mentioned in the discussion session: a lack of priority, a lack of knowledge, a lack of capacity and the complexity of online crime cases. With regard to the lack of priority, respondents mainly talked about the perceived lower (social) impact of online crime, although some of the respondents considered this unjustified. In general, the work processes of the police organization still seem to be mainly aimed at traditional forms of crime. Red-handed situations, for example shoplifting, take priority over online crime cases. At the same time, it should be noted that a clear change has been visible in recent years, with various teams being specially set up to detect online crime. With regard to the lack of knowledge, respondents point to the idea that older colleagues in particular (but not exclusively) are less open to acquiring new knowledge about online crime. According to respondents, online crime is often (wrongly) seen by colleagues as something complicated. On paper, increased priority is being given to tackling online crime. This is reflected in practice, among other things, through the establishment of various specialist cyber teams. Despite these improvements, the vast majority of respondents indicate that the frontline team, the district criminal investigation teams and the cybercrime teams, for various reasons, suffer from a lack of capacity.

During the interviews it was also mentioned that the investigation of online crime is complex and that this complexity can form a bottleneck for the smooth throughput of crime. All factors that (can) make online crime complex and were mentioned in the literature study were also mentioned during the interviews. By far the most mentioned was the international nature of online crime and the perception that obtaining and retaining digital evidence is difficult due to the volatility of data in the online world, for example when it concerns IP addresses or information on servers. In addition, respondents indicate that, as a result of legislation and regulations (particularly regarding privacy), the police often do not have sufficient investigative capabilities to secure digital evidence. In addition to the literature, respondents also point out the potentially large number of victims associated with online crime and the possibility that victims often do not live within the same police region. The speed at which new forms of online crime arise also contributes to its complexity.

Finally, it was discussed that the international nature of online crime and the fact that there are often many different victims in multiple police regions can promote a lack of ownership. If it is not clear to which investigation team a case belongs, this may lead to a case not being processed. It also happens that a case is handled by several teams at the same time, without them knowing about each other.

The international respondents paint the same picture as the Dutch respondents. Although it varies from country to country, the situation in the UK, US and Australia appears even more complex due to the multitude of local police forces and the organization of police at federal and state level.

Respondents indicate, for example, that it can be difficult for case screeners to determine where a case should be processed because in many cases there are local police services that can pick up a case, but that there are also nationally operating teams that focus on organized crime and/or also have fraud and cybercrime in their duties. If a case goes to the 'wrong' team, respondents say there is a good chance that it will never be picked up.

Prosecution and the court

There is little research that addresses the bottlenecks in the throughput of cases within the Public Prosecution Service or the courts. In 2012, Leukfeldt et al. concluded that prosecutors specialized in the field of online crime receive few or no online crime cases. This was partly because the majority of cyber cases were handled by the police themselves and partly because Public Prosecution Service employees assessed cybercrime in a broad sense as traditional offenses. Furthermore, in that study, judges did not seem to experience any bottlenecks in handling online crime cases, although they do take more time to properly understand. Other bottlenecks regarding the prosecution of online crime are the same as for investigation, and relate to legislation and regulations, evidence and the complexity of online crime cases.

It is striking that respondents across the board indicate that the majority of the bottlenecks lie with the police and to a lesser extent with the Public Prosecution Service and courts. In general, it is also stated that there are fewer problems in terms of capacity at the Public Prosecution Service and courts when it comes to handling online crime. It is also clear that online crime is a priority. This does not mean, however, that no bottlenecks have been identified - especially in the Public Prosecution Service - outside the police. For example, respondents indicate that the Public Prosecution Service - and to a lesser extent courts - also has digital fears. According to respondents, the unfamiliarity with online crime and the perception of technical complexity play a role in this. A point that was raised several times during the interviews and was also mentioned by experts during the discussion sessions is that there are bottlenecks due to the definitions of online crime used. Targets of the Public Prosecution Service with regard to online crime would mainly relate to cyber-dependent crimes. Forms of cyber-enabled crime may therefore be more likely to fall by the wayside, according to respondents and experts. This is consistent with findings from the literature and, according to respondents, partly has to do with the way in which online crime is (legally) defined. Finally, during the discussion session, both respondents and experts indicate that cases can flow out because the Public Prosecution Service opts for an alternative method of settlement such as conversations with offenders instead of summons. According to respondents and experts, such interventions are not reflected in the usual statistics.

Opportunities for improvement according to the literature, actors within the criminal justice chain and experts from home and abroad

No inflow

Some suggestions are made in the literature to increase the willingness to report crimes among victims of online crime. A first recommendation concerns the use of public awareness campaigns that emphasize the need to report online crime to the police. Another suggestion is to set up uniform and thorough crime reporting systems, for example, online. Online reporting systems would increase the willingness of users to report online crime. In Australia, for example, an online reporting system has been developed specifically for online crime. Finally, the literature suggests reducing the opportunity costs (time, effort and financial costs) of reporting a crime and increasing the perceived benefits of the reporting process.

Intake and case screening

The interviews show that the reporting process is an important step in the process of inflow and throughput of online crime. In order to improve the aforementioned bottlenecks in the intake of online crime reports, the literature recommends providing tailor-made training to intake and service employees. Respondents and experts also indicated during the discussion session that proper training of intake employees and/or case screeners is of great importance to improve the quality of crime reports.

An improvement often mentioned by respondents is the national clustering and screening of crime reports. The experts who participated in the discussion sessions confirm this. An important reason given for this is that according to respondents, someone necessarily has to take control and that this is not currently happening. Centralization should ensure that more reports contain relevant information about suspects and thus increase the chances of detection. According to respondents, this could also ensure that there is a better insight into the links between reported crimes that may individually have a (too) low damage amount and are therefore not processed at the moment, but are actually related because they were committed by the same suspect(s). In addition, according to respondents, it can also increase the efficiency of police work and make it possible to identify trends and determine priorities on that basis (for example, which reports should be dealt with first). Respondents emphasize the importance of automated data enrichment and analysis, especially because online crime would appeal less to the imagination.

We would like to note that in line with the central collection and screening of online crime cases, several respondents point to existing initiatives such as the LMIO, the ECTF and Operation Centurion.

Foreign respondents indicate that the UK, US and Australia are looking to solve problems related to intake and case screening in the same way. We can learn the most from the situation in the UK and Australia. In the UK there is a centralized intake of fraud cases. Both online and offline frauds. In Australia, there are central reporting points for various forms of crime where citizens and companies can report crimes, after which the report is sent to the correct police team. For several years now, there has also been a national reporting point for online crime. It would take us too far to describe these initiatives in detail here. According to respondents, an important lesson that we can learn from both initiatives is that the central handling of declarations ensures much better registration of crime reports and that the total number of reports will simply increase quickly. However, that says nothing about the further development within the criminal justice system. Respondents indicate that capacity must also be increased further down the chain (from investigation teams to Public Prosecution Service and the courts), because otherwise there would be more reports coming in, but an increase in the inflow would result in a lack of capacity to handle cases. The respondents from the UK indicate that they see that a relatively large number of reports are still being issued immediately, but that the reports that are bundled and enriched with information about the suspect(s) ensure that the cases they forward to teams are more successfully processed. The respondent from Australia indicates that there is another positive side effect of centrally recording crime reports, namely that the satisfaction of victims has increased in recent years. Although not all reports are successfully handled, in this case the central recording of reports still meets an important need for victims.

Investigation

In particular, suggestions are made in the literature to improve the process of detecting online crime, aimed at eliminating cold feet. For example, training could ensure that detectives become more aware of the possible seriousness of these forms of crime and see that investigations are not always complex. In addition, it is mentioned that investigation teams can be reinforced with people from outside the police because, for example, some citizens have more expertise in the field of online crime than traditional police officers. Finally, studies indicate that more (inter)national cooperation is needed between investigative agencies so that knowledge about online crime, forensic methods and investigative techniques can be shared.

A point for improvement regarding the investigation phase mentioned by both respondents from the police and the Public Prosecution Service means that the investigative work does not have to continue indefinitely. Respondents note that perpetrators of online crime can have multiple victims at the same time and that it sometimes seems as if an endless number of reports can be linked together. According to some respondents, 'smarter detection' is needed. It is not always necessary to collect all the

evidence. Cost-benefit considerations can also be made more often and the results of the investment (in time and manpower) can be examined.

Prosecution and the court

Due to the limited number of studies on the inflow and throughput of online crime at the Public Prosecution Service and the courts, there are no recommendations regarding these phases in the criminal justice system. Some recommendations mentioned in the literature to improve the inflow and throughput of online crime relate to multiple phases or the entire the criminal justice system. For example, it is recommended to make long-term plans to improve employee skills, the effectiveness of existing training should be improved and it is recommended that criminal justice system organizations actively collaborate with other relevant public and private organizations, such as banks, online marketplaces, helpdesks and credit card organizations.

During the interviews, not many bottlenecks regarding the prosecution of online crime were mentioned. The same applies to possible areas for improvement. One point mentioned by respondents and raised by experts during the discussion sessions is organizing suitable courses for both public prosecutors and judges to eliminate cold feet. There is disagreement about other areas for improvement that were mentioned. For example, some officers believe that a 'cyber-enabled crimes' portfolio should be assigned to officers, while currently only 'cyber-dependent crime' portfolio holders have been appointed. Others indicate that every officer should be able to work on such matters and gain experience with them. With regard to the judiciary, one point for improvement is to organize dedicated online crime hearings. This refers to hearings at which, in principle, only online crime cases are dealt with. In this way, judges who specialize in this theme handle these cases. The interviews do show that there are different views on the importance of a specialized group of judges on this theme. And as a result of “judicial independence”, not every region currently has a cyber cluster and the cyber clusters that do exist differ in degree of maturity and formalization.

Conclusions

Although, according to research based on victimization surveys, online crime is now one of the largest forms of crime, most forms of online crime are often not recognizable as such due to the way in which they are registered in the criminal justice system. This hinders the insight into the inflow and throughput of online crime in the criminal justice system, as well as the possibilities for a targeted approach to the bottlenecks in the criminal justice system. In order to be able to study the inflow and throughput of online crime in the criminal justice system, we had to resort to developing predictive text mining models to classify BVH registrations. This turned out not to be possible for all forms of

online crime, so we were unable to conduct inflow and throughput analyses for malware, ransomware, DDoS attacks, online threats, online stalking, online libel/slander/insult, other online scams and money muling. It would help enormously if a more extensive and regularly updated list of specific crime types was used when registering crime, so that the various types could be mapped out in a systematic manner. This improves the intelligence position, enables a more targeted approach to the bottlenecks in the criminal justice system and prevents new studies from having to perform complex analyses again in an attempt to map the inflow and throughput.

The research shows that there are obstacles to both the inflow and the throughput of online crime in the criminal justice system. While the prevalence of online crime is estimated to be very high based on victimization surveys, the low inflow figures are particularly striking in the quantitative analyzes of BVH registrations. Cyber-enabled crime is approximately 4 times more common than cyber-dependent crime, but most forms of online crime occur in less than 1% (the maximum is 4% for all cyber-enabled crime together) of the BVH registrations. This picture fits with what is known about the lower willingness to report online crime compared to traditional crime: many cases of online crime simply never enter the criminal justice system.

The experts interviewed see the biggest challenges at the front of the criminal justice system, with the police. In particular, the intake of online crime leaves much to be desired because knowledge and expertise are lacking. This would mean that in the case of online crime, a report is not always recorded and sometimes only a notification is registered, which means that the largest source of inflow (crime reports by citizens and companies) comes to a standstill. On the one hand, this picture is consistent with our findings. After all, we noted that while the prevalence of online crime is estimated to be very high based on victimization surveys, in our quantitative analyzes of BVH registrations the low inflow figures are striking. There is therefore a big difference between victimization experienced by citizens – and reported in victimization surveys – and victimization recorded by the police. Furthermore, in the quantitative analyses we indeed found BVH registrations of online crime without a crime report. This concerned approximately a quarter of the registrations. However, this is not unique to online crime, because in other forms of crime we saw even higher percentages of BVH registrations without reporting. It is therefore advisable to look in further research into the discrepancy between experienced victimization by citizens and victimization registered by the police. Furthermore, it is important to make a further analysis of the situations in which the police register a notification instead of recording a report for different forms of crime. According to the experts interviewed, the lack of knowledge and expertise at the police intake would also lead to a low quality of the reports, which could lead to problems in all subsequent steps in the criminal justice system.

If victims of online crime have reported it, it appears that in 90% of cases no suspect is identified. This low percentage in combination with the already very limited inflow means that few cases flow through the criminal justice system. The percentage of BVH registrations with a report in which at least one suspect is identified differs little between cyber-dependent and cyber-enabled crimes, although it is striking that the percentages of registrations with suspect(s) are low in those forms of online crime that are registered most often. Apparently, in those cases that determine the largest part of the police workload, it is the least successful in linking suspects to them. The low percentage of online purchase and sales fraud (2%) is particularly striking, as bank account information should often be available for this form.

Although respondents mentioned various reasons why detection of online crime is difficult and why there is cold feet, low clearance rates are not unique to online crime. We also see low percentages for property crime (in 12% of BVH registrations with a report, we also saw at least 1 suspect registered), while these are considerably higher for offline fraud (31%) and especially for violent crimes (59%). The difference with violent crimes is perhaps not so surprising, because in those cases there will often have been direct contact between perpetrator and victim, which will lead to offender information and clear investigative leads. However, the major difference between offline and online fraud cases cannot be explained in this way. Although we cannot rule out in this study that the observed differences are related to differences in investigative efforts, the interviews show that the presence of a perpetrator or investigative lead plays a major role in the choice to take on cases. Respondents indicated that this is often lacking in online crime, meaning that cases are already lost during case screening or are not successfully processed. However, the lack of offender information or investigative leads is not unique to online crime, as this also often occurs in property crimes.

When the police manage to identify suspects, the vast majority of them turn out to be adult suspects. The ratio between adult and minor suspects hardly differs between cyber-dependent and cyber-enabled crimes. About a third of both adult and minor suspects of online crime go all the way to court. We also saw that a significant proportion of adult suspects received other or unknown settlements from the police or the Public Prosecution Service (43%), while this also occurred to a lesser extent among minor suspects (33%). Underage suspects were dealt with by the police more often than adult suspects.

Although there appears to be a consensus among respondents that the greatest challenges in the inflow and throughput of online crime within the criminal justice system lie within the police, the quantitative analyses show that dismissals are registered for a significant portion of the suspects submitted to the Public Prosecution Service. We also see this picture for the three other types of

offenses with which we compared online crime. We have not investigated the reasons for the dismissals, but the picture is therefore not unique to online crime. In order to improve the inflow and throughput of online crime within the criminal justice system, it seems however wise to focus primarily on the bottlenecks and challenges within the police.

8. Literatuurverwijzingen

Akkermans, M., Kloosterman, R., Moons, E., Reep, C. & Tummers-van der Aa, M. (2022). *Veiligheidsmonitor 2021*. CBS.

Algemene Rekenkamer (2012). *Prestaties in de strafrechtketen.* Algemene Rekenkamer.

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

Bidgoli, M. & Grossklags, J. (2016). End user cybercrime reporting: What we know and what we can do to improve it. In B. Cartwright, L. Y. C. Lau & G. Weir (Eds.), *IEEE International Conference on Cybercrime and Computer Forensic.* ICCCF.

Bidgoli, M., Knijnenburg, B. P. & Grossklags, J. (2016). When cybercrimes strike undergraduates. In *2016 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1-10). IEEE.

Bidgoli, M., Knijnenburg, B. P., Grossklags, J. & Wardman, B. (2019). Report now. Report effectively. Conceptualizing the industry practice for cybercrime reporting. In *2019 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1-10). IEEE.

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

Bossler, A. M. & Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing, 35*(1), 165–181.

Brown, C. S. D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology, 9*(1), 55–119.

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

Centraal Bureau voor de Statistiek (CBS) (2020). *Veiligheidsmonitor 2019.* CBS.

Centraal Bureau voor de Statistiek (CBS) (2023). Geregistreerde criminaliteit; soort misdrijf, regio. https://opendata.cbs.nl/statline/portal.html?_la=nl&_catalog=CBS&tableId=83648NED&_theme=406

Cross, C. (2018). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice, 55*, 1–12.

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

Custers, B. (2018). Nieuwe online opsporingsbevoegdheden en het recht op privacy. Een analyse van de Wet computercriminaliteit III. *Justitiële verkenningen, 5*, 100-114.

De Cuyper, R. H. & Weijters, G. (2016). *Cybercrime in cijfers. Een verkenning van de mogelijkheden om cybercrime op te nemen in de Nationale Veiligheidsindices.* WODC.

De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M. & Martin, R. (2020). A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists. *Policing: A Journal of Policy and Practice, 15*(2), 1429–1445.

Directie Strafrechtketen (2020). *Strafrechtketen 2020. Factsheet strafrechtketenmonitor.* Ministerie van Justitie en Veiligheid.

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

Domenie, M. M. L., Leukfeldt, E. R., Van Wilsem, J. A., Jansen, J. & Stol, W. (2013). *Slachtofferschap in een gedigitaliseerde samenleving: Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit.* Boom Juridische uitgevers.

Felix, A. E. (2013). *Ongewenste uitstroom in de strafrechtketen. Oorzaken en oplossingen.* Andersson Elffers Felix.

Goodman, M. D. (1997). Why the police don't care about computer crime. *Harvard Journal of Law & Technology, 10*(3), 465-494.

Goodman, M. D. & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. *International Journal of Law and Information Technology, 10*(2), 139-223.

Goucher, W. (2010). Being a cybercrime victim. *Computer Fraud & Security, 2010*(10), 16-18.

Goudriaan, H., Nieuwbeerta, P. & Wittebrood, K. (2005). Overzicht van onderzoek naar determinanten van aangifte doen bij de politie: theorieën, empirische bevindingen, tekortkomingen en aanbevelingen. *Tijdschrift voor Veiligheid en Veiligheidszorg, (4)*1, 27-48.

Goudriaan, H., Wittebrood, K. & Nieuwbeerta, P. (2006). Neighbourhood characteristics and reporting crime: Effects of social cohesion, confidence in police effectiveness and socio-economic disadvantage. *British Journal of Criminology, 46*(4), 719–742.

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

Hadlington, L., Lumsden, K., Black, A. & Ferra, F. (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., Whelan, C. & Chang, L. (2018). The challenges facing specialist police cyber-crime units: An empirical analysis. *Police Practice and Research, 19*(6), 519–536.

Harrendorf, S. (2018). Attrition in and performance of criminal justice systems in Europe: A comparative approach. *European Journal on Criminal Policy and Research, 24*(1), 7–36.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20–40.

Holt, T. J., Burruss, G. W. & Bossler, A. M. (2019). An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents. *Policing and Society, 29*(8), 906-921.

Holt, T. J., Van Wilsem, J., Van de Weijer, S. & Leukfeldt, E. R. (2018). Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review, 38*(2), 187-206.

Inspectie Justitie en Veiligheid (2019a). *Selectie en toewijzing in de opsporing.* Ministerie van Justitie en Veiligheid.

Inspectie Justitie en Veiligheid (2019b). *Periodiek beeld opsporing.* Ministier van Justitie en Veiligheid.

Jewkes, Y. and Yar, M. (2008). Policing cybercrime, emerging trends and future challenges. In T. Newman (Ed.), *Handbook of Policing* (pp. 580-605). Willan.

Johnson, H. & Krone, T. (2007). Internet purchasing: perceptions and experiences of Australian households. *Trends and Issues in Crime and Criminal Justice,* 330, 1-6.

Jong, L., Leukfeldt, E. R., & van de Weijer, S. (2018). Determinanten en motivaties voor intentie tot aangifte na slachtofferschap van cybercrime. *Tijdschrift voor Veiligheid, 17*(1–2), 66–78.

Kääriäinen, J. & Sirén, R. (2011). Trust in the police, generalized trust and reporting crime. *European Journal of Criminology, 8*(1), 65-81.

Karie, N. M. & Venter, H. S. (2015). Taxonomy of challenges for digital forensics. *Journal of forensic sciences, 60*(4), 885-893.

Kemp, S. (2020). Fraud reporting in Catalonia in the Internet era: Determinants and motives. *European Journal of Criminology, 19*(5), 1-22.

Kuhn, M. & Wickham, H. (2020). Tidymodels. A collection of packages for modeling and machine learning using tidyverse principles.

Landman, W. (2023). *Politiewerk aan de horizon. Technologie, criminaliteit en de toekomst van politiewerk*. Den Haag: Politie en Wetenschap.

Lee, J. R., Holt, T. J., Burruss, G. W. & Bossler, A. M. (2021). Examining English and Welsh detectives' views of online crime. *International Criminal Justice Review, 31*(1), 20-39.

Leukfeldt, E. R. (2017). *Cybercriminal networks: origin, growth and criminal capabilities.* Eleven International Publishing.

Leukfeldt, E. R., Domenie, M. M. L. & Stol, W. (2010). *Verkenning Cybercrime in Nederland 2009.* Boom Juridische Uitgevers.

Leukfeldt, E. R., Notté, R. & Malsch, M. (2018). *Slachtofferschap van online criminaliteit. Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit.* WODC.

Leukfeldt, E. R., Veenstra, S., Domenie M., Stol, W. (2012). *De strafrechtketen in een gedigitaliseerde samenleving. Een onderzoek naar de strafrechtelijke afhandeling van cybercrime.* Sdu Uitgevers.

Leukfeldt, R., Veenstra, S., & Stol, W. (2013). 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.

Moitra, S. D. (2005). Developing policies for cybercrime. *European Journal of Crime, Criminal Law and Criminal Justice, 13*(3), 435–464.

Morgan, A., Dowling, C., Brown, R., Mann, M., Voce, I. & Smith, M. (2016). *Evaluation of the Australian Cybercrime Online Reporting Network.* Australian Institute of Criminology.

Odinot, G., Verhoeven, M. A., Pool, R. L. D. & de Poot, C. J. (2017). *Organised cybercrime in the Netherlands. Empirical findings and implications for law enforcement.* WODC.

Reitsma, J. & Heijmen, T. (2015). *Nog niet uitgestroomde strafzaken: Een kwalitatief onderzoek.* Significant.

Rokven, J. J., Weijters, G. & van der Laan, A. M. (2017). *Jeugddelinquentie in de virtuele wereld. Een nieuw type daders of nieuwe mogelijkheden voor traditionele daders?* WODC.

Struiksma, N., de Vey Mestdagh, C. N. J. V. & Winter, H. B. (2012). *De organisatie van de opsporing van cybercrime door de Nederlands politie.* Politie & Wetenschap.

Tarling, R., & Morris, K. (2010). Reporting crime to the police. *British Journal of Criminology, 50*(3), 474–490.

Tollenaar, N. & Rokven, J., Macro, D., Beerthuizen, M. & van der Laan, A.M. (2019). *Predictieve textmining in politieregistraties. Cyber- en gedigitaliseerde criminaliteit.* WODC.

Torrente, D., Gallo, P. & Oltra, C. (2017). Comparing crime reporting factors in EU countries. *European Journal on Criminal Policy and Research, 23*(2), 153–174.

Toutenhoofd-Visser, M. H., Veenstra, S., Domenie, M.M.L., Leukfeldt, E.R. & Stol, W. (2009). *Politie en Cybercrime. Intake en Eerste Opvolging. Een onderzoek naar de intake van het werkaanbod cybercrime door de politie.* NHL Hogeschool.

Van den Eeden, C. A. J., van Berkel, J. J., Lankhaar, C. C. & de Poot, C.J. (2021). *Opsporen, vervolgen en tegenhouden van cybercriminaliteit.* WODC.

Van de Weijer, S. & Bernasco, W. (2016). *Aangifte- en meldingsbereidheid: Trends en determinanten.* 113. NSCR.

Van de Weijer, S. G. A., Leukfeldt, E. R. & Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology, 16*(4), 486–508.

Van de Weijer, S. G. A., Leukfeldt, E. R. & Van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing, 43*(1), 17–34.

Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research, 8*(2), 183-205.

Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology, 22*(1-2), 45-63.

Wijffels, J. (2022). *udpipe: Tokenization, parts of speech tagging, lemmatization and dependency parsing with the 'UDPipe' 'NLP' toolkit.* R package version 0.8.9.

Yar, M. & Steinmetz, K. F. (2019). *Cybercrime and Society (3rd ed.)*. Sage Publications.

9. Bijlagen

Bijlage 1: Frequentieverdelingen en rubriceringen van in BOSZ en GPS geregistreerde afhandelingen/afdoeningen

Het databestand met BOSZ-gegevens bevatte 48.023 rijen gegevens die op basis van uniek BVH-registratienummer gekoppeld konden worden aan de steekproef van 300.000 BVH-registraties. In Tabel 20 wordt de frequentieverdeling van alle in het BOSZ-bestand geregistreerde afhandeling codes weergegeven alsmede hoe deze voor dit onderzoek zijn gerubriceerd.

Tabel 20 BOSZ frequentieverdeling en rubricering

Originele 'Afhandeling code'	Aantal	Rubricering
Casusoverleg (jeugd)	52	Overig/onbekend
Geringe hoeveelheid drugs voor eigen gebruik	168	Overig/onbekend
Gesignaleerd	112	Overig/onbekend
Onbekend	3.499	Overig/onbekend
Overg. andere opsp. inst.	3.740	Overig/onbekend
Retour OM Beoordelaar	96	Overig/onbekend
Valse Naam	43	Overig/onbekend
Inzenden HALT	631	Politiestrafbeschikking/HALT/reprimande
Politiestrafbeschikking	1.156	Politiestrafbeschikking/HALT/reprimande
Reprimande (jeugd en winkeldiefstal)	93	Politiestrafbeschikking/HALT/reprimande
Reprimande (jeugd en/of winkeldiefstal)	5	Politiestrafbeschikking/HALT/reprimande
Reprimande (jeugd)	347	Politiestrafbeschikking/HALT/reprimande
Inzenden OM	38.062	Inzenden ===> zie Tabel 21
Inzenden OM-overig	19	Inzenden ===> zie Tabel 21
Totaal	**48.023**	

Voor BVH-registraties waarbij sprake was van inzending naar het Openbaar Ministerie zijn GPS-registraties opgevraagd. Het databestand met GPS-gegevens bevatte 38.188 rijen gegevens die op basis van de unieke combinatie van BVH-registratienummer en een persoonsleutel aan de steekproef van 300.000 BVH-registraties konden worden gekoppeld. GPS-registraties hebben betrekking op strafbare feiten en sommige registraties bevatten informatie over de afdoeningen voor twee verschillende feiten. Omdat we unieke BVH-registraties als uitgangspunt nemen voor onze analyses, hebben we de informatie over verschillende feiten moeten samennemen. Als bij tenminste 1 feit 'dagvaarden' stond geregistreerd dan hebben we dat laten prevaleren. Als er vervolgens bij 1 feit 'OM-strafbeschikking' of 'transactie' stond, dan hebben we dat laten prevaleren boven sepot. In Tabel 21 wordt de frequentieverdeling van alle in het GPS-bestand geregistreerde afdoeningen weergegeven alsmede hoe deze voor dit onderzoek zijn gerubriceerd.

Tabel 21 GPS frequentieverdeling en rubricering

Afdoening Feit 1	Afdoening Feit 2	Aantal	Rubricering
0	0	967	Overig/onbekend
Administratief beëindigd	0	7	Overig/onbekend
Lik op stuk	0	5	Overig/onbekend
Onvoorwaardelijk sepot	0	7.081	Sepot
Overdracht	0	4	Overig/onbekend
Voorwaardelijk sepot	0	1.208	Sepot
0	Onvoorwaardelijk sepot	424	Sepot
Onvoorwaardelijk sepot	Onvoorwaardelijk sepot	1.590	Sepot
Overdracht	Overdracht	9	Overig/onbekend
Voorwaardelijk sepot	Onvoorwaardelijk sepot	2	Sepot
0	Voorwaardelijk sepot	132	Sepot
Onvoorwaardelijk sepot	Voorwaardelijk sepot	2	Sepot
Voorwaardelijk sepot	Voorwaardelijk sepot	260	Sepot
<<Missing>>	<<Missing>>	6.299	Overig/onbekend
OM-strafbeschikking	0	2.771	Strafbeschikking/transactie
OM-strafbeschikking	OM-strafbeschikking	645	Strafbeschikking/transactie
OM-strafbeschikking	Voorwaardelijk sepot	1	Strafbeschikking/transactie
Onvoorwaardelijk sepot	Transactie	2	Strafbeschikking/transactie
Transactie	0	396	Strafbeschikking/transactie
Transactie	Onvoorwaardelijk sepot	4	Strafbeschikking/transactie
Transactie	Transactie	105	Strafbeschikking/transactie
0	Dagvaarden	8	Dagvaarden/voegen
Dagvaarden	0	8.214	Dagvaarden/voegen
Dagvaarden	Dagvaarden	7.932	Dagvaarden/voegen
Dagvaarden	Onvoorwaardelijk sepot	48	Dagvaarden/voegen
Dagvaarden	Voegen ad informandum	4	Dagvaarden/voegen
OM-strafbeschikking	Dagvaarden	1	Dagvaarden/voegen
Onvoorwaardelijk sepot	Dagvaarden	6	Dagvaarden/voegen
Voegen ad informandum	0	1	Dagvaarden/voegen
Voegen ter berechting	0	34	Dagvaarden/voegen
Voegen ter berechting	Voegen ter berechting	26	Dagvaarden/voegen
Totaal		**38.188**	

Bijlage 2: Definities van typen online criminaliteit

Type online criminaliteit	Definitie	Bron
1. Hacking	*Ongeautoriseerd toegang tot ICT; inloggen op een computer, website, e-mailaccount, (sociale) netwerksite of (online) smartphone applicaties zonder toestemming (MZJ + Leukfeldt et al., 2009). Met behulp van ICT wachtwoorden of gegevens veranderen of misbruiken (bijvoorbeeld ongeautoriseerd gebruikmaken van een wachtwoord) zonder toestemming (MZJ + Leukfeldt et al., 2009).*	Tollenaar (2019)
2. Malware	*Malware is een verzamelnaam voor verschillende typen kwaadaardige software. Hieronder vallen typen malware zoals virussen, wormen en Trojaanse paarden.*	Leukfeldt *et al.* (2015); Van der Wagen & Oerlemans (2020)
3. Ransomware	*Computerbestanden (computers, informatiesystemen, websites) gijzelen/versleutelen met behulp van software die pas na betaling of ander soortige tegenpresentatie worden vrijgegeven (THTC; Bernaards et al., 2012).*	Tollenaar (2019)
4. DDoS-aanval	*Een actie waarbij een computer, een systeem of telecommunicatienetwerk (bijvoorbeeld een website of mailserver) opzettelijk overbelast wordt en niet meer beschikbaar/bereikbaar is (THTC; Bernaards et al., 2012).*	Tollenaar (2019)
5. Online bedreiging	*Dreigementen van fysieke aard via online medium, zoals via e-mail, website(s) en sociale media (hieronder vallen ook smartphone applicaties waarbij gebruik wordt gemaakt van het internet, zoals WhatsApp of Snapchat), richting persoon en/of goederen (MZJ + Van der der Heijden et al., 2017).*	Tollenaar (2019)
6. Online stalking	*Wederrechtelijk stelselmatig opzettelijk inbreuk maken op een ander zijn/haar persoonlijke levenssfeer met het oogmerk die ander te dwingen iets te doen, niet te doen of te dulden dan wel vrees aan te jagen.*	Tollenaar (2019)

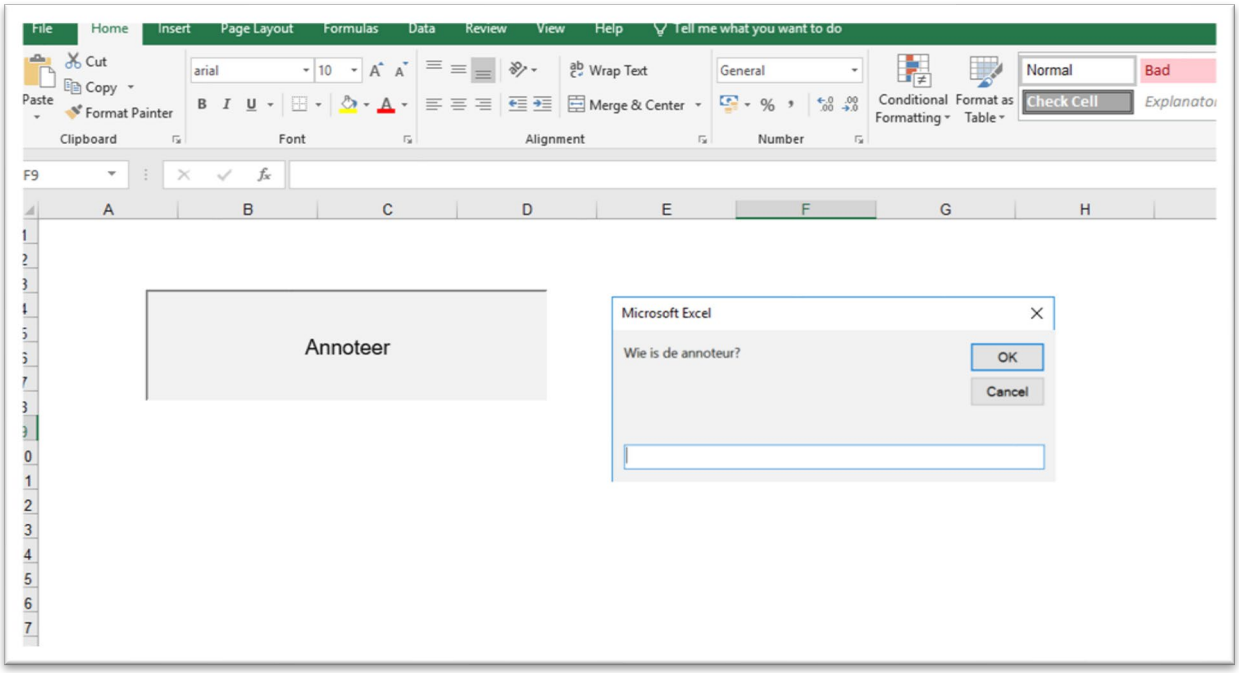
7. Online smaad/laster/belediging	*Het via ICT uitvoeren en/of bedreigen met smaad, smaadschrift of openbaring van een geheim, laster of belediging. Smaad wordt gedefinieerd als opzettelijk iemands eer of goede naam aanranden, door telastlegging van een bepaald feit, met het kennelijke doel om daaraan ruchtbaarheid te geven. Laster wordt gedefinieerd als smaad waarbij sprake is van onwaarheden. Van belediging wordt gesproken wanneer er met opzet kwaad over iemand wordt gesproken, zonder dat er sprake is van smaad.*	Tollenaar (2019)
8. Online oplichting	*Iemand die via een online medium, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, hetzij (1) door het aannemen van een valse naam of van een valse hoedanigheid, (2) hetzij door listige kunstgrepen, (3) hetzij door een samenweefsel van verdichtsels, iemand beweegt tot de afgifte van enig goed, tot het verlenen van een dienst, tot het ter beschikking stellen van gegevens, tot het aangaan van een schuld of tot het teniet doen van een inschuld.*	Art. 326 Sr; *eigen toevoeging*
8.1 Phishing	*Phishing is een poging om via digitale middelen (e-mail, sms, whatsapp, snapchat) persoonlijke gegevens (gebruikersnamen, wachtwoorden, IP-adressen en bankgegevens) van mensen te ontfutselen, vaak door zich voor te doen als een vertrouwde instantie. Er zijn grofweg drie methoden: (1) een list om mensen zo ver te krijgen dat ze persoonsgegevens afstaan (2) een bijlage die malware bevat (3) een link naar een website.*	Leukfeldt *et al.* (2015); Van der Wagen & Oerlemans (2020)
8.2 Online identiteitsfraude	*Het via ICT stelen van persoonsgegevens (bijvoorbeeld door phishing, keyloggers of spyware) (Leukfeldt et al., 2009). Het creëren van een fictieve identiteit middels ICT (Leukfeldt et al., 2009). Het onrechtmatig gebruikmaken van persoonsgegevens op internet (THTC; Bernaards et al., 2012).*	Tollenaar (2019)

8.3 Online aan- en verkoopfraude	*Iets verkocht via internet, het geld gekregen van de koper, maar het artikel nooit opgestuurd (MZJ). Iets gekocht en ontvangen via internet, maar nooit betaald (MZJ). Dit geldt ook als het product niet wordt geleverd zoals afgesproken. Naast producten vallen ook diensten onder de definitie.*	Tollenaar (2019); *eigen toevoeging*
8.4 VIN-fraude	*Bij vriend-in-noodfraude doet een dader zich voor als bekende van het slachtoffer. Via een WhatsApp bericht geeft 'de bekende' aan een nieuw telefoonnummer te hebben en snel geld nodig te hebben. De dader vraagt het geld over te maken op een bankrekening. Deze vorm van fraude komt op WhatsApp verreweg het meeste voor maar kan ook plaatsvinden via e-mail, SMS, Snapchat en Telegram.*	OM (2020); Politie (2020)
8.5 Helpdesk-fraude	*Individuen worden telefonisch benaderd door iemand die zich voordoet als medewerker van een bepaald bedrijf (zoals Microsoft) en aangeeft dat er problemen zijn met software op de computer van het slachtoffer. Vervolgens probeert de oplichter het slachtoffer (kwaadaardige) software te laten installeren of de oplichter toegang te geven tot de computer. Zo kunnen persoonlijke gegevens worden verkregen, accounts worden overgenomen of geld worden afgetroggeld.*	Wikipedia; Politie (2020)
8.6 Overig	*Alle vormen van online oplichting die niet in een van de eerdere categorieën van online oplichting vallen.*	
9. Money muling	*Een geldezel (money mule) is iemand die bewust of onbewust zijn of haar bankrekening ter beschikking stelt voor criminele activiteiten.*	Aston *et al.* (2009); Bekkers *et al.* (2020)

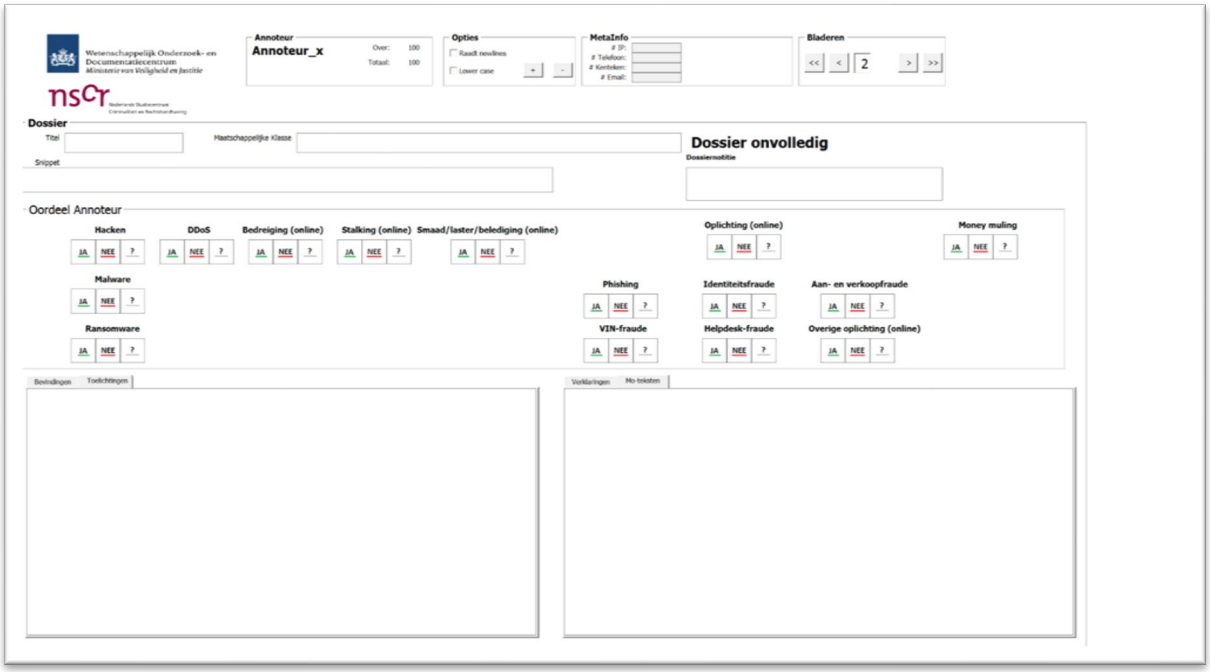
Bijlage 3: Query online criminaliteit (Tollenaar *et al.*, 2019)

(hack% | gehack% | computervredebreuk | {computer vredebreuk} | {computer vrede breuk} | computercriminaliteit | {computer criminaliteit} | computerfraude | {computer fraude} | botnet | {bot net} | antivirus | virus | {anti virus} | virussen | virusen | defaced | defacing | facing | cyber% | %__ware | trojan | trojans | trojaan | trojaans | keylogger | keyloggen | {key logger} | wachtwoord | password | bitcoin | bitcoins | versleutel | versleutelt | versleuteld | versleuteled | versleutelen | versleutelde | ddos% | geddos% | {d dos} | ransom% | proxy | proxyserver | proxyservice | {proxy server} | {proxy service} | ipadres | {ip adres} | computerbestanden | {geautomatiseerd werk} | fishing | fisjing | fishjing | phising | phisjing | pfishing | vishing | visjing | spo_fen | spo_fing | spo_phing | spo_phen | internetoplichting | {internet oplichting} | marktplaatsoplichting | LMIO)
OR
((dreig% | bedreig% | afdreig% | afpers% | stalk% | identiteitsfraude | {identiteits fraude} | identiteitfraude | {identiteit fraude} | identiteitsdiefstal | {identiteits diefstal} | {valse identiteit} | {gestolen identiteit} | aankoopfraude | verkoopfraude | fraude | oplichting | opgelicht | {niet geleverd} | {nooit geleverd} | {niet opgestuurd} | {nooit opgestuurd} | {niet betaald} | {nooit betaald} | sabotage | gesaboteerd | gesabooteerd | gesabotteerd | gesabotteerd | gijzel | gijzelen | gijzelt | gegijzelt | gegijzeld | gegijzelde | gegijzelden | platleggen | blokkeren | geblokkeerd | chantage | chanteren | gechanteerd |gechanteerd)
AND
(whatsapp | whatsap | whatsappen | gewhatsappt | whatsappte | whatsapte| chat% | gechat%| twitter | tweet | getweet | facebo_k | facebo_ken | gefacebo_kt | {face book} | {face boek}| instagram | {insta gram}| snapchat | {snap chat}| skype | dumperd | dumpert | messenger | youtube | {you tube} | linkedin | {linked in} | linktin | {linkt in} | linkdin | {linkd in} | hyves | google_ | googleplus | {google plus} | webwinkel | webshop | marktplaats | {markt plaats} | speurders | ebay | {e bay} | amazon | microsoft | gmail | hotmail | socialmedia | {social media} | socialemedia | {sociale media} | online | {on line} | digitaal | digitale | digitalen | cyber% | internet | internette | internetten | geinternet | {inter net} | %site | sms | smste | smsen | gesmst | gesmsd | gesmsdt | imessage | apps | appen | geappt | webcam | webcams | webcammen | webcamt | webcamde | gewebcamd | gewebcamt | ipadres | {ip adres} | %account | %accounts | screenshot | screensthots | nicknaam | niknaam | nickname | nicknames | nicknamen | {nick namen} | gebruikersnaam | username))

Bijlage 4: Annotatietool



Figuur 4 Excel VBA macro voor annotatie van BVH-registraties (I)



Figuur 5 Excel VBA macro voor annotatie van BVH-registraties (II)

Bijlage 5: Instructies voor annoteurs

In- en exclusiecriteria

Type online criminaliteit	Inclusie	Exclusie
1. Hacking	- Website defacen - Ransomware - Microsoft-scam (ook poging tot) - Malware - Tikkie-fraude - URL aanpassen om toegang te krijgen tot niet-toegankelijk bedoelde delen van de pagina	- Poortscan om te zoeken naar kwetsbaarheden - Ethisch hacken (toestemming van bedrijf d.m.v. overeenkomst/Reponsible Disclosure/CVD) - Helpdeskfraude waarbij geld moet worden overgemaakt naar een kluisrekening
2. Malware	- Ransomware	
3. Ransomware		
4. DdoS-aanval	- DoS-aanval - E-mail bomb	
5. Online bedreiging		
6. Online stalking		- Indien er alleen sprake is van lastig vallen (wederrechtelijkheid en stelselmatigheid is vereist)
7. Online smaad/laster/belediging	- Online discriminatie - (dreigen met) verspreiden van naaktfoto's of andere privacygevoelige informatie	- Indien iemand niet in het openbaar wordt beledigd
8. Online oplichting		
8.1 Phishing	- Indien iemand vanuit een valse hoedanigheid om wachtwoorden vraagt	
8.2 Online identiteitsfraude	- VIN-fraude - Microsoft-scam - Tikkie-fraude	- Indien iemand een huis verhuurd of te koop aanbiedt

		dat niet van de dader is (wel als dit via een nepprofiel is)
8.3 Online aan- en verkoopfraude	- Liegen over of verzwijgen van staat van goederen	- Online contact gelegd/product gezien, maar offline afhandeling - Gestolen goederen aanbieden op internet
8.4 VIN-fraude		
8.5 Helpdesk-fraude	- Indien slachtoffer zelf een (frauduleus) helpdesk-nummer belt - Indien iemand zich voordoet als bankmedewerker en geld moet overmaken naar zogenaamde 'kluisrekening'	
8.6 Overige identiteitsfraude		
9. Money muling		- Indien een verdachte geldezels ronselt

Overige instructies

Let op algemeen:

- Indien het gaat om online delicten die een verdachte eerder heeft gepleegd/waar iemand eerder slachtoffer van is geworden, dan **niet** annoteren. Dit kan bijvoorbeeld in een verhoor worden besproken.
- Bedreiging/stalking/smaad via de telefoongesprek is geen online bedreiging/stalking/smaad. Wel online indien (ook) via e-mail, sms of ander online medium.
- Let op! Een registratie pas als 'money muling' annoteren indien de registratie gaat om een verdachte van money muling. Dus niet wanneer bijvoorbeeld een oplichter gebruik heeft gemaakt van money mules.

Notities maken:

- Indien een registratie weinig informatie bevat en onvolledig lijkt (voorbeelden waren een rechtshulpverzoek, aantekening van een diender, of melding uit andere eenheid).
    - Notitie: Let op! Lijkt geen volledige registratie.

- Indien een registratie online criminaliteit betreft, maar niet in een categorieën is te plaatsen.
    - Notitie: Let op! Wel online criminaliteit.
- Indien er sprake is van een melding van een niet-strafbare gedraging volgens verbalisant (bijvoorbeeld een verward persoon) wel annoteren welk delict het betreft, maar ook een notitie maken.
    - Notitie: Let op! Melding niet strafbare gedraging.
- Indien er sprake is van een aangifte die is ingetrokken de registratie wel annoteren, maar ook een opmerking maken.
    - Notitie: Let op! Aangifte ingetrokken, goederen toch geleverd.

<u>Voorbeelden van online delicten en bijbehorende categorieën:</u>

- Botnets = netwerk van geïnfecteerde computers met malware
    - Altijd malware
    - Altijd computervredebreuk
- Tikkie-fraude = er wordt een betaalverzoek van 0,01 euro verstuurd naar een slachtoffer, bij betaling van de 0,01 euro worden de gegevens afgevangen en gebruikt
    - Altijd online oplichting (phishing + identiteitsfraude)
    - Altijd computervredebreuk (want ongeautoriseerd toegang tot bankrekening)
- Microsoft fraude
    - Altijd online oplichting (helpdeskfraude + identiteitsfraude)
    - Altijd computervredebreuk
    - Soms phishing indien duidelijk wordt dat inloggegevens bank zijn afgevangen. Dit is bijvoorbeeld het geval indien de bedragen die slachtoffers denken over te maken niet overeenkomen met uiteindelijke afgeschreven bedragen.
- Sextortion = het gebruiken van seksueel getint beeldmateriaal als chantagemiddel
    - Vaak smaad/laster/belediging
    - Soms sprake van computervredebreuk
- Ransomware
    - Altijd computervredebreuk
    - Altijd malware
- Malware
    - Altijd computervredebreuk
- Webwinkel levert product niet na betaling
    - Altijd aan-/verkoopfraude
    - In principe geen ID-fraude, tenzij heel duidelijk dat het een neppe webwinkel betreft, zoals een neppe airbnb site. Enkel offline gaan van webwinkel is niet voldoende voor ID-fraude.

- Account hijacking
    - Altijd computervredebreuk
    - Soms ook online identiteitsfraude indien bijvoorbeeld bestellingen worden geplaatst

Bijlage 6: Kruistabellen interbeoordelaarsbetrouwbaarheid (n=500)

1. Hacking

Cohen's kappa = 0.90 (p<.001)		Tweede annoteur		
		Weet niet	Nee	Ja
Eerste annoteur	Weet niet	1	0	2
	Nee	0	324	12
	Ja	1	10	150

2. Malware

Cohen's kappa = 0.81 (p<.001)		Tweede annoteur		
		Weet niet	Nee	Ja
Eerste annoteur	Weet niet	1	0	0
	Nee	0	486	1
	Ja	0	3	9

3. Ransomware

Cohen's kappa = 0.92 (p<.001)		Tweede annoteur		
		Weet niet	Nee	Ja
Eerste annoteur	Weet niet	0	0	0
	Nee	0	493	1
	Ja	0	0	6

4. DDoS-aanval

Cohen's kappa = 0.86 (p<.001)		Tweede annoteur		
		Weet niet	Nee	Ja
Eerste annoteur	Weet niet	0	0	0
	Nee	0	496	1
	Ja	0	0	3

5. Online bedreiging

Cohen's kappa = 0.83 (p<.001)		Tweede annoteur		
		Weet niet	Nee	Ja
Eerste annoteur	Weet niet	0	2	3
	Nee	0	454	6
	Ja	1	5	29

6. Online stalking

Cohen's kappa = 0.57 (p<.272)		Tweede annoteur		
		Weet niet	Nee	Ja
Eerste annoteur	Weet niet	0	1	0
	Nee	0	482	2
	Ja	0	8	7

7. Online smaad/laster/belediging

Cohen's kappa = 0.62 (p<.319)		Tweede annoteur		
		Weet niet	Nee	Ja
Eerste annoteur	Weet niet	1	0	0
	Nee	1	468	13
	Ja	0	3	14

8. Online oplichting

Cohen's kappa = 0.92 (p<.001)		Tweede annoteur		
		Weet niet	Nee	Ja
Eerste annoteur	Weet niet	0	0	0
	Nee	0	206	12
	Ja	2	8	273

8.1 Phishing

Cohen's kappa = 0.85 (p<.001)		Tweede annoteur		
		Weet niet	Nee	Ja
Eerste annoteur	Weet niet	0	1	0
	Nee	0	411	10
	Ja	0	10	68

8.2 Online identiteitsfraude

Cohen's kappa = 0.90 (p<.001)		Tweede annoteur		
		Weet niet	Nee	Ja
Eerste annoteur	Weet niet	0	0	1
	Nee	0	288	13
	Ja	2	12	184

8.3 Online aan- en verkoopfraude

Cohen's kappa = 0.95 (p<.001)		Tweede annoteur		
		Weet niet	Nee	Ja
Eerste annoteur	Weet niet	0	0	0
	Nee	1	401	1
	Ja	1	6	90

8.4 VIN-fraude

Cohen's kappa = 0.97 (p<.001)		Tweede annoteur		
		Weet niet	Nee	Ja
Eerste annoteur	Weet niet	0	0	0
	Nee	1	464	2
	Ja	0	0	33

8.5 Helpdesk-fraude

Cohen's kappa = 0.89 (p<.001)		Tweede annoteur		
		Weet niet	Nee	Ja
Eerste annoteur	Weet niet	0	0	0
	Nee	0	464	4
	Ja	0	3	29

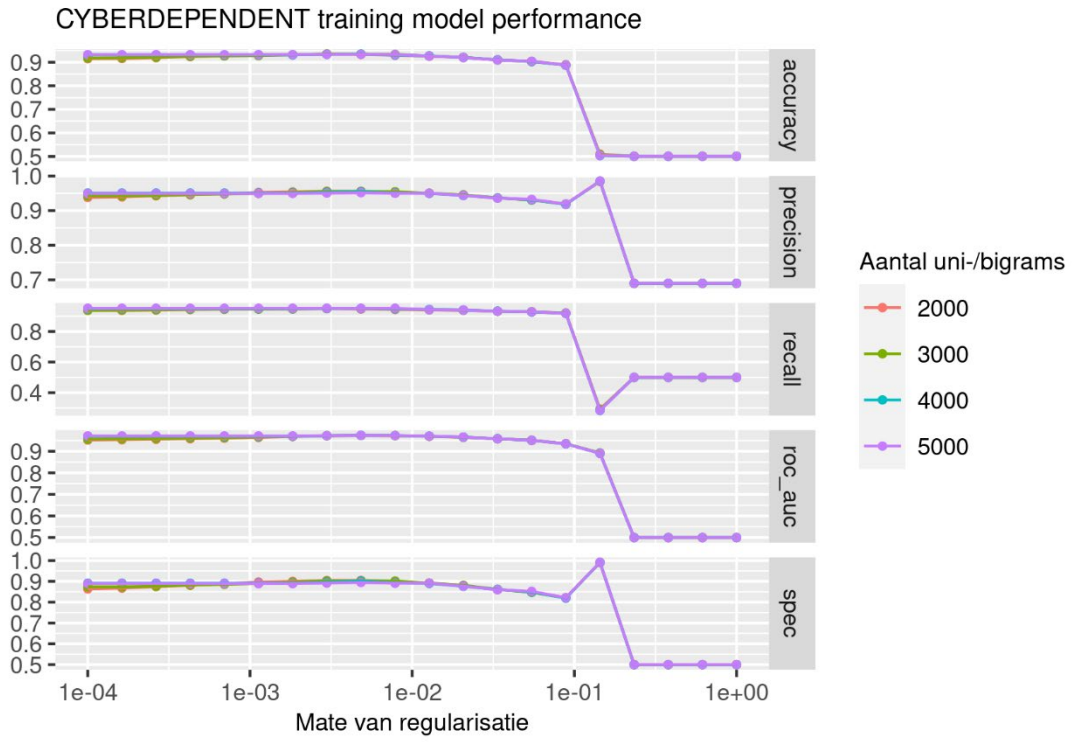
8.6 Overige oplichting

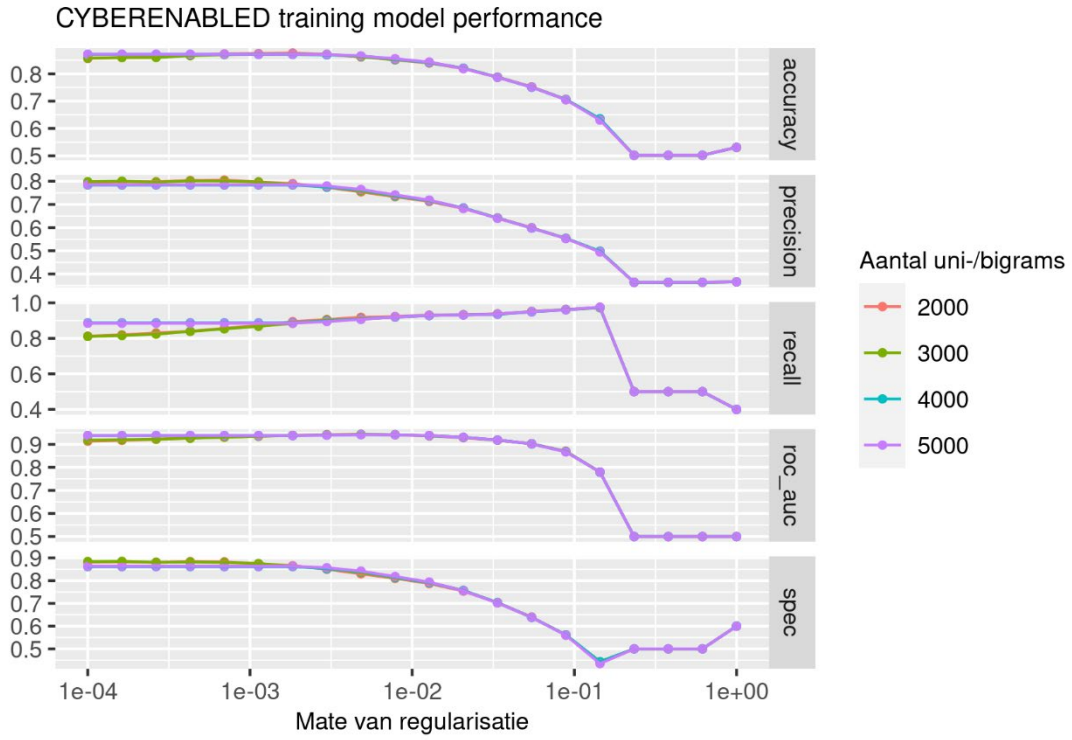
Cohen's kappa = N/A		Tweede annoteur		
		Weet niet	Nee	Ja
Eerste annoteur	Weet niet	0	0	0
	Nee	1	497	2
	Ja	0	0	0

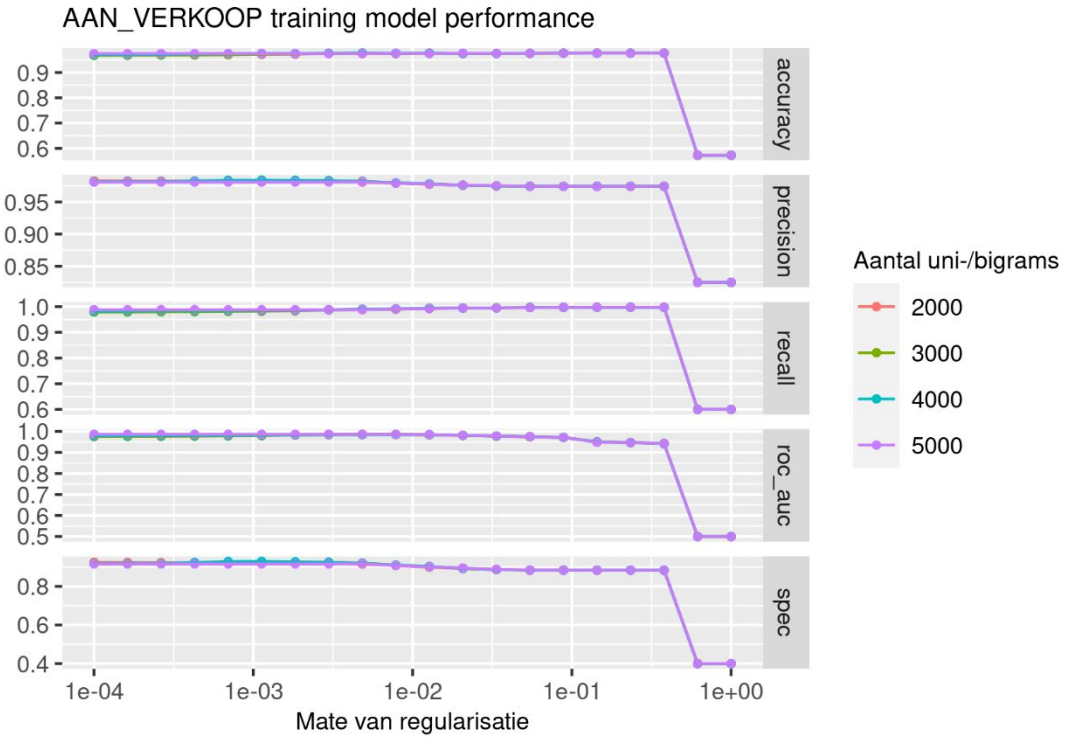
9. Money muling

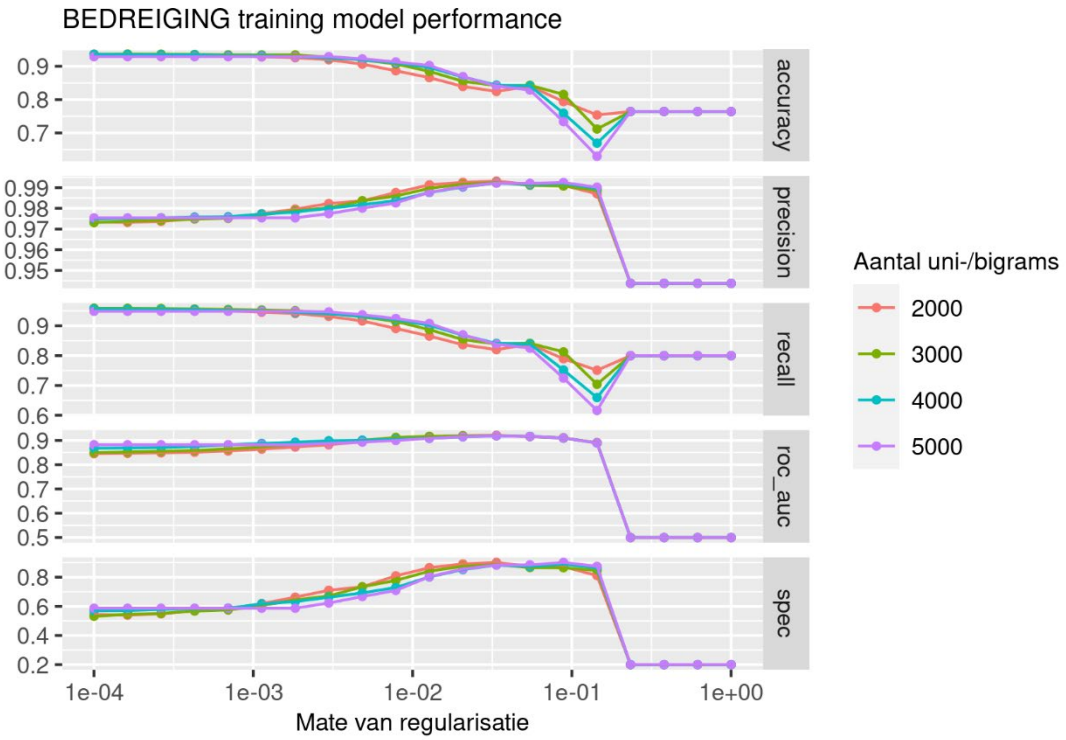
Cohen's kappa = 0.50 (p<.008)		Tweede annoteur		
		Weet niet	Nee	Ja
Eerste annoteur	Weet niet	0	0	0
	Nee	2	492	1
	Ja	0	3	2

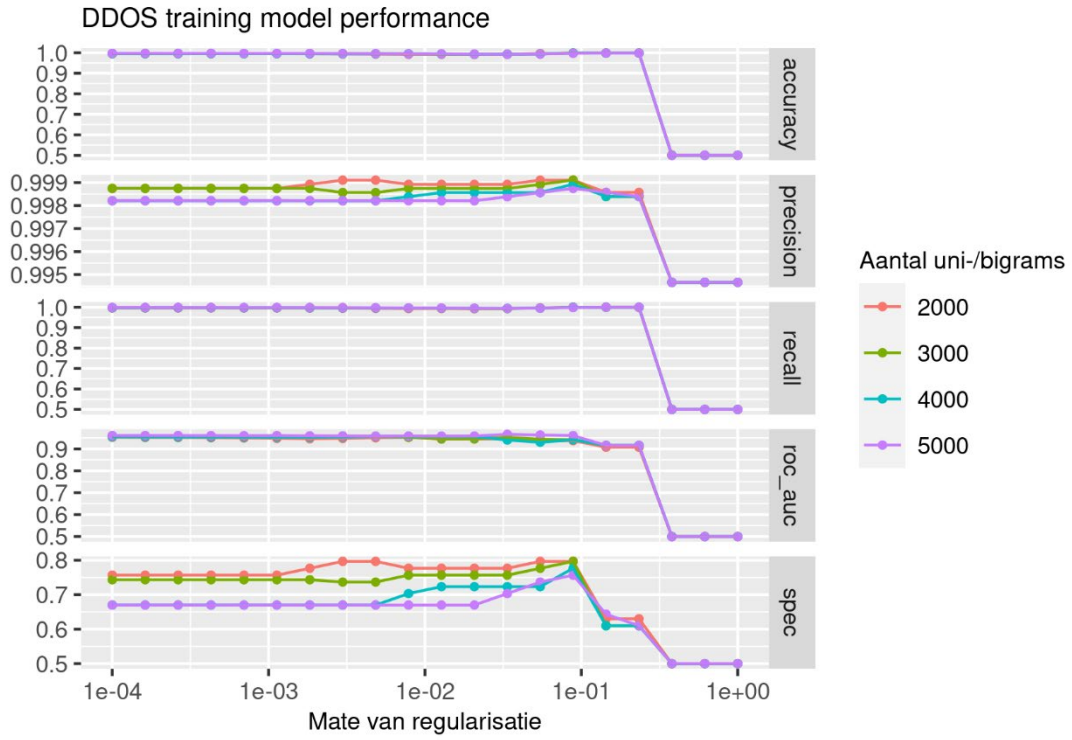
Bijlage 7: Training model performances

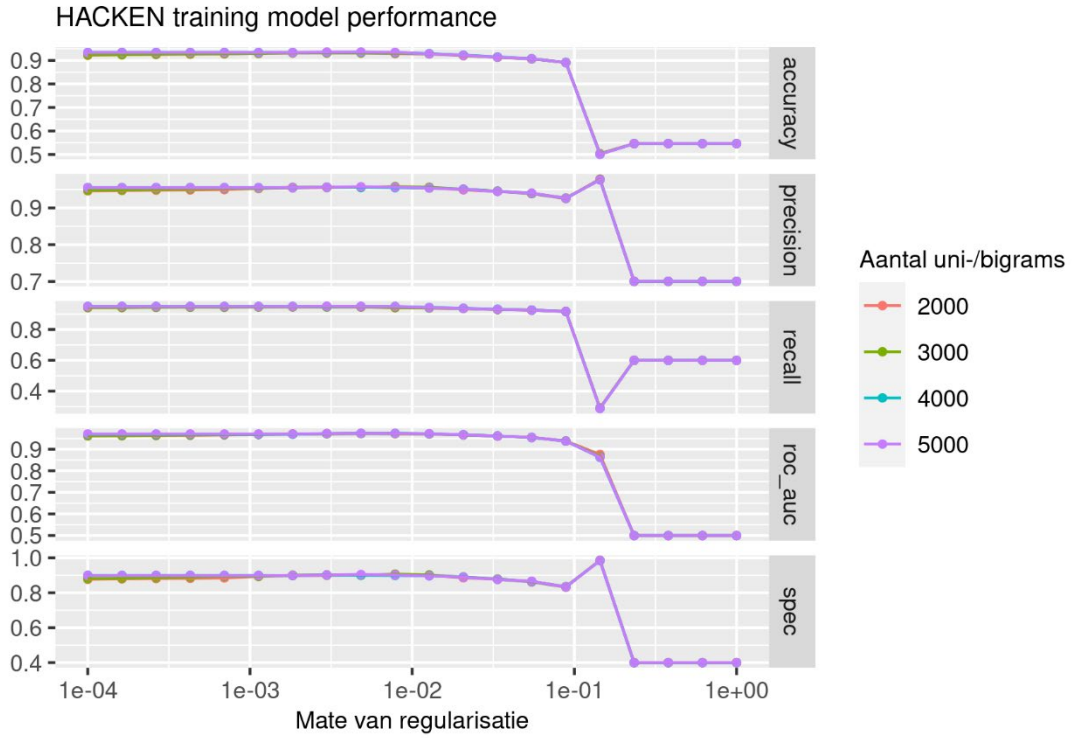


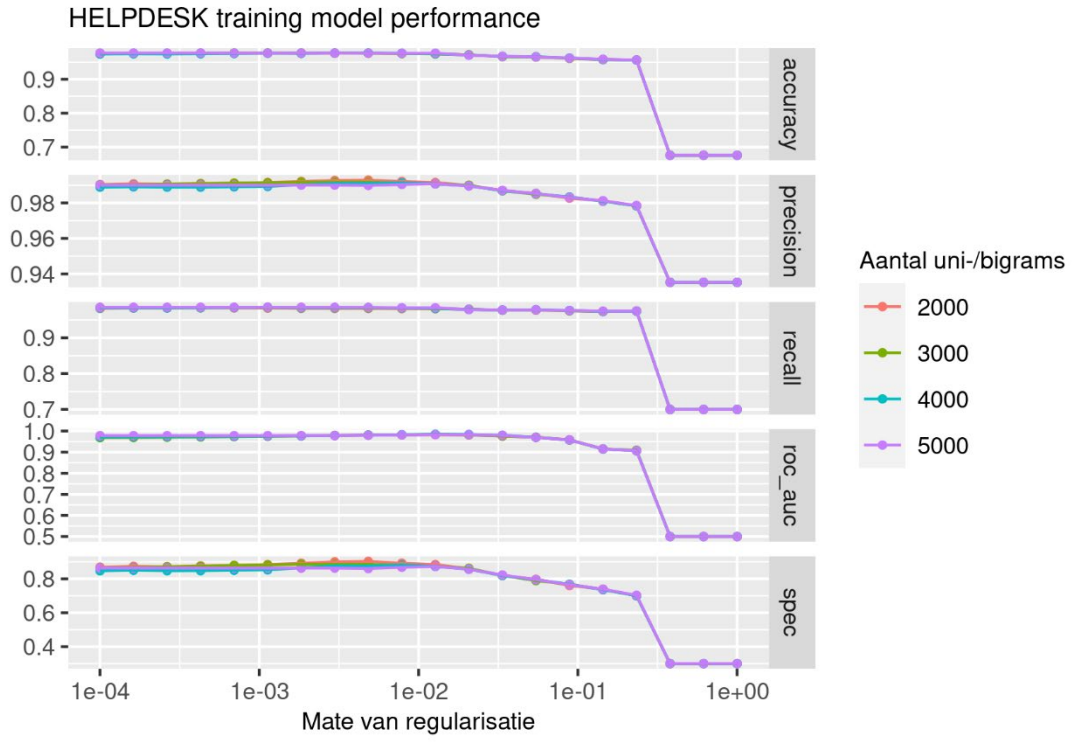


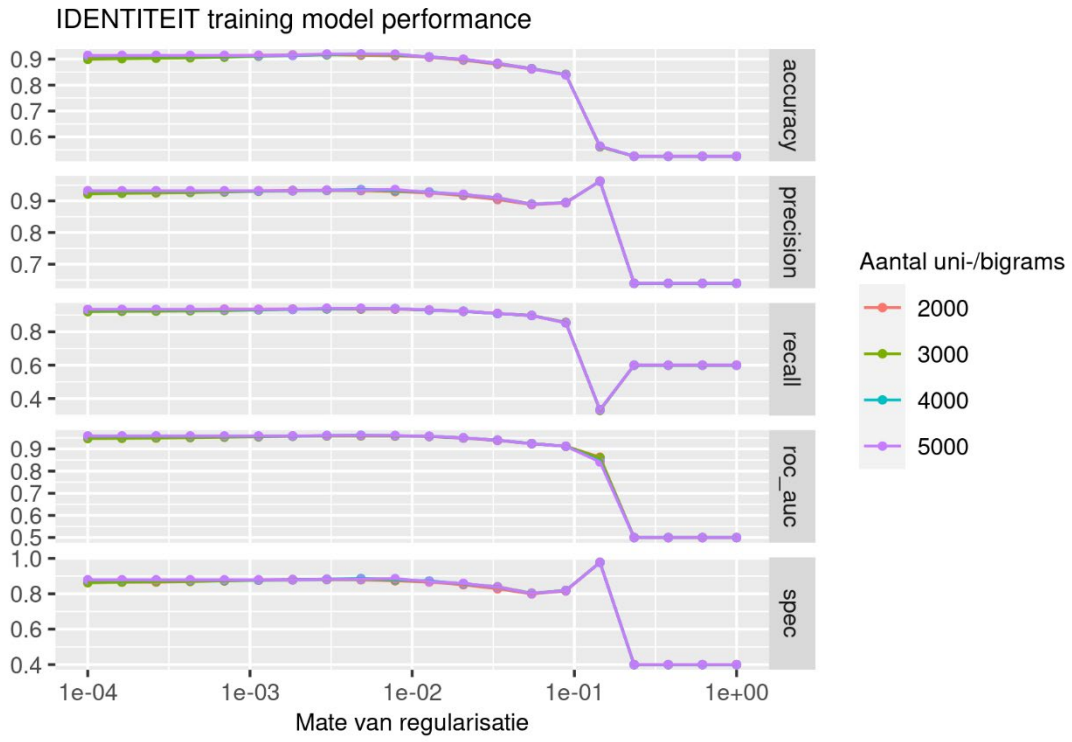

AAN_VERKOOP training model performance
accuracy
precision
recall
roc_auc
spec
1e-04
1e-03
1e-02
1e-01
1e+00
Mate van regularisatie
Aantal uni-/bigrams
2000
3000
4000
5000

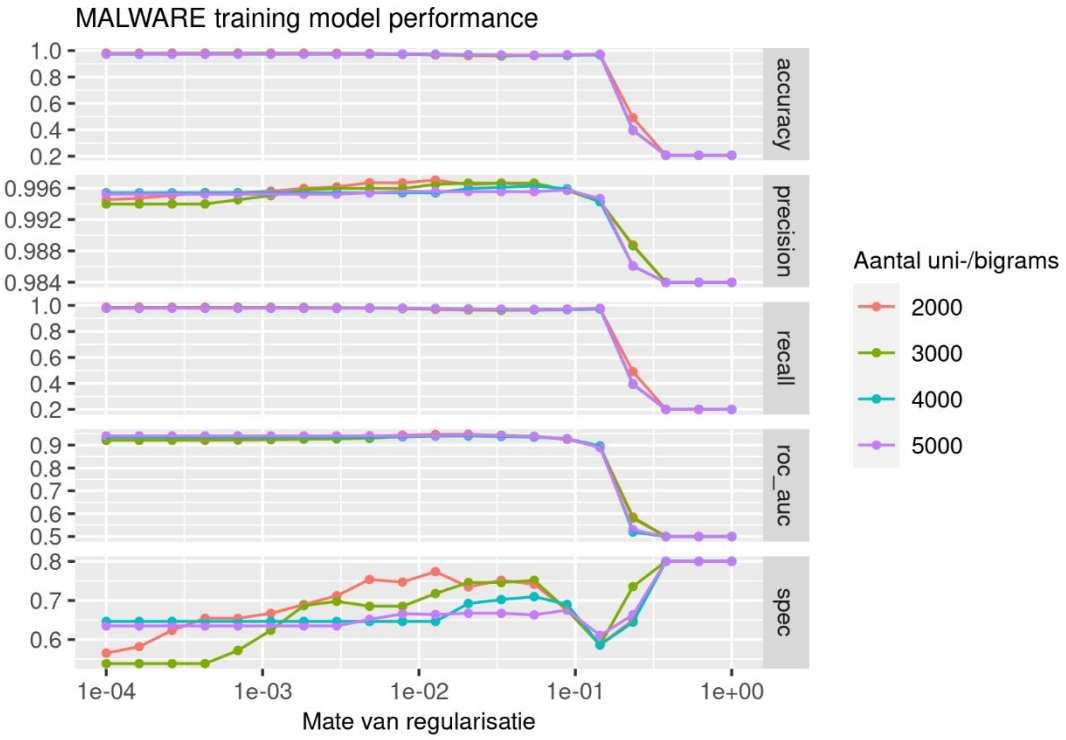

BEDREIGING training model performance
accuracy
precision
recall
roc_auc
spec
1e-04
1e-03
1e-02
1e-01
1e+00
Mate van regularisatie
Aantal uni-/bigrams
2000
3000
4000
5000

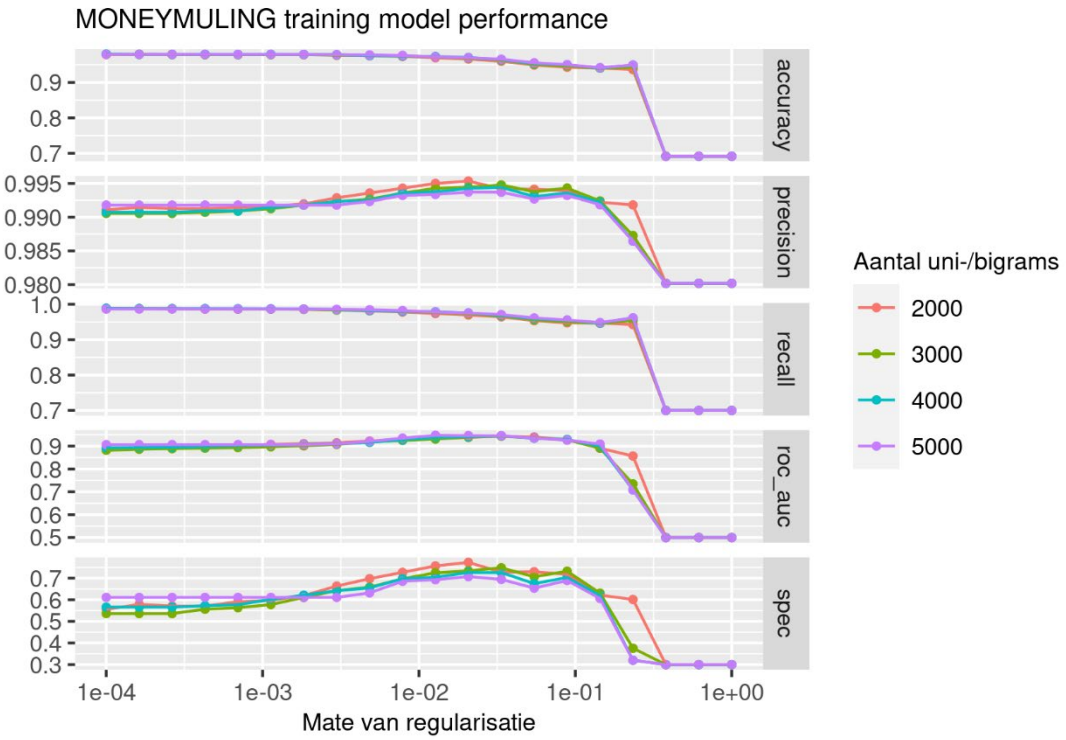

DDOS training model performance
accuracy
precision
recall
roc_auc
spec
1e-04
1e-03
1e-02
1e-01
1e+00
Mate van regularisatie
Aantal uni-/bigrams
2000
3000
4000
5000

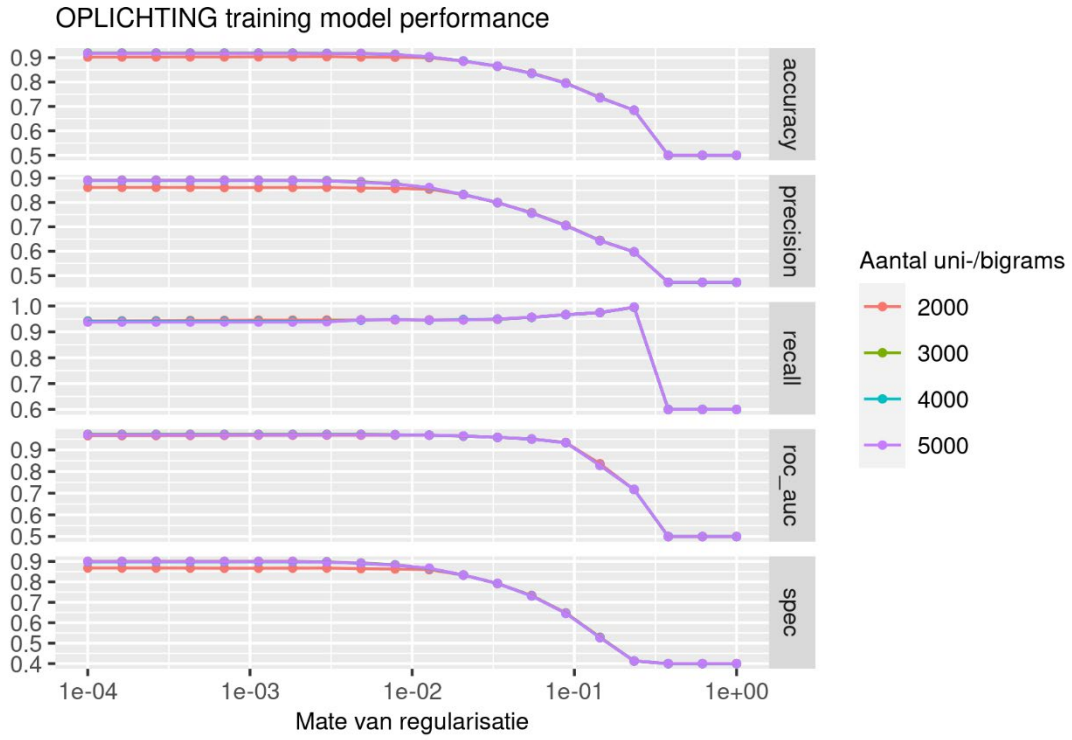

HACKEN training model performance
accuracy
precision
recall
roc_auc
spec
1e-04
1e-03
1e-02
1e-01
1e+00
Mate van regularisatie
Aantal uni-/bigrams
2000
3000
4000
5000

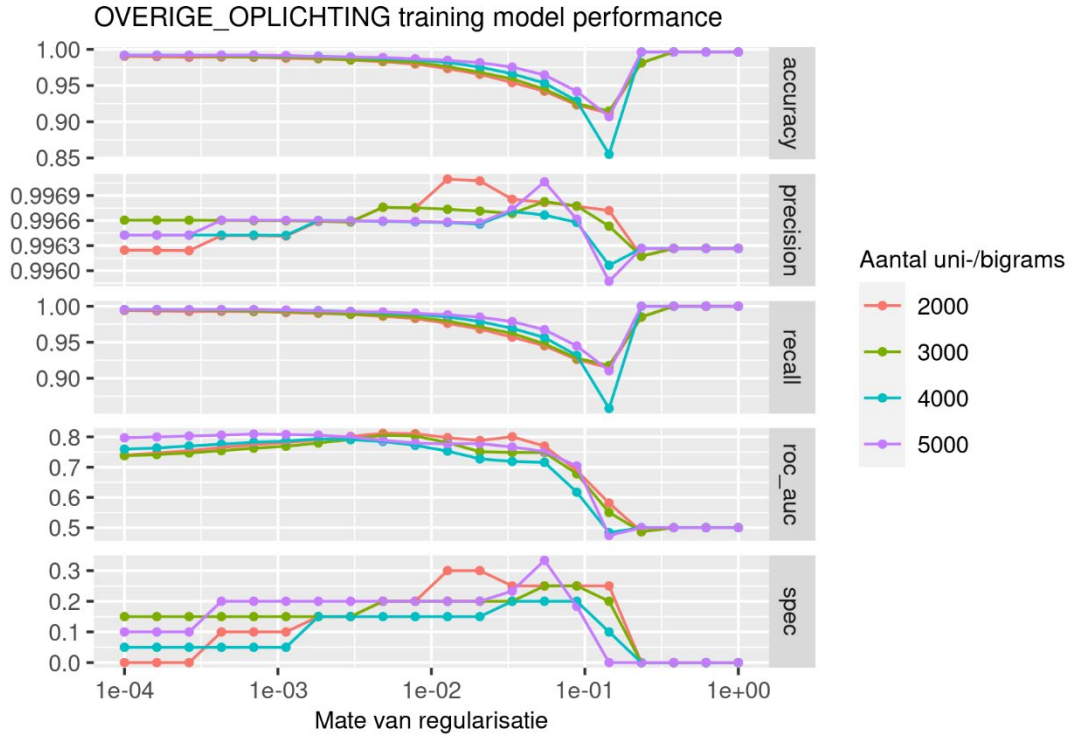

HELPDESK training model performance
accuracy
precision
recall
roc_auc
spec
0.9
0.8
0.7
0.98
0.96
0.94
1.0
0.6
0.5
0.4
1e-04
1e-03
1e-02
1e-01
1e+00
Mate van regularisatie
Aantal uni-/bigrams
2000
3000
4000
5000

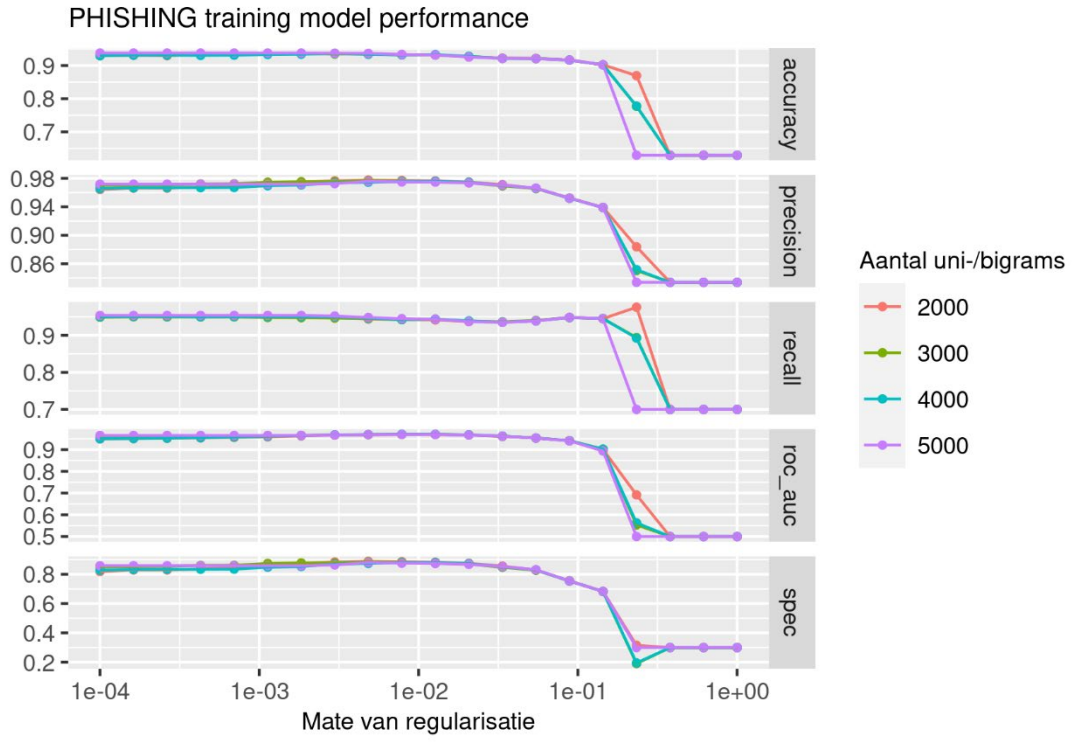

IDENTITEIT training model performance
accuracy
precision
recall
roc_auc
spec
0.9
0.8
0.7
0.6
0.5
0.4
1.0
1e-04
1e-03
1e-02
1e-01
1e+00
Mate van regularisatie
Aantal uni-/bigrams
2000
3000
4000
5000

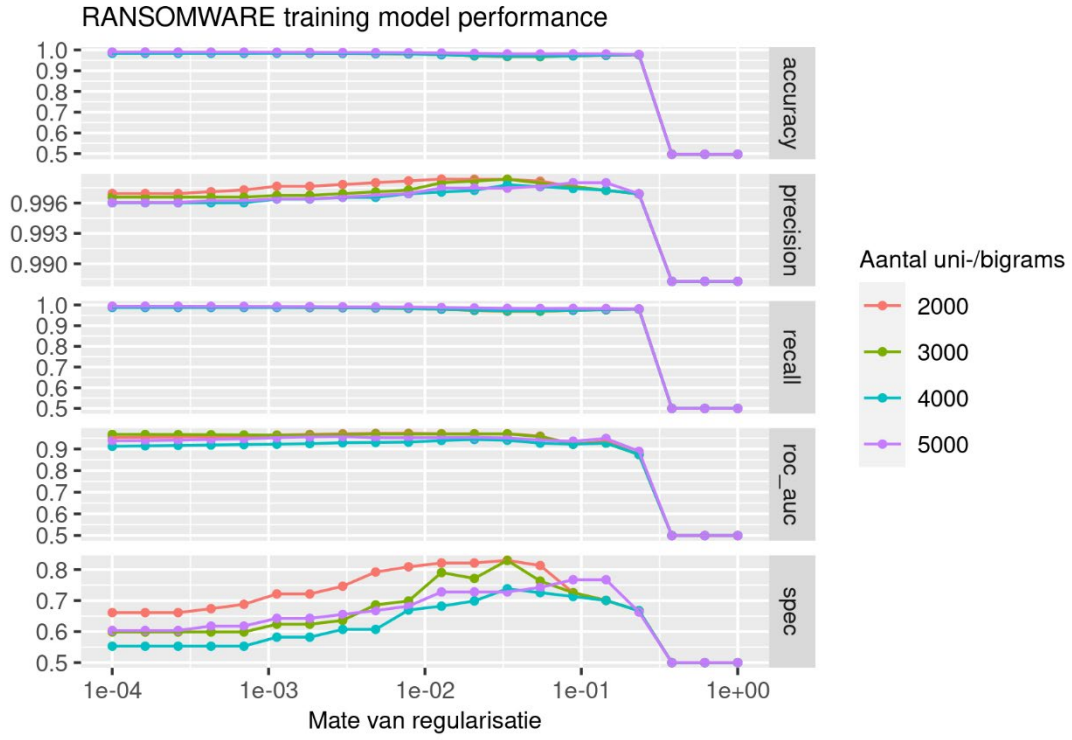

MALWARE training model performance
accuracy
precision
recall
roc_auc
spec
1e-04
1e-03
1e-02
1e-01
1e+00
Mate van regularisatie
Aantal uni-/bigrams
2000
3000
4000
5000

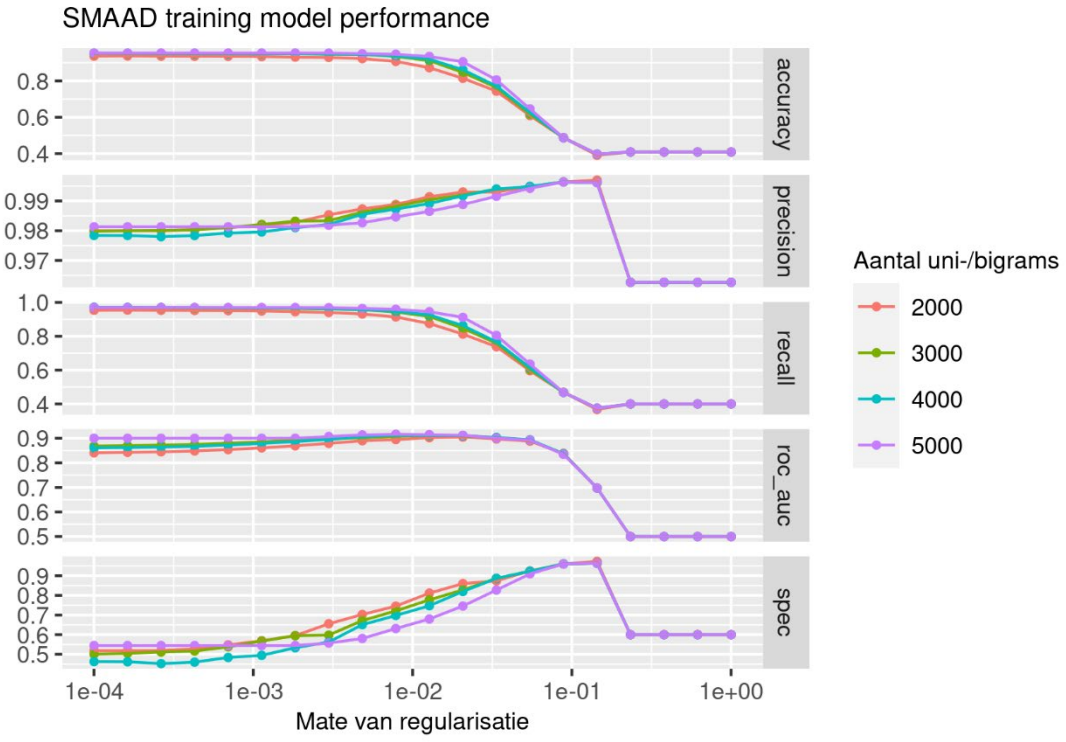

MONEYMULING training model performance
accuracy
precision
recall
roc_auc
spec
1e-04
1e-03
1e-02
1e-01
1e+00
Mate van regularisatie
Aantal uni-/bigrams
2000
3000
4000
5000

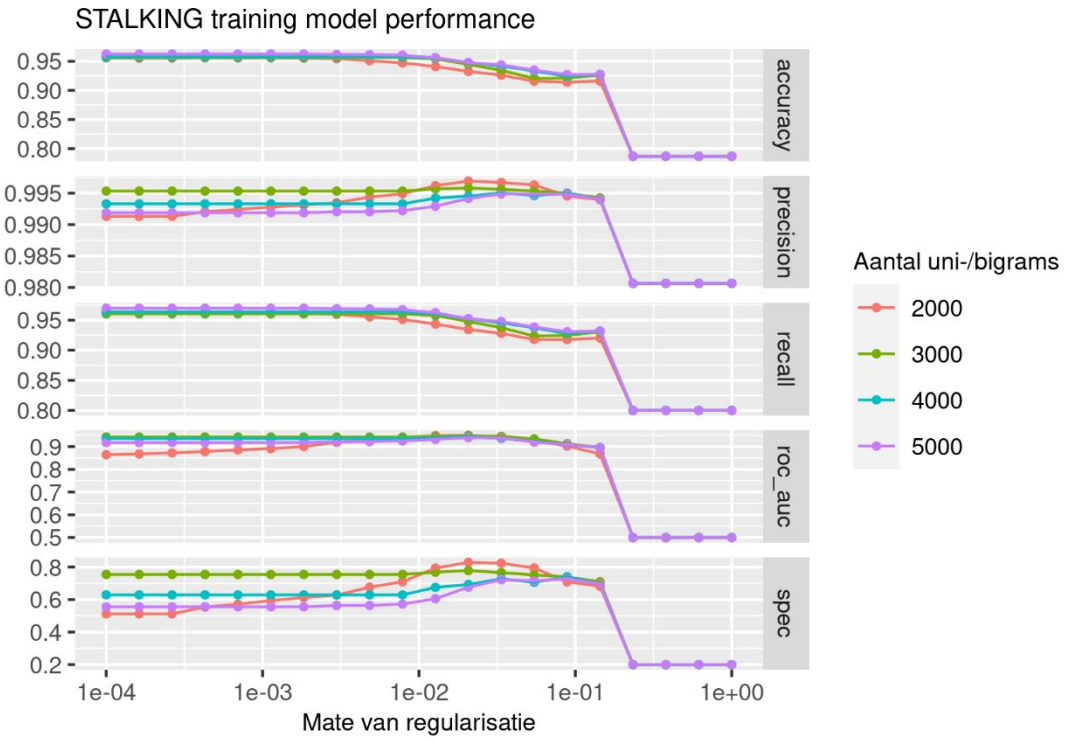

OPLICHTING training model performance
accuracy
precision
recall
roc_auc
spec
1e-04
1e-03
1e-02
1e-01
1e+00
Mate van regularisatie
Aantal uni-/bigrams
2000
3000
4000
5000

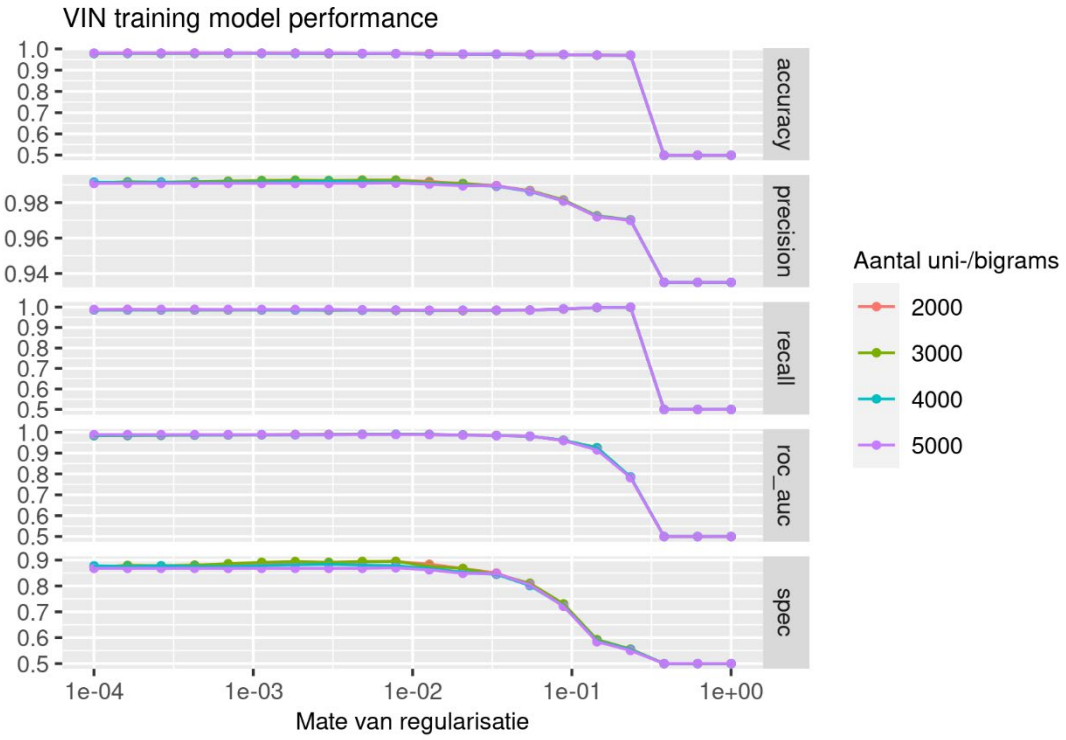

OVERIGE_OPLICHTING training model performance
accuracy
precision
recall
roc_auc
spec
1e-04
1e-03
1e-02
1e-01
1e+00
Mate van regularisatie
Aantal uni-/bigrams
2000
3000
4000
5000


PHISHING training model performance
accuracy
precision
recall
roc_auc
spec
0.9
0.8
0.7
0.98
0.94
0.90
0.86
0.6
0.5
0.4
0.2
1e-04
1e-03
1e-02
1e-01
1e+00
Mate van regularisatie
Aantal uni-/bigrams
2000
3000
4000
5000


RANSOMWARE training model performance
accuracy
precision
recall
roc_auc
spec
1.0
0.9
0.8
0.7
0.6
0.5
0.996
0.993
0.990
1e-04
1e-03
1e-02
1e-01
1e+00
Mate van regularisatie
Aantal uni-/bigrams
2000
3000
4000
5000


SMAAD training model performance
accuracy
precision
recall
roc_auc
spec
0.8
0.6
0.4
0.99
0.98
0.97
1.0
0.8
0.6
0.4
0.9
0.8
0.7
0.6
0.5
0.9
0.8
0.7
0.6
0.5
1e-04
1e-03
1e-02
1e-01
1e+00
Mate van regularisatie
Aantal uni-/bigrams
2000
3000
4000
5000

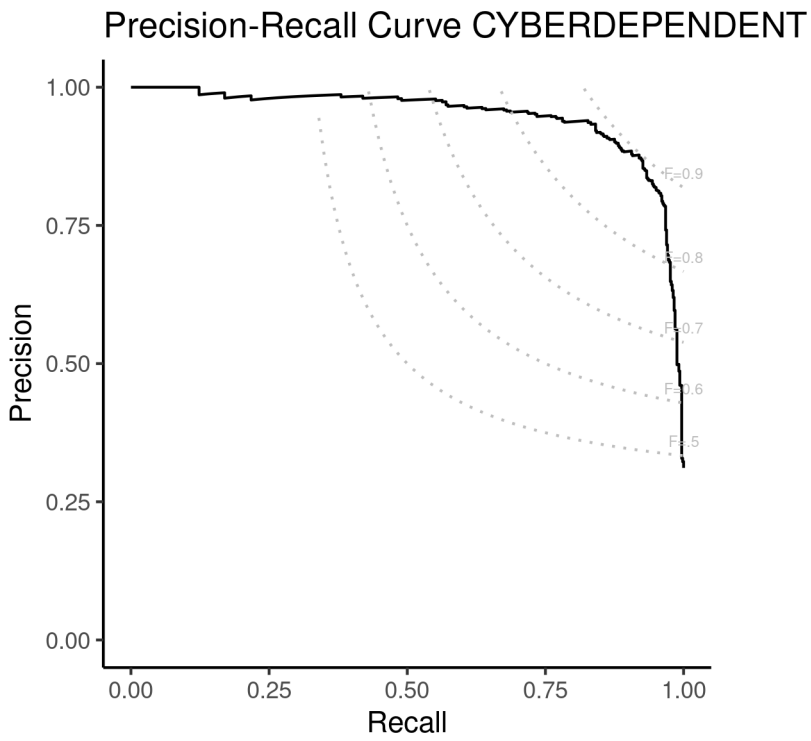

STALKING training model performance
accuracy
precision
recall
roc_auc
spec
0.95
0.90
0.85
0.80
0.995
0.990
0.985
0.980
0.95
0.90
0.85
0.80
0.9
0.8
0.7
0.6
0.5
0.8
0.6
0.4
0.2
1e-04
1e-03
1e-02
1e-01
1e+00
Mate van regularisatie
Aantal uni-/bigrams
2000
3000
4000
5000

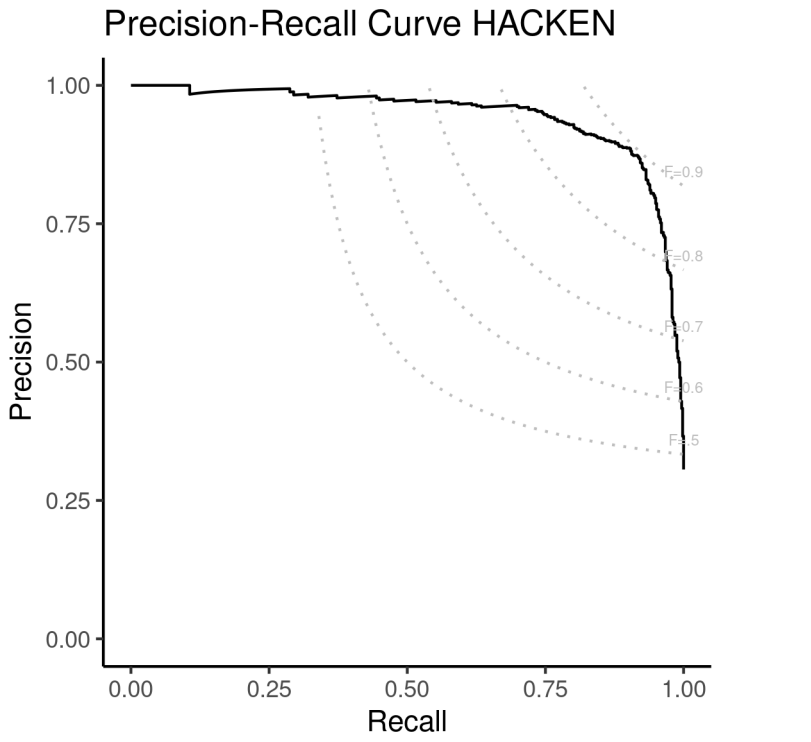

VIN training model performance
accuracy
precision
recall
roc_auc
spec
1.0
0.9
0.8
0.7
0.6
0.5
0.98
0.96
0.94
1e-04
1e-03
1e-02
1e-01
1e+00
Mate van regularisatie
Aantal uni-/bigrams
2000
3000
4000
5000

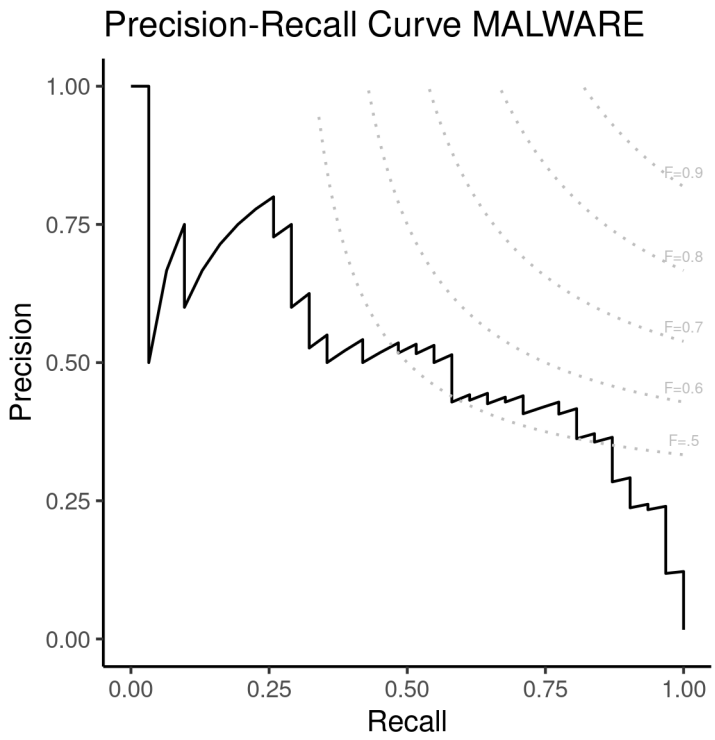
Bijlage 8: Confusion matrices (bij `drempelwaarde` met hoogste F_1-waarde) en *Precision-Recall* grafieken voor test set

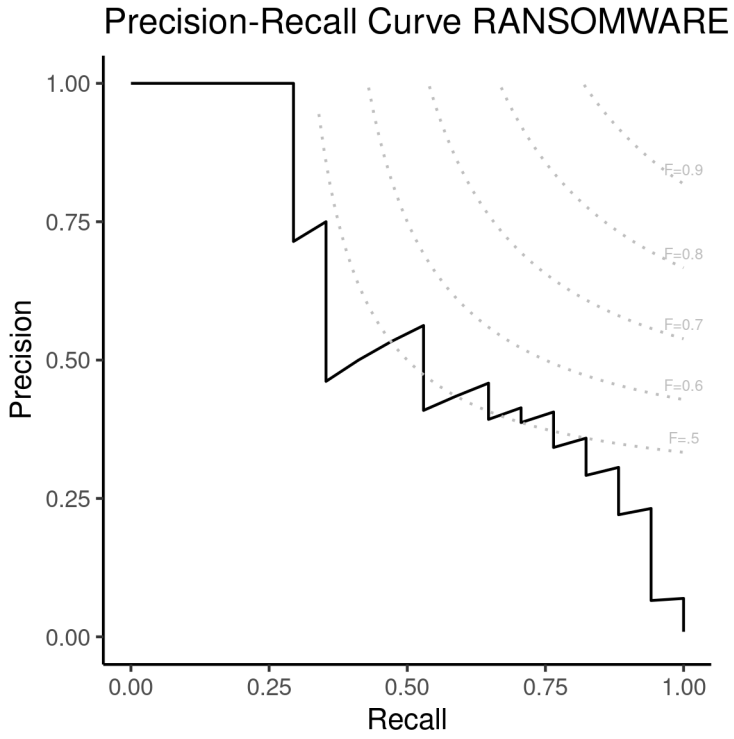
		0	1		
Cybercrime	0	1217	47	*Precision*:	0.88
	1	75	537	*Recall*:	0.92
				F_1-waarde:	0.90
		0	1		
Hacken	0	1235	55	*Precision*:	0.89
	1	67	519	*Recall*:	0.90
				F_1-waarde:	0.89
		0	1		
Malware	0	1812	7	*Precision*:	0.43
	1	32	24	*Recall*:	0.77
				F_1-waarde:	0.55
		0	1		
Ransomware	0	1851	8	*Precision*:	0.56
	1	7	9	*Recall*:	0.53
				F_1-waarde:	0.55
		0	1		
DDoS-aanval	0	1862	2	*Precision*:	0.45
	1	6	5	*Recall*:	0.71
				F_1-waarde:	0.56
		0	1		
Gedigitaliseerde criminaliteit	0	585	122	*Precision*:	0.92
	1	94	1075	*Recall*:	0.90
				F_1-waarde:	0.91
		0	1		
Online bedreiging	0	1650	28	*Precision*:	0.37
	1	124	73	*Recall*:	0.72
				F_1-waarde:	0.49
		0	1		
Online stalking	0	1820	13	*Precision*:	0.50
	1	21	21	*Recall*:	0.62
				F_1-waarde:	0.55
		0	1		
Online smaad/laster/belediging	0	1741	22	*Precision*:	0.46
	1	60	52	*Recall*:	0.70
				F_1-waarde:	0.56
		0	1		
Online oplichting	0	787	54	*Precision*:	0.91
	1	88	946	*Recall*:	0.95
				F_1-waarde:	0.93
		0	1		
Phishing	0	1504	37	*Precision*:	0.80
	1	68	267	*Recall*:	0.88
				F_1-waarde:	0.84
		0	1		
Online identiteitsfraude	0	1125	60	*Precision*:	0.89
	1	79	612	*Recall*:	0.91
				F_1-waarde:	0.90
		0	1		
Online aan- en verkoopfraude	0	1518	44	*Precision*:	0.95
	1	15	299	*Recall*:	0.87
				F_1-waarde:	0.91
		0	1		
VIN-fraude	0	1736	12	*Precision*:	0.89
	1	14	113	*Recall*:	0.90
				F_1-waarde:	0.90

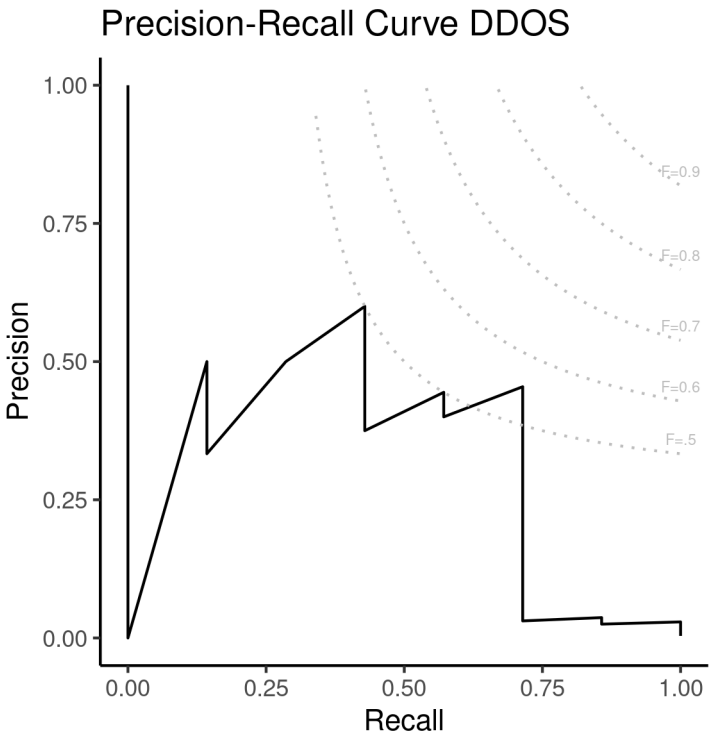
		0	1	*Precision*:	0.89
Helpdesk-fraude	0	1731	24	*Recall*:	0.82
	1	13	107	F_1-waarde:	0.85
		0	1	*Precision*:	0.06
Overige online oplichting	0	1835	9	*Recall*:	0.18
	1	29	2	F_1-waarde:	0.10
		0	1	*Precision*:	0.55
Money muling	0	1836	17	*Recall*:	0.41
	1	10	12	F_1-waarde:	0.47

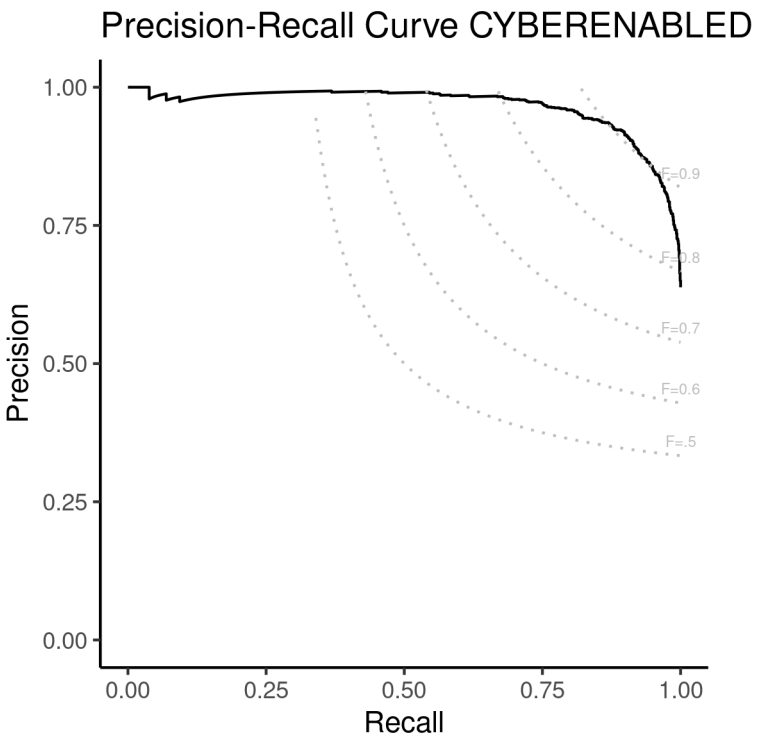

Precision-Recall Curve CYBERDEPENDENT
Precision
Recall
1.00
0.75
0.50
0.25
0.00
0.00
0.25
0.50
0.75
1.00
F1=0.9
F1=0.8
F1=0.7
F1=0.6
F1=0.5

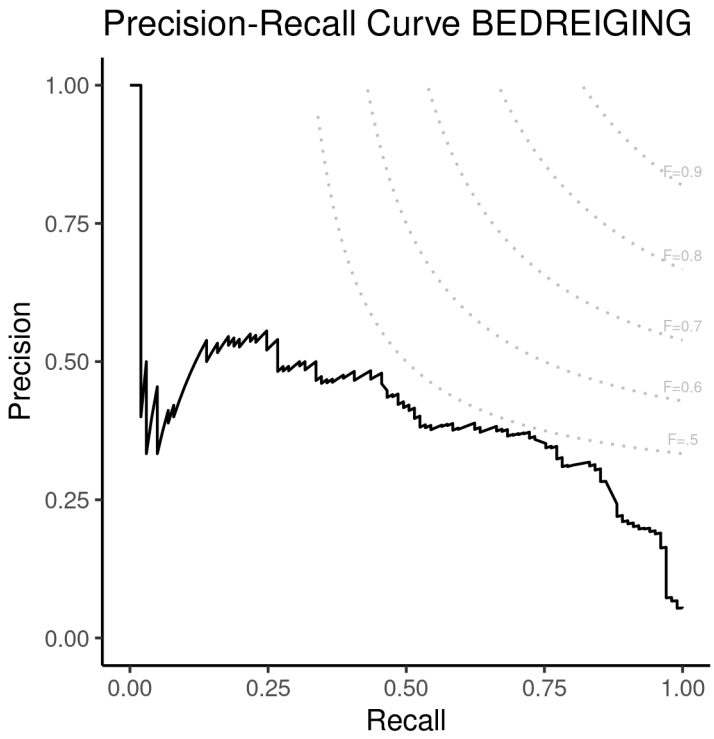

Precision-Recall Curve HACKEN
Precision
Recall
1.00
0.75
0.50
0.25
0.00
0.00
0.25
0.50
0.75
1.00
F1=0.9
F1=0.8
F1=0.7
F1=0.6
F1=0.5

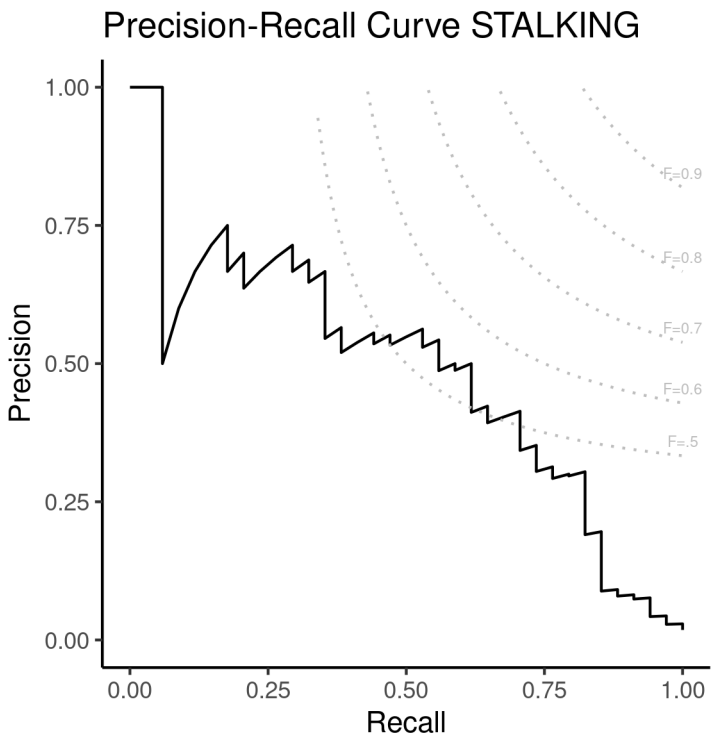

Precision-Recall Curve MALWARE
Precision
Recall
1.00
0.75
0.50
0.25
0.00
0.00
0.25
0.50
0.75
1.00
F=0.9
F=0.8
F=0.7
F=0.6
F=.5

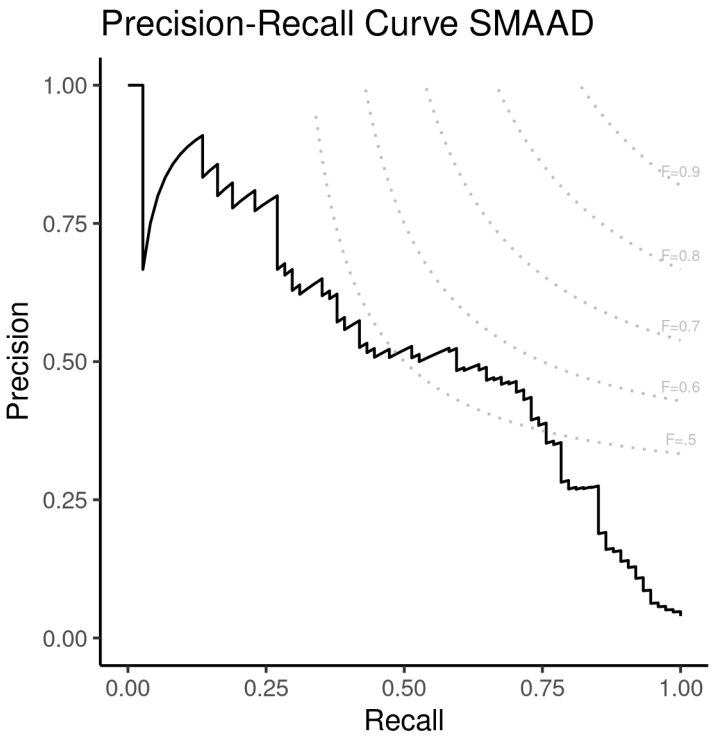

Precision-Recall Curve RANSOMWARE
Precision
Recall
1.00
0.75
0.50
0.25
0.00
0.00
0.25
0.50
0.75
1.00
F=0.9
F=0.8
F=0.7
F=0.6
F=.5

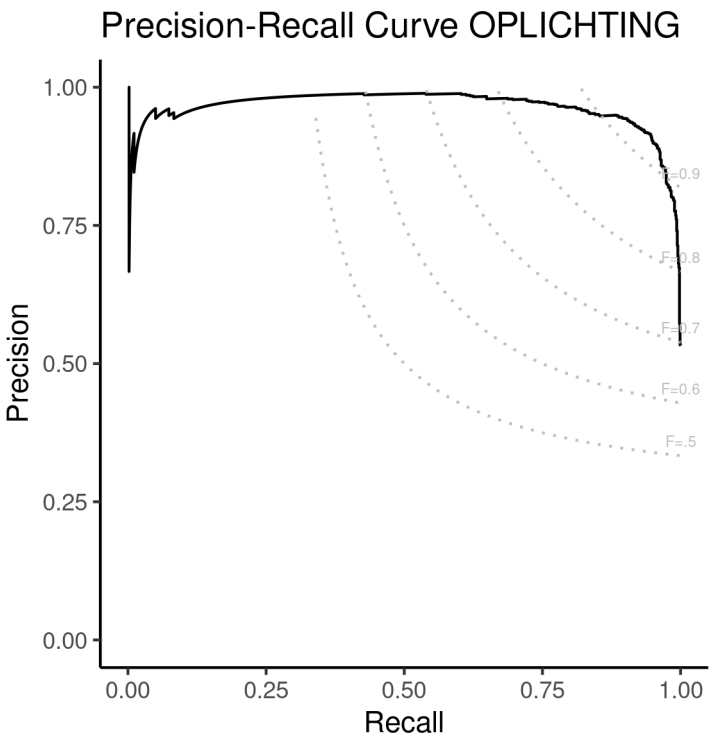

Precision-Recall Curve DDOS
Precision
Recall
1.00
0.75
0.50
0.25
0.00
0.00
0.25
0.50
0.75
1.00
F=0.9
F=0.8
F=0.7
F=0.6
F=.5

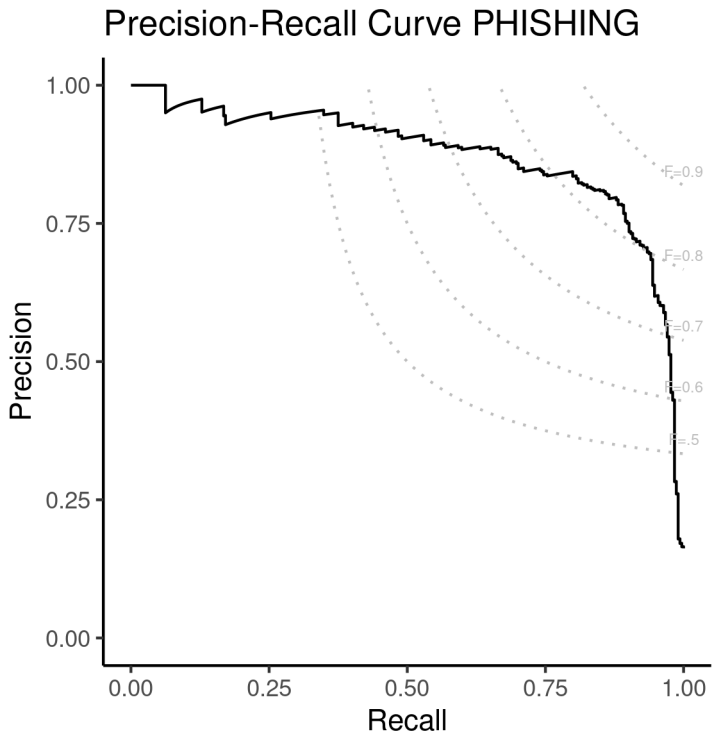

Precision-Recall Curve CYBERENABLED
Precision
Recall
1.00
0.75
0.50
0.25
0.00
0.00
0.25
0.50
0.75
1.00
F=0.9
F=0.8
F=0.7
F=0.6
F=.5

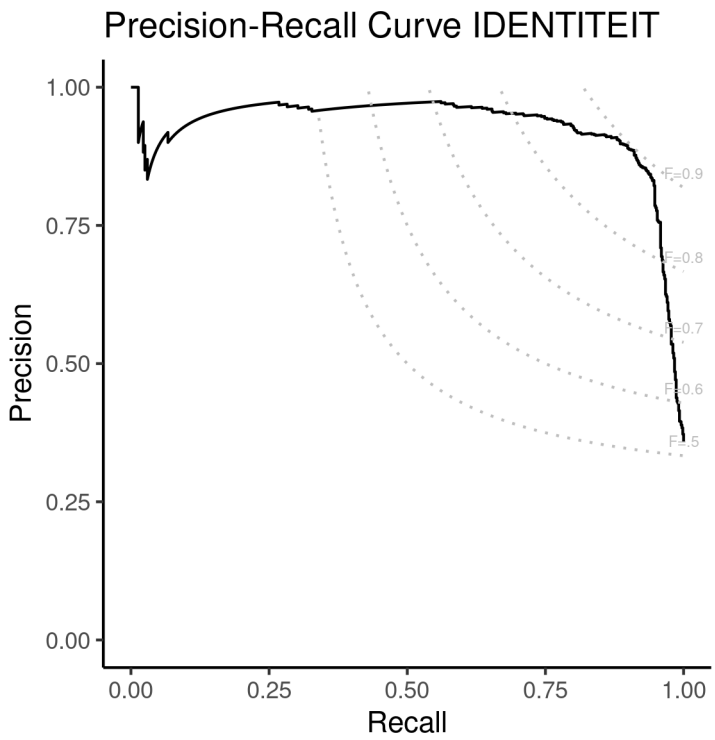

Precision-Recall Curve BEDREIGING
Precision
Recall
1.00
0.75
0.50
0.25
0.00
0.00
0.25
0.50
0.75
1.00
F=0.9
F=0.8
F=0.7
F=0.6
F=.5

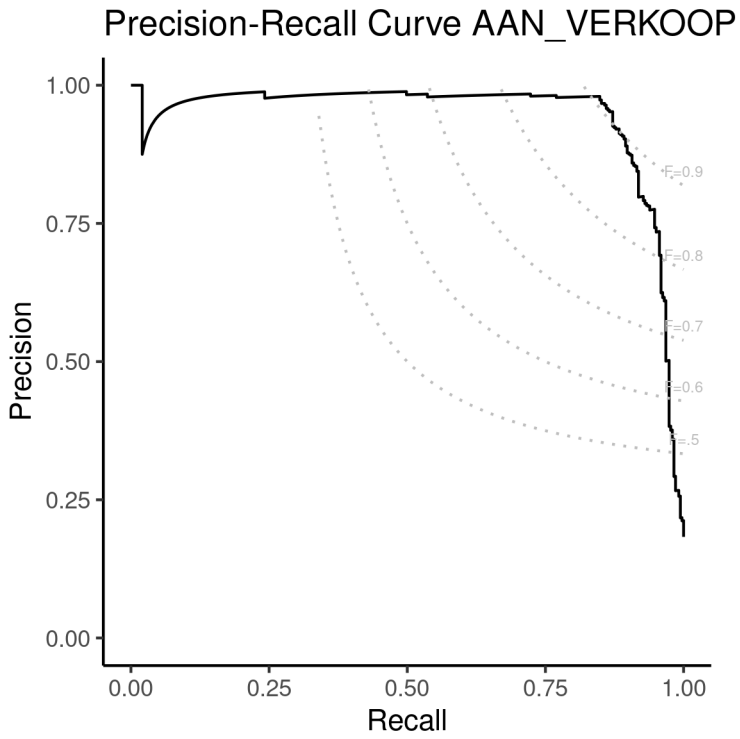

Precision-Recall Curve STALKING
Precision
Recall
1.00
0.75
0.50
0.25
0.00
0.00
0.25
0.50
0.75
1.00
F=0.9
F=0.8
F=0.7
F=0.6
F=.5

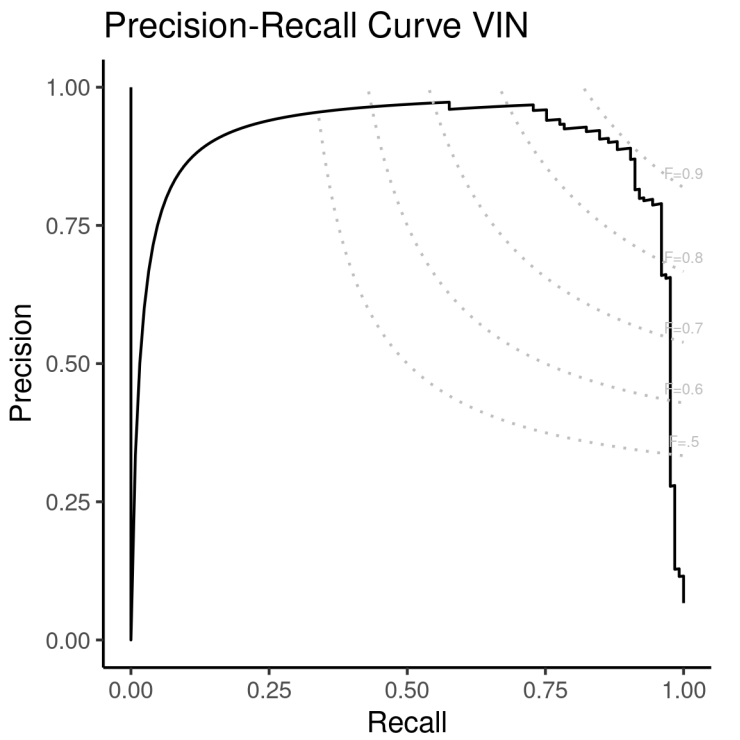

Precision-Recall Curve SMAAD
Precision
Recall
1.00
0.75
0.50
0.25
0.00
0.00
0.25
0.50
0.75
1.00
F=0.9
F=0.8
F=0.7
F=0.6
F=.5

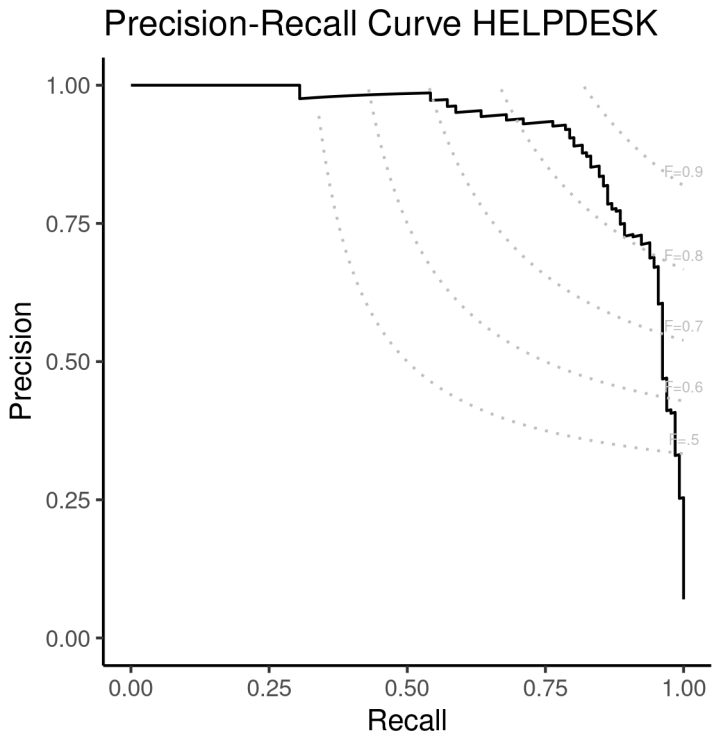

Precision-Recall Curve OPLICHTING
Precision
Recall
1.00
0.75
0.50
0.25
0.00
0.00
0.25
0.50
0.75
1.00
F=0.9
F=0.8
F=0.7
F=0.6
F=.5

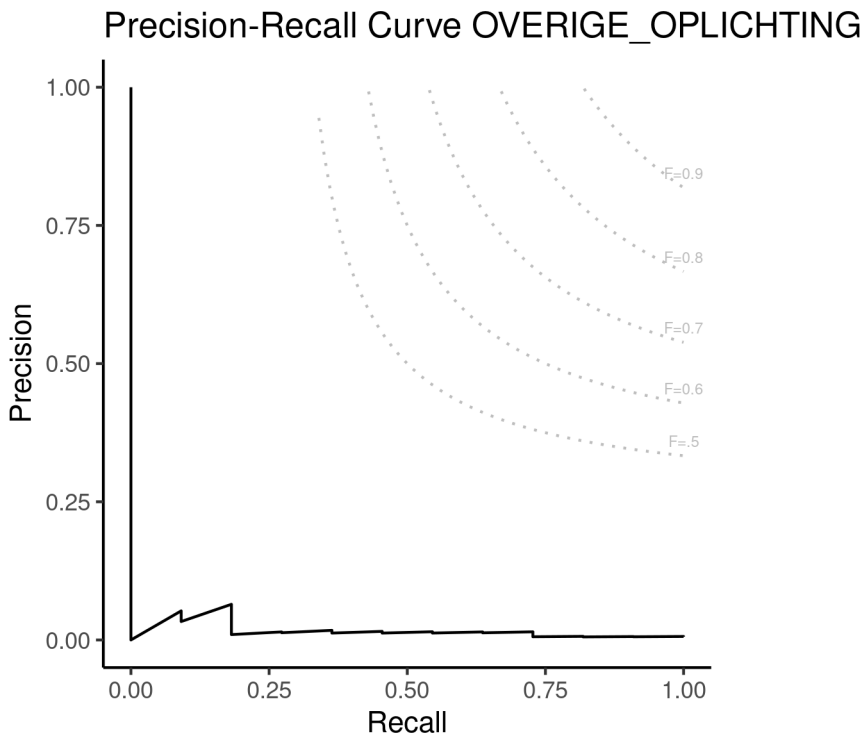

Precision-Recall Curve PHISHING
Precision
Recall
1.00
0.75
0.50
0.25
0.00
0.00
0.25
0.50
0.75
1.00
F=0.9
F=0.8
F=0.7
F=0.6
F=.5

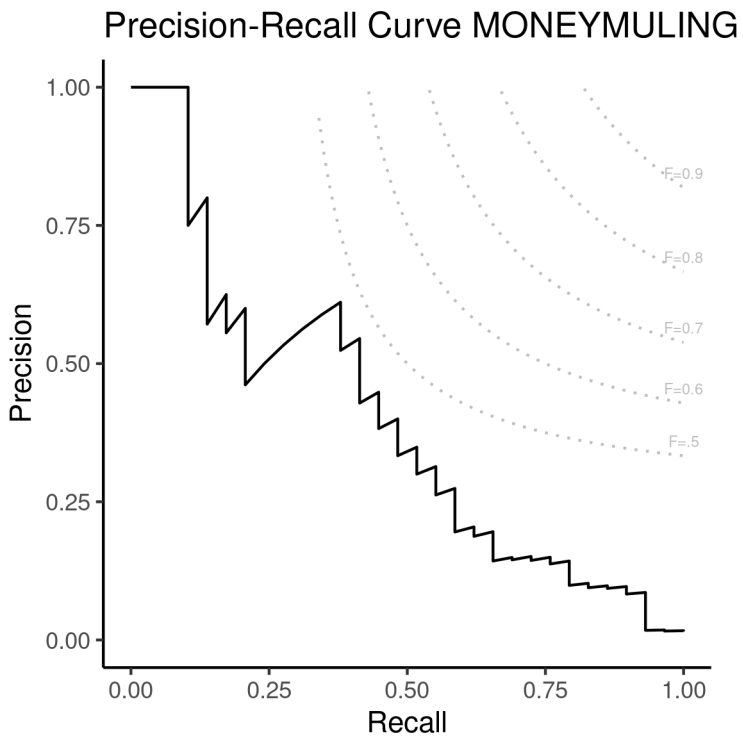

Precision-Recall Curve IDENTITEIT
Precision
Recall
1.00
0.75
0.50
0.25
0.00
0.00
0.25
0.50
0.75
1.00
F=0.9
F=0.8
F=0.7
F=0.6
F=.5


Precision-Recall Curve AAN_VERKOOP
Precision
Recall
1.00
0.75
0.50
0.25
0.00
0.00
0.25
0.50
0.75
1.00
F1=0.9
F1=0.8
F1=0.7
F1=0.6
F1=.5


Precision-Recall Curve VIN
Precision
Recall
1.00
0.75
0.50
0.25
0.00
0.00
0.25
0.50
0.75
1.00
F1=0.9
F1=0.8
F1=0.7
F1=0.6
F1=.5


Precision-Recall Curve HELPDESK
Precision
Recall
1.00
0.75
0.50
0.25
0.00
0.00
0.25
0.50
0.75
1.00
F=0.9
F=0.8
F=0.7
F=0.6
F=.5


Precision-Recall Curve OVERIGE_OPLICHTING
Precision
Recall
1.00
0.75
0.50
0.25
0.00
0.00
0.25
0.50
0.75
1.00
F=0.9
F=0.8
F=0.7
F=0.6
F=.5


Precision-Recall Curve MONEYMULING
Precision
Recall
1.00
0.75
0.50
0.25
0.00
0.00
0.25
0.50
0.75
1.00
F=0.9
F=0.8
F=0.7
F=0.6
F=.5

Bijlage 9: Meest predictieve uni-/bigrams cybercrime en gedigitaliseerde criminaliteit

CYBERCRIME	GEDIGITALISEERDE CRIMINALITEIT
hacken	internetvia
f90	euro maken
terugstorten	schadeloos stellen
aangifte cybercrime	neehebben
computervredebreuk	betaling aangifte
janamelijk	betalingsmethoÃ«n
engelsspreken man	nieuw nummer
overnameprogramma	neebetaling
afgeschreven	engel spreken
verificatie	bank rekening
hacking	onbekend persoon
af schrijven	phishing
aangifte computervredebreuk	mail staan
ingelgen	profielfoto gebruiken
link	bericht staan
phishing	uiten
hack	aangifte oplichting
cybercrime	klikken
klikken	hierbij aangifte
email zien	geld maken

AAN_VERKOOP	HACKEN	HELPDESK	IDENTITEIT
goed overgaan	hacken	microsoffen	neebetaling
bestellen betalen	f90	spreken man	internetvia formulier
betalen bedrag	terugstorten	vinden telefoonnummer	identiteitsfraude
kopen via	computervredebreuk	bellen telefoonnummer	f90
nagenoeg	engelsspreken man	moeten geld	afgifte overgaan
verdenken oplichting	janamelijk	moeten inloggen	email zien
aangifte oplichting	aangifte cybercrime	accent	whl
denken gaan	overnameprogramma	bank bellen	willen overmaken
reageren bericht	afgeschreven	vader willen	phishing
toegezonden	aangifte computervredebreuk	microsoft	nieuw nummer
tevens geven	verificatie	bellen telefoonnr	afgeschreven
nooit ontvangen	link	voordijden	bank bellen
volgen rekeningnummer	phishing	engel spreken	overnameprogramma downloaen
lmio	oplichting vinden	opnemen aangifte	neehebben
investeren	vinden telefoonnummer	aanvullen informatie	aangifte cybercrime
duperen	cybercrime	helpdesk	klikken
opsturen	klikken	uur bellen	aangifte identiteitsfraude
email mail	hack	gemaild	link
terugkrijgen	account blokkeren	bellen ing	whatsapp fraude
zien advertentie	inloggen	verbinding verbreken	microsoffen

- Bijlage 9 -

OPLICHTING	PHISHING	VIN
internetvia	f90	formulier whatsapp
identiteitsfraude	phishing	nieuw nummer
aangifte oplichting	phising	whatsapp fraude
microsoffen	bank bellen	betreffen melding
phishing	microsoffen	geld maken
link	bankrekening blokkeren	rekening betalen
hierbij aangifte	moeten inloggen	oud nummer
klikken	aangifte cybercrime	euro willen
afgeschreven	verificatie	poging oplichting
neebetaling	link	bericht afkomstig
geld maken	afgeschreven	nieuw telefoonnummer
aangifte cybercrime	klikken	eenheid oost
annuleren	rekening halen	geld storten
aangifte identiteitsfraude	formulier helpdeskfraude	ander telefoonnummer
bank bellen	invoeren	nieuw telefoon
schadeloos	betaallink	contact oplichter
neehebben	plaatsen marktplaats	whatsapp
euro maken	koop staan	benaderen
niemand toestemming	welk programma	moeten overmaken
nieuw nummer	euro rekening	profielfoto

Bijlage 10: In- en doorstroom afzonderlijke vormen van online criminaliteit

Tabel 22 BVH-registraties online criminaliteit zonder en met aangifte

	Zonder aangifte		Met tenminste 1 aangifte		Totaal	
Hacking	471	20%	1.838	80%	2.309	100%
Online oplichting	1.194	12%	8.368	88%	9.562	100%
Phishing	83	7%	1.106	93%	1.189	100%
Online identiteitsfraude	900	17%	4.393	83%	5.293	100%
Aan- en verkoopfraude	470	10%	4.098	90%	4.568	100%
VIN-fraude	93	10%	862	90%	955	100%
Helpdeskfraude	42	12%	319	88%	361	100%

Tabel 23 Doorstroom afzonderlijke vormen online criminaliteit - meerderjarige verdachten

		Hacking		Oplichting		Phishing		Identiteitsfraude	
Politie	Overig / onbekend	57	35%	194	35%	39	35%	166	34%
	Politiestrafbeschikking / Halt / reprimande	4	2%	5	1%	0	0%	4	1%
OM	Overig / onbekend	19	12%	83	15%	12	11%	66	14%
	Sepot	37	23%	101	18%	24	21%	84	17%
	Strafbeschikking / transactie	8	5%	27	5%	8	7%	24	5%
Rechtspraak	Dagvaarden	39	24%	144	26%	29	26%	141	29%
	Totaal	164	100%	554	100%	112	100%	485	100%

		Aan- en verkoopfraude		VIN-fraude		Helpdeskfraude	
Politie	Overig / onbekend	9	13%	60	56%	15	23%
	Politiestrafbeschikking / Halt / reprimande	4	6%	1	1%	0	0%
OM	Overig / onbekend	22	31%	9	8%	5	8%
	Sepot	15	21%	11	10%	16	25%
	Strafbeschikking / transactie	4	6%	6	6%	4	6%
Rechtspraak	Dagvaarden	17	24%	21	19%	24	38%
	Totaal	71	100%	108	100%	64	100%

Tabel 24 Doorstroom afzonderlijke vormen online criminaliteit - minderjarige verdachten

		Hacking		Oplichting		Phishing		Identiteitsfraude	
Politie	Overig / onbekend	5	21%	7	13%	1	7%	5	12%
	Politiestrafbeschikking / Halt / reprimande	0	0%	4	7%	0	0%	3	7%
OM	Overig / onbekend	7	29%	15	28%	3	21%	13	31%
	Sepot	3	12%	11	20%	3	21%	8	19%
	Strafbeschikking / transactie	0	0%	1	2%	0	0%	0	0%
Rechtspraak	Dagvaarden	9	38%	16	30%	7	50%	13	31%
	Totaal	24	100%	54	100%	14	100%	42	100%

		Aan- en verkoopfraude		VIN-fraude		Helpdeskfraude	
Politie	Overig / onbekend	2	20%	1	11%	0	0%
	Politiestrafbeschikking / Halt / reprimande	0	0	0	0%	1	6%
OM	Overig / onbekend	1	10%	1	11%	2	12%
	Sepot	4	40%	3	33%	4	24%
	Strafbeschikking / transactie	1	10%	0	0%	2	12%
Rechtspraak	Dagvaarden	2	20%	4	44%	8	47%
	Totaal	10	100%	9	100%	17	100%

Bijlage 11: Operationalisering drie andere typen delict voor vergelijking met online criminaliteit

Type delict	Onderliggende misdrijven	Operationalisering
Vermogenscriminaliteit	Diefstal/inbraak woning Diefstal inbraak box/garage/schuur/tuinhuis Diefstal uit/vanaf motorvoertuigen Diefstal van motorvoertuigen Diefstal van brom-, snor-, fietsen Zakkenrollerij Diefstal af/uit/van overige voertuigen Overige vermogensdelicten Diefstal/inbraak bedrijven en instellingen Winkeldiefstal	Delict J/N=="J" & (INP niv3 code=="1.1.1"| INP niv3 code=="1.1.2"| INP niv3 code=="1.2.1"| INP niv3 code=="1.2.2"| INP niv3 code=="1.2.3"| INP niv3 code=="1.2.4"| INP niv3 code=="1.2.5"| INP niv3 code=="1.6.2"| INP niv3 code=="2.5.1"| INP niv3 code=="2.5.2")
Misdrijven tegen lichamelijke integriteit	Bedreiging Mishandeling Openlijk geweld (persoon) Overval Straatroof Moord, doodslag Zedenmisdrijf	Delict J/N=="J" & INP niv2 code=="1.4"
Fraude delicten	Horizontale fraude Verticale fraude Overige fraude	Delict J/N=="J" & INP niv2 code=="3.9"

Bijlage 12: Samenstelling begeleidingscommissie

prof. dr. P.G.M. van der Heijden (Universiteit Utrecht) - voorzitter, vanaf 31 augustus 2022

prof. dr. B.F.M. Bakker (Centraal Bureau voor de Statistiek / Vrije Universiteit Amsterdam) - voorzitter, tot 31 augustus 2022

drs. A.W.M. Eijken (Ministerie van Justitie en Veiligheid - Directoraat-Generaal Straffen en Beschermen)

dr. H.C.J. van der Veen (Wetenschappelijk Onderzoek- en Datacentrum)

dr. J.A. van Wilsem (Algemene Rekenkamer)

dr. A. Bagheri, vanaf 11 mei 2023 (Universiteit Utrecht)

Het NSCR is onderdeel van de institutenorganisatie van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO)

Bezoekadres:
De Boelelaan 1077
1081 HV Amsterdam

Postadres:
Postbus 71304
1008 BH Amsterdam

T 020 598 5239
E nscr@nscr.nl
W www.nscr.nl

nscr

Nederlands Studiecentrum
Criminaliteit en Rechtshandhaving