De coronacrisis als cyberkeerpunt?

Op zoek naar lokaal handelingsperspectief in de aanpak van gedigitaliseerde criminaliteit

Jelle Kort
Remco Spithoven

« waakzaam en dienstbaar »

De coronacrisis als cyberkeerpunt?
Op zoek naar lokaal handelingsperspectief in de aanpak van gedigitaliseerde criminaliteit.

Jelle Kort
Remco Spithoven

Colofon

Uitgave: Politie, in opdracht van portefeuillehouder Gebiedsgebonden Politie, Frans Heeres
Datum: december 2021
Oplage: 150 exemplaren
Fotografie: Beeldbank politie, coverfoto: Rens Hulman
Drukwerk: Koninklijke Van der Most BV, Heerde
Informatie: portefeuille-ggp.korpsstaf@politie.nl

Inhoud

Voorwoord

'The streets were deserted though the police were alerted'

Met deze zin opende het nummer *Robbery, Assault and Battery* van het album *A trick of the tail* uit 1976, van de inmiddels klassiek geworden rockband Genesis. Het is een vreemde zin, uit een wellicht even vreemd muzikaal avontuur, wat maar net je smaak moet zijn. 45 jaar later was deze zin van Phil Collins en Tony Banks misschien wel relevanter dan ooit: de straten waren van 23 januari tot 28 april 2021 tussen tien uur 's avonds en half vijf in de ochtend praktisch verlaten, als gevolg van de avondklok die onderdeel was van de coronamaatregelen. Veel van het maatschappelijk verkeer werd ook buiten die tijden stilgelegd om het coronavirus te bestrijden. Maar dat betekende niet dat de criminaliteit is stilgevallen. Deze is verder van de wijk naar het web verplaatst. En de aangiften van gedigitaliseerde criminaliteit blijven binnenkomen. Ook lokaal is deze trend inmiddels zichtbaar.

Al voor de coronapandemie in het begin van het jaar 2020 zijn intrede deed, was de wind van de criminaliteit van richting aan het veranderen. Als neveneffect van de digitalisering werden en worden steeds meer mensen in Nederland het slachtoffer van gedigitaliseerde criminaliteit. De keerzijde van het gemak van onze digitale voorzieningen is een nieuwe kwetsbaarheid die criminelen maar al te graag uitbuiten. Voor 2018 werd de schade van cybercriminaliteit in Nederland alleen al op 10 miljard euro geschat (Deloitte, 2017). Voor het jaar 2021 wordt de wereldwijde schade van cybercriminaliteit geschat op 6 biljoen dollar. Dat zou verdubbeling zijn in vergelijking met 2015 en zelfs een overschrijding van de wereldwijde opbrengst van drugshandel (Ahamad, 2020; Naidoo, 2020). Cybercriminaliteit is big business.

De coronapandemie en de maatregelen om de verspreiding van het virus tegen te gaan hebben de gelegenheid om criminaliteit digitaal te plegen verder opgestuwd. Meer mensen werken thuis en zijn meer gebruik gaan maken van sociale media om contacten met vrienden en familie te onderhouden. Wat zouden we zonder het internet in deze pandemie moeten? Maar ook criminelen profiteren van het internet tijdens de coronacrisis. Met een beetje technische kennis en wat drukken op de knop – of het inkopen daarvan – kan een groot aantal slachtoffers veel geld afhandig worden gemaakt, zonder dat je er als crimineel de deur voor uit hoeft. Dit had de Nederlandse politie al langere tijd door (Politie Oost-Nederland, 2019). Toch is het anno 2021 nog steeds zoeken wat de politie nu met de gedigitaliseerde criminaliteit aan moet, zeker op lokaal niveau.

De beweging binnen de politie van de wijk naar het web gaat niet zonder slag of stoot. Ook lokaal zal verdere invulling gegeven moeten worden aan de digitale politietaak. Daarbij kent de verbinding tussen de wijk en het web de nodige potentie voor de aanpak van gedigitaliseerde criminaliteit. De *old school* crimineel die Collins en Banks in hun muziekstuk uit 1976 beschreven, heeft immers goeddeels plaatsgemaakt voor een nieuwe, online generatie. Daar lijkt met de coronapandemie een nieuwe aanwas bijgekomen (Vu et al., 2020; Collier et al., 2020; Horgan et al., 2021). Maar ook deze generatie woont ergens en kan daar als zodanig worden gekend. Hoe krijgen gebiedsgebonden politiemedewerkers deze scherper in het vizier, en hoe kan de politie op digitalisering inspelen?

Bij deze belangrijke zoektocht hopen wij een helpende hand te bieden met ons verkennende onderzoek naar het lokale handelingsperspectief van districten en basisteams in de aanpak van gedigitaliseerde criminaliteit. Dit onderzoek hebben wij bij het district IJsselland kunnen uitvoeren, in opdracht van de portefeuillehouder Gebiedsgebonden Politie Frans Heeres. Wij zijn hen hier zeer erkentelijk voor.

Jelle Kort & Remco Spithoven,
November 2021

Samenvatting

De aanpak van gedigitaliseerde criminaliteit is een actueel en belangrijk vraagstuk voor de politie, dat door corona nog belangrijker werd. Cybercriminaliteit was ook vóór de coronapandemie al sterk in opkomst, maar het aantal geregistreerde gevallen nam het afgelopen jaar sterk toe. Dit onderzoek richt zich op de versterking van de aanpak op lokaal niveau, in het politiedistrict IJsselland. Het doel is enkele recente leerervaringen te verzilveren: Wat zijn de opgedane ervaringen in een grootschalig onderzoek naar vriend-in-noodfraude, waarbij tussen het basisteam IJsselland-Zuid en het cybercrimeteam van de eenheid Oost-Nederland werd samengewerkt? Waar loopt het IJssellandse digitaal flexteam tegenaan? Aan de hand van deze vragen wordt geprobeerd een eerste beeld te schetsen van de stand van zaken, van de mogelijkheden en van de uitdagingen waar het gaat om de aanpak van gedigitaliseerde criminaliteit anno 2021 – vooral op het lokale niveau.

De toename van gedigitaliseerde vormen van criminaliteit is zodanig dat de politie hier op elk niveau in de organisatie op zal moeten inspelen. Volgens geïnterviewde politiemensen hebben ook al langer bekende criminelen de omschakeling naar het wereldwijde web gemaakt bij het plegen van misdaden. Kennis van de lokale situatie en van de digitale dimensie van criminaliteit zijn beide cruciaal geworden voor goed gebiedsgebonden politiewerk. Ondersteuning van basisteams en districtsrecherche met opleidingen, faciliteiten en de invoering van nieuwe functies (bv. taakaccenthouders in de basisteams of digitale wijkagenten) kunnen daarbij als belangrijke, zij het nog beperkt ingevulde randvoorwaarden worden beschouwd. Daarnaast lijkt samenwerking voor de districten van groot belang. Gedigitaliseerde criminaliteit is vaak sterk vertakt, waarbij daders zich zelden tot een klein geografisch gebied beperken. Om te zorgen dat cybercriminaliteit toch kan worden aangepakt, ook op het districtelijke niveau, is samenwerking met onder meer het cybercrimeteam Oost-Nederland cruciaal gebleken. Zo heeft een projectmatige samenwerking tussen het district IJsselland en dit team in korte tijd aanzienlijk resultaat opgeleverd: na een ‘veegweek’ kon in 26 zaken een strafrechtelijke reactie volgen, waarbij twee digitale oplichters fikse celstraffen kregen.

Het digitaal flexteam binnen het district IJsselland toont aan dat er digitaal potentieel zit in het basisteam. Op basis van een brede taakstelling wordt door dit team ondersteuning geboden op het gebied van social media en de aanpak van gedigitaliseerde criminaliteit. Focus, faciliteiten en opleiding verdienen aandacht bij de eventuele doorontwikkeling van dit team. Ook wordt duidelijk uit de opgedane ervaringen dat voor een steviger leereffect nodig is dat er meer prioriteit wordt gegeven aan gedigitaliseerde criminaliteit, zodat basisteams en districtsrecherche ook zelfstandig meer kennis en routine kunnen verkrijgen rond deze nieuwe materie.

Bij het voor de politie relatief nieuwe werkveld gedigitaliseerde criminaliteit is nog vaak onderwerp van discussie waar de eigen verantwoordelijkheid stopt en die van een ander politieonderdeel begint. Gedigitaliseerde criminaliteit is vrijwel niet aan grenzen gebonden, dus ook niet aan grenslijnen die door politieorganisatie en -informatie heenlopen. Deze grenslijnen veroorzaken momenteel sterke belemmeringen voor het aanpakken en voorkomen van gedigitaliseerde criminaliteit. Het cybercrimeteam Oost-Nederland is ten tijde van dit onderzoek een nieuwe, veelbelovende werkwijze opgestart om in te spelen op de specifieke kenmerken van gedigitaliseerde criminaliteit.

Allereerst heeft dit team het initiatief genomen om uitsluitend gestandaardiseerde, digitale aangiften te verzamelen en analyseren. Vervolgens worden gegevens gevorderd bij derden, o.a. op basis van verkregen bankrekeningnummers. Daarna worden verschillende aangiften gebundeld wanneer blijkt dat er overeenkomsten zijn die mogelijk in de richting van dezelfde verdachte wijzen. Deze aanpak stelt het cybercrimeteam in staat om de gebundelde aangiften als ‘werkpakket’ bij de districten uit te zetten

waar de verdachten woonachtig zijn. Daarbij kan het cybercrimeteam de criminele netwerken overzien en coördinerend opereren bij het oprollen van de netwerkstructuren in samenwerking met meerdere politiedistricten. In het district IJsselland zijn hier inmiddels goede ervaringen mee opgedaan.

De sleutels voor een effectieve aanpak van gedigitaliseerde criminaliteit op lokaal niveau liggen ons inziens in (I) het versterken van de landelijke informatiehuishouding, (II) het optimaliseren van de samenwerking tussen organisatieonderdelen van de politie en met partnerorganisaties en (III) het versterken van het bewustzijn en de digitale kennis en vaardigheden onder politiepersoneel.

1

Inleiding

Hoofdstuk 1
Inleiding

De ontwikkelagenda Gebiedsgebonden Politiewerk (de Vries & Hensen, 2018) geeft wat andere woorden aan de wettelijke politietaak en stelt dat de taak van de politie is: *'Mensen die in gevaar zijn beschermen of mensen die juist het gevaar veroorzaken tegen te houden'* (idem, p. 1). Terecht wordt in deze agenda opgemerkt dat het beschermen van potentiële slachtoffers en het tegenhouden van gemotiveerde daders op zichzelf niet verandert, maar de context waarbinnen deze taak wordt uitgevoerd verandert terwijl we ernaar kijken. Dat werd eens te meer duidelijk door de coronacrisis.

Ook voor de coronapandemie omarmden wij als samenleving massaal nieuwe digitale middelen zodra zij beschikbaar waren (Spithoven, 2020). Maar de coronacrisis heeft verandering gebracht in de relatieve vrijblijvendheid van digitale technologie: er wordt veel (meer) thuisgewerkt, maar ook sociale ontmoetingen vinden meer online plaats. Straten zijn soms leeg, maar het wereldwijde web is bij momenten overbelast. Niet alleen werknemers en jongeren zijn noodgedwongen 'van de straat naar het web' gegaan. Ook voor criminelen is er als gevolg van de coronacrisis letterlijk minder op straat te halen. Daar waren criminelen en criminele netwerken echter al ruimschoots voor de coronacrisis op toegerust. Als neveneffect van de maatschappelijke digitalisering heeft zich de afgelopen decennia immers online een walhalla aan mogelijkheden voor het plegen van criminaliteit ontwikkeld. Daarbij is iedereen intussen zo gewend aan snel betalen, bestellen en doorgeven van zaken dat er handig op dit maatschappelijk vertrouwen in digitale transacties kan worden ingespeeld.

De coronacrisis heeft de routine-activiteiten van nagenoeg de totale wereldbevolking in een ongekend korte tijd zeer ingrijpend veranderd (Lallie et al., 2021; Hawdon, Parti & Dearden, 2020; Monteith et al., 2021; Horgan et al., 2021). Daarmee is de – al voor de coronacrisis verschuivende – balans tussen wijk en web synchroon lopend met de coronamaatregelen verder naar het web doorgezet. Een soortgelijke stroomversnelling is echter ook zichtbaar in het slachtofferschap. Tijdens de *lockdowns* nam het digitaal slachtofferschap een vlucht terwijl veel van de klassieke criminaliteit die in de openbare ruimte plaatsvond sterk afnam. In de periode tussen de *lockdowns* kwamen de winkeldiefstallen, openbare geweldplegingen en woninginbraken overigens wel weer terug. Te verwachten is dat cybercriminaliteit na de coronacrisis op een hoog niveau zal blijven: *'Even as lockdowns ease, it is reasonable to suspect that certain far-reaching socialorganisational and economic changes, for example to working patterns and online shopping, are likely to persist well into the future.'* (Horgan et al., 2021: 8). Op basis van de ontwikkeling van de criminaliteitsstatistieken tussen de *lockdowns* is de verwachting immers dat de klassieke offline criminaliteit na de coronapandemie weer terug zal komen omdat de gelegenheid daartoe weer toe zal nemen, maar dat cybercriminaliteit daarnaast zal blijven bestaan (Buil-Gil et al., 2020).

Met de coronapandemie, mede onder invloed van verveling en werkloosheid, heeft een nieuwe aanwas van cybercriminelen plaatsgevonden (Vu et al., 2020; Collier et al., 2020; Horgan, et al., 2021). De coronacrisis maakt eens temeer duidelijk: cybercriminaliteit is *here to stay*. Maar waar begin je in de lokale aanpak van cybercriminaliteit? Duidelijk is dat de aanpak van wat gedigitaliseerde criminaliteit (of *cyber-enabled crime*) wordt genoemd hierbij het meest relevant en opportuun wordt geacht omdat op lokaal niveau de daders en dadergroepen actief zijn maar ook potentiële slachtoffers goed te bereiken zijn (Leukfeldt, Spithoven & Misana-ter Huurne, 2020). Gedigitaliseerde criminaliteit wordt – gezien de aantallen slachtoffers en de omvang van de maatschappelijke schade – door veel politiemensen al als de nieuwe Veel Voorkomende Criminaliteit (VVC) beschouwd. In het volgende hoofdstuk wordt het begrip cybercriminaliteit nader gedefinieerd. Wij leggen in wat volgt vooral de nadruk op de lokale aanpak van gedigitaliseerde criminaliteit.

De gemiddelde diender op straat en de basisteams waar zij toe behoren hebben doorgaans de handen vol aan de noodhulp en de offline criminaliteit. Als gevolg van een optelsom van verschillende bezuinigingen in combinatie met taakuitbreiding is er in het reguliere politiewerk al sprake van een chronische overbelasting (Terpstra, Five & Salet, 2019). Toch zal er een beweging richting de aanpak van (met name) gedigitaliseerde criminaliteit moeten komen. Boekhoorn (2020) benadrukte recent de noodzaak voor de Nederlandse politie om kennis en kunde in de omgang met gedigitaliseerde criminaliteit breder over de lagen van politie-eenheden te verspreiden. Een kennisimpuls is volgens (Jansen et al., 2020) vooral nodig bij medewerkers Intake & Service, GGP-medewerkers en basisteam-recherche. Hierbij kunnen cybercrimeteams een aanjagende functie vervullen. Maar de komst van deze teams, aangevuld met een Landelijk Meldpunt Internetoplichting (LMIO) en een Cyber Offender Prevention Squad (COPS), lijkt er vooral toe te leiden dat lokale onderdelen van politie-eenheden de urgentie voor de aanpak van gedigitaliseerde criminaliteit niet ervaren en hier weinig tot geen taken of ontwikkelopgaven voor zichzelf zien.

Al in 2012 constateerden Struiksma, de Vey Mestdagh en Winter dat er ook op lokaal operationeel niveau kennis en vaardigheden moeten bestaan in de omgang met gedigitaliseerde criminaliteit. Toen klassieke vormen van criminaliteit min of meer opdroogden tijdens de eerste *lockdown* werd het echter ook op lokaal niveau glashelder dat veel mensen slachtoffer worden van gedigitaliseerde criminaliteit en dat dit wel degelijk een grote impact op slachtoffers heeft. Er moet duidelijk iets veranderen in de lokale omgang met gedigitaliseerde criminaliteit: het neemt fors toe en doet zich steeds weer in nieuwe gedaanten voor, waarbij criminelen hun modus operandi veranderen en het onderscheid tussen gedigitaliseerde criminaliteit en andere vormen van cybercriminaliteit vervaagt. Maar wat is de rol van gebiedsgebonden politiemedewerkers
in de aanpak van die toenemende gedigitaliseerde criminaliteit?

De opdracht die de portefeuille GGP voor zichzelf in 2018 stelde – *'(...) om het werken in de wijk én op het web verder te ontwikkelen en te integreren. We moeten bij de tijd zijn, dat willen wij zelf, maar dat verwacht de burger ook van ons.'* (de Vries & Hensen 2018, p. 2) – sluit bij deze beweging aan en heeft als gevolg van de coronacrisis meer urgentie gekregen. Daarbij is ook van belang het volgende te beseffen: ondanks dat gedigitaliseerde criminaliteit voor veel dienders, om verschillende begrijpelijke redenen, nog een vaag begrip zal zijn, maakt hun lokale bekendheid en verbondenheid wel degelijk een potentieel verschil (Collier et al., 2020; Horgan et al., 2021; Leukfeldt, Spithoven & Misana – ter Huurne, 2020). De vraag is echter wat men lokaal nodig heeft om een effectieve invulling aan deze rol te kunnen geven.

Om deze vraag te beantwoorden sluiten wij in dit onderzoek aan bij de praktijk van het politie-district IJsselland. Tijdens de coronacrisis heeft dit district de handschoen opgepakt om hun eerste stap in het lokaal aanpakken van gedigitaliseerde criminaliteit te zetten. In samenwerking met het cybercrimeteam Oost-Nederland hebben zij de nodige successen behaald en leereffecten opgedaan. Samen met medewerkers van dit district beantwoorden wij in dit onderzoek de onderzoeksvraag *'Hoe kan het Gebiedsgebonden Politiewerk in het district IJsselland in samenspel met andere (organisatie) onderdelen meer worden toegerust op het effectief aanpakken van gedigitaliseerde criminaliteit?'*. Daarbij is onze doelstelling niet alleen om het district IJsselland te ondersteunen, maar tevens het lokale leereffect beschikbaar te stellen aan andere politieonderdelen.
In het volgende hoofdstuk werken wij de onderzoeksvraag verder uit in deelvragen en voorzien wij deze van een onderzoeksopzet met verschillende methoden en onderzoeksstappen.

2

Op zoek naar gebiedsgebonden handelingsperspectief

Hoofdstuk 2

Op zoek naar gebiedsgebonden handelingsperspectief

In dit hoofdstuk werken we de onderzoeksopzet uit. We beginnen in paragraaf 2.1 met de doelstelling en onderzoeksvragen. Daarna behandelen we in paragraaf 2.2 de onderzoeksmethoden en in paragraaf 2.3 de voorgenomen onderzoeksstappen. Duidelijk was dat in dit actieonderzoek niet alles op voorhand kon worden overzien en dat mogelijk extra aandacht moest worden besteed aan deelaspecten, zoals de (landelijke) informatiehuishouding van de Nationale Politie ten aanzien van gedigitaliseerde criminaliteit. De vijfde en laatste onderzoeksstap, aansluitend bij de vijfde deelvraag, wordt in paragraaf 2.4 behandeld.

2.1 Doelstelling en onderzoeksvragen

Het doel van dit onderzoek is om (I) het leereffect van het district IJsselland in de aanpak van gedigitaliseerde criminaliteit landelijk in kaart te brengen en beschikbaar te stellen en (II) aanknopingspunten voor een versteviging van de lokale aanpak te vinden. Samen met medewerkers van het politiedistrict IJsselland en de eenheid Oost-Nederland onderzochten wij hoe de verschillende onderdelen van het district en de bredere, Nederlandse politieorganisatie met elkaar kunnen leren om gezamenlijk, lokaal meer toegerust te zijn op de gedigitaliseerde criminaliteit. De hoofdvraag luidde daarbij:

Hoe kan het Gebiedsgebonden Politiewerk in het district IJsselland in samenspel met andere (organisatie)onderdelen meer worden toegerust op het effectief aanpakken van gedigitaliseerde criminaliteit?

De deelvragen bij deze hoofdvraag luiden als volgt:

1. Wat is er in de internationale en nationale literatuur bekend over de ontwikkeling van gedigitaliseerde criminaliteit tijdens de coronacrisis en over hoe deze vormen van criminaliteit effectief kunnen worden aangepakt?
2. Wat is het leereffect van de gebiedsgebonden medewerkers van het district IJsselland in de aanpak van gedigitaliseerde criminaliteit?
3. Wat is het leereffect van het digitaal flexteam van het district IJsselland in de aanpak van gedigitaliseerde criminaliteit?
4. Welke knelpunten ontstaan er in de huidige, gebiedsgebonden aanpak van gedigitaliseerde criminaliteit door het district IJsselland?
5. Hoe kan Gebiedsgebonden Politiewerk in het district IJsselland bijdragen aan het effectief aanpakken van gedigitaliseerde criminaliteit in samenwerking met andere onderdelen van het district IJsselland, de eenheid Oost-Nederland en het nationale niveau?

2.2 Onderzoeksmethoden

In dit onderdeel beschrijven wij de onderzoeksmethoden die wij in dit onderzoek hebben gehanteerd. We beginnen bij de hoofdmethode van actieonderzoek, gevolgd door de submethoden van deskresearch en kwalitatieve interviews en focusgroepen.

2.2.1 Hoofdmethode: Actieonderzoek

De hoofdmethode van dit project is actieonderzoek. Onder actieonderzoek verstaan wij het streven om geëvalueerde interventies te ontwikkelen om een aspect van een huidige beroepspraktijk te verbeteren en vernieuwen (De Lange, Schuman & Montesano Montessori, 2011). Dit onderzoeksproject komt direct voort uit een concrete hulpvraag om de huidige situatie rondom het relatief nieuwe fenomeen van gedigitaliseerde criminaliteit te 'beschrijven, begrijpen en op te lossen' (idem, p. 109). Het project is dan ook volledig gericht op verbetering en innovatie van praktische werkwijzen in de aanpak van gedigitaliseerde criminaliteit.

Naast onderzoekers van het lectoraat Maatschappelijke Veiligheid van Hogeschool Saxion, werken ook professionals uit het politiedistrict IJsselland mee (Berding & Witte, 2013) om 'de eigen beroepspraktijk te veranderen' door 'er iets nieuws aan toe te voegen' (De Lange, Schuman & Montesano Montessori 2011, p. 109; Migchelbrink 2013, p. 90). Het proces dat met dit project zal worden ingegaan, kon op voorhand niet volledig in detail worden uitgewerkt. Actieonderzoek is immers *'(...) een dynamisch, complex en soms chaotisch verlopend proces waarin verschillende fasen door elkaar lopen, parallel aan elkaar zich ontwikkelen en/of in elkaar overgaan'* (De Lange, Schuman & Montesano Montessiori, 2011, p. 114).

Er kan bij actieonderzoek echter wel op voorhand worden nagedacht over te nemen onderzoeksstappen, maar het verloop van de uitvoer van deze stappen is minder rigide dan bij klassiek wetenschappelijk onderzoek. Zo bleek gedurende het onderzoeksproces dat er meer aandacht moest worden besteed aan de informatiehuishouding van de Nationale Politie om de vijfde en laatste onderzoeksvraag goed te kunnen beantwoorden.

2.2.2 Sub methode 1: Deskresearch

Onder deskresearch verstaan wij kortweg het gebruik maken van bestaande gegevens. Daarbij ligt de focus in dit onderzoek vooral op het onderzoeken van overheidsbronnen en academische bronnen (Baarda, de Goede & Teunissen, 2013). Onder overheidsbronnen verstaan wij numerieke overzichten en rapporten van politie, openbaar ministerie en gemeenten over cybercriminaliteit en de coronacrisis. Deze overzichten zijn aangevuld met academische publicaties als boeken en numerieke databestanden.

2.2.3 Sub methode 2: Kwalitatieve interviews en focusgroepen

De inzichten op basis van deskresearch zijn aangevuld met interviews en focusgroepen. Onder interviews worden vraaggesprekken verstaan waarin respondenten wordt gevraagd toe te lichten hoe zij concepten begrijpen en hoe zij daar betekenis aan verlenen (Barbour, 2008). Daarbij gaat het om het begrijpen van de respondenten aan de hand van hun referentiekader door te luisteren wat zij zeggen en hoe ze dat zeggen (Beyens & Tournel, 2009). Onder focusgroepen wordt een groepsgesprek tussen deelnemers verstaan, waarbij de nadruk niet zozeer op betekenisgeving maar vooral ligt op het genereren van ideeën. Hierdoor kunnen zowel meerdere mensen tegelijk worden gesproken als meningen van deelnemers onderling worden uitgewisseld (Baarda, de Goede & Teunissen, 2013). Omdat er nog relatief weinig bekend is over de lokale aanpak van gedigitaliseerde criminaliteit, was voor het slagen van de interviews en focusgroepen cruciaal dat de respondenten voor het toelichten van hun opvattingen voldoende ruimte zouden krijgen. De vragen zijn daarom beperkt tot een beperkt aantal items, en van een vaste volgorde en formulering was geen sprake (vgl. Babbie, 1998). Dit is overigens vrij gangbaar in actieonderzoek (Berding & Witte, 2013; De Lange, Schuman & Montesano Montessori 2011; Migchelbrink, 2013).

Tijdens de diepte-interviews (25 geïnterviewden in totaal, zie bijlagen voor een overzicht) en tevens tijdens twee focusgroepen (idem), werden respondenten zo vrij mogelijk gelaten om de voor hen meest belangrijke aspecten eruit te lichten (Barbour, 2008; Beyens & Tournel, 2009). De focusgroepen of *brainstorms* werden gehouden met hoofdzakelijk medewerkers van Basisteam IJsselland-Zuid en van Basisteam Vechtdal; o.a. operationeel expert OCP, Intake & Service medewerkers, GGP- en

noodhulpmedewerkers. Hieraan werd ook deelgenomen door rechercheurs van het cybercrimeteam Oost-Nederland en een teamchef van een basisteam. Deze onderzoeksactiviteiten hebben plaatsgevonden in de periode september 2020-juli 2021. Van alle interviews zijn geluidsopnames gemaakt om deze te transcriberen. Op deze wijze kon de benodigde diepgang van de analyse worden geborgd (Weiss, 1995). Bij het analyseren van de transcripten zijn de richtlijnen van Saldaña (2012) en Frieze (2014) gevolgd.

2.3 Vier onderzoeksstappen

Om de onderzoeksvragen te beantwoorden zijn naast de eerste, theoretische onderzoeksvraag, de volgende vier empirische onderzoeksstappen bij aanvang van het actieonderzoek voorzien.

2.3.1 Stap 1: Leren

Binnen het district IJsselland is het flexteam al voor de coronacrisis ingezet op gedigitaliseerde criminaliteit. Ook heeft het districtelijk recherecheteam de laatste jaren de nodige zaken met componenten van gedigitaliseerde criminaliteit gedraaid. De meeste betrokken medewerkers van het district IJsselland hadden voorafgaand geen specifieke kennis op dit gebied maar moesten noodgedwongen snel leren. Waar liepen zij tegenaan? Deze leerervaring moeten we niet verliezen en snel in retrospectief verzilveren. Om dit leereffect te verzilveren zullen we interviews houden met de direct betrokken personen.

2.3.2 Stap 2: Nadenken

Brainstormsessies met Medewerkers Service en Intake, Medewerkers GGP, Generalist GGP, Senior GGP, Generalist Tactische Opsporing (TO). Senior TO, Operationeel Expert TO op het niveau van het basisteams IJsselland-Zuid (Deventer en omgeving) en Vechtdal (Ommen en omgeving): Waar zouden onze lokale criminelen tijdens de *lockdown* mee bezig zijn geweest? Waar is online de veelvoorkomende criminaliteit te plegen? En welke digitale middelen gebruiken zij daarbij? Wat is de lokale rol in de aanpak van gedigitaliseerde criminaliteit? Om antwoord op deze vragen te krijgen werden twee focusgroepen gehouden.

2.3.3 Stap 3: Afstemmen lokaal en landelijk niveau

In de toewijzing van zaken hebben de verschillende Operationele Coördinatie Punten (OCP's) van de basisteams en districtsrecherche een belangrijke rol. De districtsrecherche heeft een rol in het oppakken van zaken die in complexiteit, seriematigheid of qua demografisch gebied de basisteams overstijgen. Wat hebben de OCP's en de districtsrecherche hiervoor aan informatie nodig van de cybercrimeteams en eventuele andere collega's? En welke rol speelt de lokale prioritering van zaken terwijl zaken rondom gedigitaliseerde criminaliteit in de toekomst meer uit verschillende delen van het land of uit de landelijke organisatie zullen komen? Om antwoord op deze vragen te krijgen zijn interviews gehouden met medewerkers van het OCP en de Districtsrecherche. Ook is de leiding van de Districtsrecherche hierop in een groepsgesprek bevraagd.

2.3.4 Stap 4: Lokale ambitie bepalen

Stap 4 sluit aan bij de interviews onder stap 3. Criminaliteit is van oudsher lokaal ingebed: zowel daders en slachtoffers bevinden zich niet zelden in het lokale verzorgingsgebied. Maar gedigitaliseerde criminaliteit maakt criminaliteit minder grijpbaar: slachtoffers bevinden zich in heel het land. Dit heeft implicaties voor de haalbaarheid van lokale ambities. Hoe gaat het district IJsselland hiermee om? Welke zaken pakken zij lokaal op? En wat heeft iedereen daar – van Service en Intake, wijkagenten, districtsrecherche tot het cybercrimeteam van de eenheid Oost-Nederland – van elkaar voor nodig?

2.4 Een aanvullende, vijfde onderzoeksstap: Het land in

Om de laatste onderzoeksvraag 'Hoe kan Gebiedsgebonden Politiewerk in het district IJsselland bijdragen aan het effectief aanpakken van gedigitaliseerde criminaliteit in samenwerking met andere onderdelen van het district IJsselland, de eenheid Oost-Nederland en het nationale niveau?' te kunnen beantwoorden bleek nader onderzoek naar de landelijke informatiehuishouding rond gedigitaliseerde criminaliteit noodzakelijk. Daarom is in overleg met de opdrachtgever een aanvullende onderzoeksstap aan dit actieonderzoek toegevoegd.

Gedigitaliseerde criminaliteit is zelden een lokaal verschijnsel: daders werken op afstand en werken in criminele netwerken. De sterk geografisch gebonden verantwoordelijkheden binnen de politie (per basisteam, district en eenheid) en de hieraan gekoppelde informatiehuishouding kunnen hierbij tegenwerken. Al met al moet er worden nagedacht over: (I) Op welke manier moet gedigitaliseerde criminaliteit worden geregistreerd? (II) Op welk niveau en op welk thema moeten er analyses van die registraties plaatsvinden? (III) Wie of wat prioriteert en coördineert zaken die een bovenlokaal karakter hebben? (IV) Welke rol is hierbij weggelegd voor eenheids- en districtsniveau?

Om deze aanvullende vragen te beantwoorden gingen we in gesprek met het Landelijk Meldpunt Internetoplichting (LMIo), het cybercrimeteam Oost-Nederland en enkele andere sleutelfiguren die zich met de portefeuille Cybercrime van de Nationale Politie bezighouden. Deze stap zou kunnen leiden tot een vervolg-actieonderzoek waarin de opgedane inzichten in samenwerking met de praktijk tot aanpassingen in werkprocessen en informatiehuishouding zullen leiden om op het niveau van de Nationale Politie, de cybercrimeteams in het land, de eenheden, districten en de basisteams optimaal op gedigitaliseerde criminaliteit in te spelen.

In het volgende hoofdstuk richten wij ons op de eerste deelvraag: 'Wat is er in de internationale en nationale literatuur bekend over de ontwikkeling van gedigitaliseerde criminaliteit tijdens de corona-crisis en hoe deze vormen van criminaliteit effectief kunnen worden aangepakt?'

3

Gedigitaliseerde criminaliteit & de coronacrisis


51% 15:53
+31 6 251
online
Hoi pap! Dit is Suus. Kun je me helpen? 15:49
Ja natuurlijk. Wat is er? Heb je een nieuw nummer? 15:50
Ja, want ik heb een nieuwe provider. En daardoor kan ik nu nog niet internetbankieren... 15:50
Maar ik moet vandaag echt iets betalen. Ik stuur je de betaallink door. Je krijgt het morgen terug! Ok? 15:50
Ok. Stuur maar door. 15:50
Fijn pap, dankjewel! 15:50
1 ONGELEZEN BERICHT
Betaalverzoek van Pa@Linkie
linkie.me
Wil je mij alsjeblieft € 149,95 betalen voor “Rekening spoed” via https://linkie.me/pay/9aqqteqs2q1vtesjvul7
Typ een bericht

Hoofdstuk 3
Gedigitaliseerde criminaliteit & de coronacrisis

In dit hoofdstuk wordt allereerst het thema van gedigitaliseerde criminaliteit besproken. Want waar hebben we het dan precies over en hoe gaan cybercriminelen te werk? Deze vragen beantwoorden we in paragraaf 3.1. Daarna trachten we in paragraaf 3.2 grip te krijgen op het aandeel cybercriminaliteit in de Nederlandse politiecijfers en benaderen we de omvang van het slachtofferschap. In paragraaf 3.3 kijken we naar enkele digitale criminele verschijnselen die sinds de uitbraak van corona in Nederland door de politie en enkele andere organisaties in het Nederlandse nieuws zijn gebracht om de samenleving te waarschuwen. Vervolgens verkennen we in paragraaf 3.4 de internationale, wetenschappelijke *state of the art* van wat er bekend is over cybercriminaliteit tijdens de coronacrisis en de aanpak daarvan door de politie. In de afsluitende paragraaf (3.5) beargumenteren we waarom het noodzakelijk is om de nieuwe, digitale politietaak lokaal verder te verkennen.

3.1 Van cybercriminaliteit naar digitale vormen van bedrog en diefstal

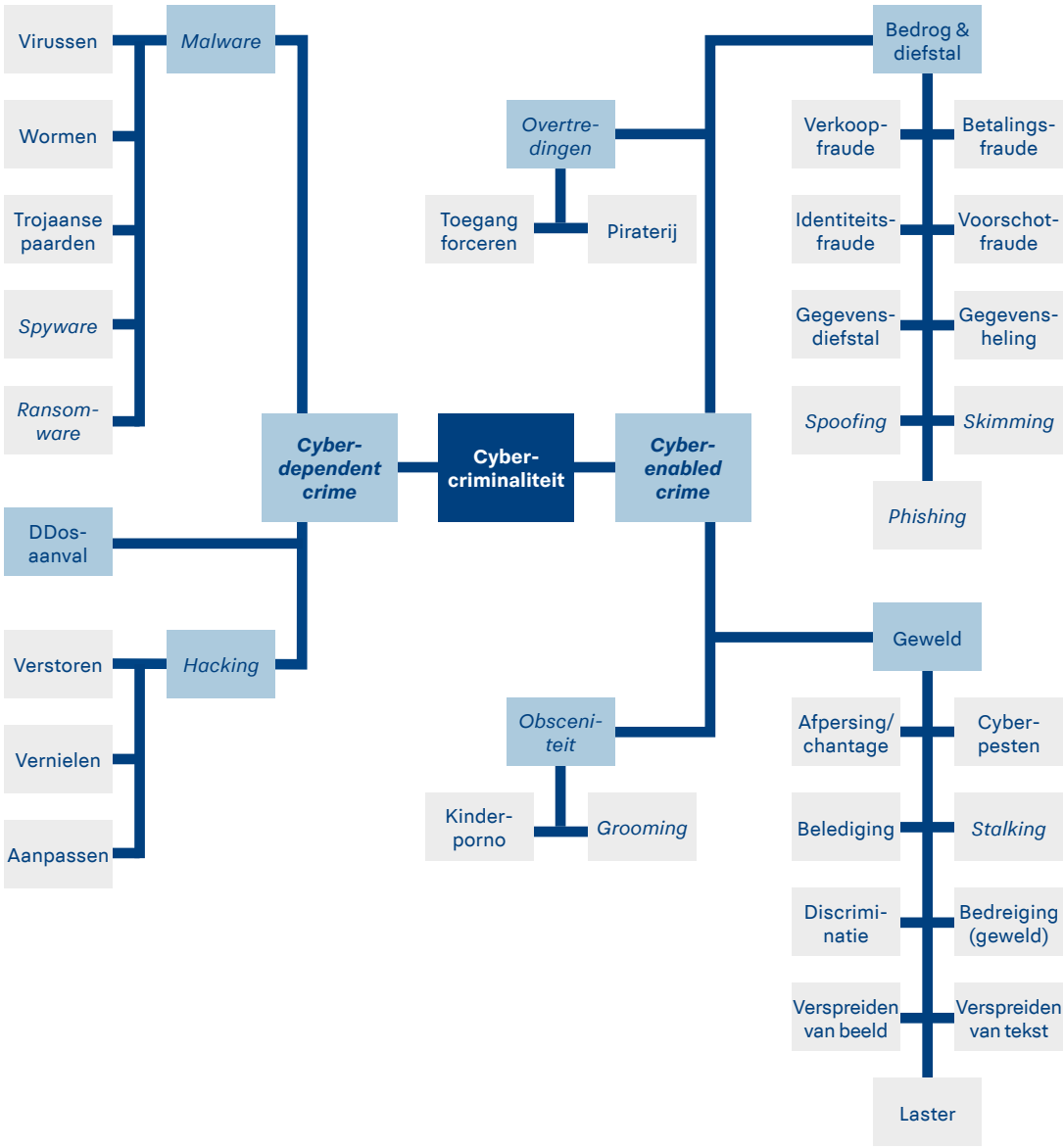
De context van gebiedsgebonden politiewerk verandert voortdurend. Zo bepalen in 2020 en 2021 de coronamaatregelen voor een belangrijk deel wat er van politiemensen wordt gevraagd. De opkomst van ICT, internet en cybercriminaliteit vormen voor de politie al langere tijd een meer structurele ontwikkeling waarop ingespeeld moet worden. Simpel gezegd betekent de opkomst van criminaliteit op het internet, dat politiewerk deels en in toenemende mate van de *wijk* naar het *web* zal moeten verschuiven (Politieacademie, 2019). In de afgelopen decennia heeft cybercriminaliteit een vlucht genomen, maar de coronacrisis heeft deze opkomende vorm van criminaliteit zichtbaarder gemaakt. De coronacrisis vormt daarmee een duidelijke, extra aanleiding voor de politie om haar rol in de aanpak van cybercriminaliteit verder te verkennen.

Cybercriminaliteit heeft de afgelopen decennia een vlucht kunnen nemen door drastische veranderingen in gelegenheidsstructuren die zich in korte tijd hebben voltrokken. Waardevolle zaken zijn van een fysieke vorm goeddeels in een gedigitaliseerde vorm overgegaan of hebben een digitale equivalent gekregen. Data is het nieuwe goud. Tegelijkertijd zijn inwoners zich in de fysieke wereld meer gaan beveiligen, omdat zij zich bewuster zijn geworden van de gelegenheid die zij met hun gedrag creëren. Maar online is van dergelijk risicobewustzijn en van daarop aangepast gedrag helaas nog te weinig sprake. Daarbij komt dat op het internet vrije informatiedeling hoog in het vaandel staat en bevoegdheden voor overheden om toezicht te houden beperkt zijn. De enorme gelegenheid voor gedigitaliseerde criminaliteit is daarbij te beschouwen als een belangrijk neveneffect van onze maatschappelijke digitalisering (Spithoven, 2020).

Spithoven stelde op basis van nationale en internationale wetenschappelijke publicaties de volgende taxonomie voor cybercriminaliteit op (Figuur 1). Daarbij bestaat er onderscheid tussen (I) *cyber-dependent* en (II) *cyber-enabled* criminaliteit. De eerste categorie (*cyber-dependent* criminaliteit) betreft compleet nieuwe vormen van criminaliteit die zonder de nieuwe informatietechnologie onmogelijk zouden zijn. Deze criminaliteit wordt gepleegd door middel van ICT waarbij ICT ook het doelwit is, zoals *hacks*, DDoS-aanvallen, virussen, *ransomware* en andere *malware*. Onder de tweede categorie (*cyber-enabled* criminaliteit) worden klassieke vormen van criminaliteit verstaan die door middel van ICT op een grotere schaal kunnen worden uitgevoerd, zoals oplichting, identiteitsfraude en *phishing* (Spithoven, 2020; Leukfeldt, 2016; 2018). Daarom wordt deze categorie cybercriminaliteit ook wel gedigitaliseerde criminaliteit genoemd. Zoals eerder vermeld ligt de focus van dit onderzoek op deze *cyber-enabled* of gedigitaliseerde criminaliteit, aangezien de aanpak hiervan voor het

lokale niveau het meest relevant lijkt. Deze vorm vertoont overeenkomsten met (veelvoorkomende) criminaliteit als bedrog en diefstal waarmee al ervaring bestaat, en de categorie *cyber-dependent* criminaliteit wordt eerder door specialistische teams opgepakt. Gedigitaliseerde criminaliteit: waar hebben we het precies over?

Figuur 1 – Taxonomie van cybercriminaliteit (Spithoven 2020, p. 49)



In deze categorie doelen Holt en Bossler (2014, p. 25 – eigen vertaling) op: 'het stelen van informatie of het illegaal verkrijgen van digitale eenheden van waarde van individuen of organisaties'. Het gaat daarbij om uiteenlopende digitale praktijken van oplichting en ontvreemding. Hieronder volgt een bloemlezing (Spithoven, 2020: 50-51): *'Onder (A) verkoopfraude wordt verstaan het niet ontvangen van goederen waarvoor wel is betaald. Bij (B) betalingsfraude wordt automatisch – via een complexe programmering – een groter bedrag afgeschreven dan het slachtoffer denkt over te maken wanneer online wordt betaald. Identiteitsfraude (C) betreft het buitmaken van persoonlijke gegevens door criminelen om zich voor te kunnen doen als het slachtoffer of om wederrechtelijk van diens digitale platformen gebruik te maken. Onder (D) voorschotfraude wordt het voorhouden van een groot geldbedrag gezien waarbij het slachtoffer om dit bedrag te bemachtigen eerst zelf een geldbedrag moet overmaken, maar het grote geldbedrag nooit ontvangt. Gegevensdiefstal (E) betreft het overnemen van gegevens die niet voor de dader bestemd zijn. Bij (F) gegevensheling worden buitgemaakte gegevens doorverkocht. In het geval van (G) spoofing doen criminelen zich digitaal voor als een door het slachtoffer vertrouwde identiteit – bijvoorbeeld de bank of overheid – om illegaal voordeel in de vorm van informatie of geld buit te maken. Bij (H) skimming worden op een onrechtmatige manier gegevens van of over een bankpas verkregen om deze na te kunnen maken en de eigenaar vervolgens geld afhandig te maken. Phishing (I) betreft het proces waarbij andermans persoonlijke informatie op een schijnbaar vertrouwde wijze wordt buitgemaakt.'*

Voor deze vormen van gedigitaliseerde criminaliteit maken daders naast technologie gebruik van *social engineering.* Daarbij gaat het om beïnvloeden, manipuleren en/of misleiden van slachtoffers met als doel hen geld of waardevolle informatie afhandig te maken. Daarbij kunnen cybercriminelen terugvallen op ervaringen van oplichting en misleiding die zo oud zijn als de mensheid. Digitale oplichters spelen in op de onwetendheid en de emoties van hun slachtoffers. Daarbij wordt doelbewust op de sociaalpsychologische beïnvloedbaarheid van mensen ingespeeld, meeliftend op de dagelijkse *overload* aan gedigitaliseerde communicatie. Ook wordt slim gebruik gemaakt van het inmiddels onbewust uitvoeren van digitale betalingen en het online afgeven van informatie. Mensen doen dat intussen op de automatische piloot, aan de lopende band, tussen alle bedrijven door. Digitale oplichters proberen vertrouwen bij hun slachtoffers te wekken door openbaar beschikbare en interne kennis over hun doelwit te benutten, bekende merken en beelden te gebruiken of tot in detail na te maken. Ook vragen zij niet direct om geld of informatie maar spelen zij in op emoties, percepties en denkfouten (Steinmetz, Goe & Pimentel, 2020).

Het aanspreken van sterke emoties bij de ontvanger – zoals vertrouwen, angst, urgentiegevoel, spanning, empathie, hebzucht en nieuwsgierigheid – leidt ertoe dat het denken van het slachtoffer wordt vertroebeld. Om dat verder kracht bij te zetten worden doelwitten gemanipuleerd om zo snel mogelijk te handelen (Steinmetz, Goe & Pimentel, 2020; Kayser, 2020). Daarnaast doen oplichters in hun boodschap vaak een beroep op de volgende principes (Steinmetz, Goe & Pimentel, 2020; Hadnagy, 2018):

- *Autoriteit*: men stuurt het bericht namens een bekende en gezaghebbende persoon of organisatie;
- *Consistentie*: de boodschap sluit grotendeels aan bij de strekking van eerdere berichten of de ontvanger wordt voor een keuze gesteld of in een situatie gebracht die zijn/haar consistentie in twijfel zou kunnen trekken;
- *Waarschijnlijkheid*: de afgegeven boodschap ligt in de lijn der verwachting bij het slachtoffer en speelt daarom vaak in op de actualiteit;
- *Wederkerigheid*: als de ontvanger iets voor de verstuurder of een ander doet, krijgt deze er iets anders voor terug;
- *Sociale validatie*: al meer mensen hebben gebruik gemaakt van de unieke kans;
- *Sociale verplichting*: kwetsbare mensen of onrecht worden aangevoerd waarbij de ontvanger van de boodschap hulp kan bieden of op kan treden;
- *Concessie*: er wordt eerst teveel van de ontvanger gevraagd om daarna hetgeen te vragen waar men op uit is, omdat het minder ingrijpend of duur is dan wat eerst werd gevraagd is men eerder geneigd om in te stemmen;

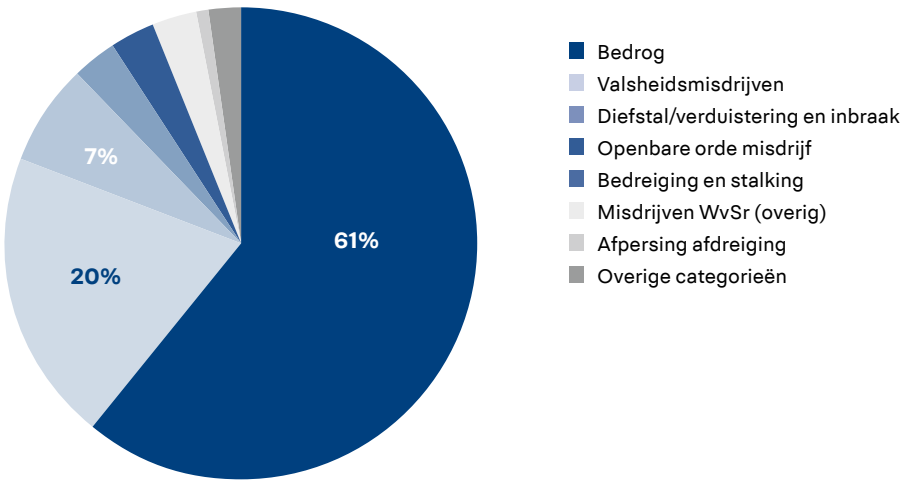
- *Schaarste*: er is maar een korte tijd weinig beschikbaar, waardoor men snel moet handelen;
- *Leuk vinden*: men wordt in de gelegenheid gebracht om iets te doen of ontvangen waardoor andere mensen hen leuk(er) zullen vinden.

Het moge duidelijk zijn: de digitale gelegenheid voor het uitoefenen van bedrog en diefstal wordt intussen flink uitgebuit. We zullen in de volgende paragraaf het aandeel cybercriminaliteit in de Nederlandse politiecijfers en de omvang van het slachtofferschap in kaart brengen. Daarbij zullen we zien dat het slachtofferschap van bedrog en diefstal, belangrijke vormen van gedigitaliseerde criminaliteit, hoogtij viert.

3.2 Aandeel cybercriminaliteit in Nederlandse politiecijfers

Het benaderen van de omvang van cybercriminaliteit in de door de politie geregistreerde criminaliteit is nog niet zo eenvoudig, zo stelt ook het CBS (z.d.): *'Slechts een klein deel van de relevante delicten kan namelijk via de huidige registratiemethoden worden afgeleid. Dit betekent dat er handmatig een onderscheid moet worden gemaakt tussen digitale delicten en traditionele vormen van criminaliteit in processen-verbaal. Deze handmatige methode is echter erg tijdrovend en bovendien foutgevoelig.'* Om toch een zinvolle benadering te kunnen geven heeft het CBS samen met de politie in de processen verbaal van 2016 een geautomatiseerde zoekslag gemaakt. Deze bestond uit drie delen: (I) het definiëren van cybercriminaliteit; (II) het opstellen van een algoritme welke via tekstanalyse werd getraind om cybercriminaliteitszaken te herkennen en (III) het testen en verbeteren van dit model. Als gevolg van deze exercitie werd duidelijk dat er bij negen procent van alle processen verbaal in 2016 sprake was van cybercriminaliteit, waarbij het veelal gaat om gedigitaliseerde criminaliteit. Het aandeel cybercriminaliteit dat geautomatiseerd door het CBS werd getraceerd in alle processen verbaal van 2016 betrof overwegend bedrog (61%) en valsheidsmisdrijven (20%), gevolgd door diefstal en/of verduistering en inbraak (7%), zie Figuur 2.

Figuur 2 - Cybercriminaliteit naar type delict (CBS, z.d.).



In de grove politiecijfers is direct een duidelijk effect van de eerste Nederlandse *lockdown* te zien. Met de verschuiving in gelegenheidsstructuren nam het aantal geregistreerde gevallen van cybercriminaliteit sterk toe, met in Nederland een extreme piek in mei 2020 van 1886 gevallen tegenover 'slechts' 387 in dezelfde maand een jaar eerder. Tegelijkertijd was sprake van een afname van de geregistreerde criminaliteit in het algemeen. Zo registreerde de politie in juli 2020 bijna 10 duizend minder misdrijven dan in juli 2019. De politie registreerde eveneens in juli 2019 bijna 600 woninginbraken minder dan een jaar eerder; een afname van 21 procent. Ook het aantal registraties van zakkenrollerij was in juli 2020 59 procent minder dan in juli 2019 [1]. De klassieke veelvoorkomende en *high impact crime* in het publieke domein daalde tijdens de *lockdown* en de cybercriminaliteit nam toe. Daarbij moet er voor de Nederlandse situatie wel rekening mee worden gehouden dat een deel van de gevallen van cybercriminaliteit vermoedelijk wordt geregistreerd onder andere categorieën, zoals (horizontale) fraude. Dat was overigens ook al voor corona het geval. Hierover later in dit rapport meer.

Ondanks dat er niet een harde uitspraak over de ontwikkeling van cybercriminaliteit kan worden gedaan is aannemelijk dat ook in Nederland het vooral de categorieën bedrog en diefstal zijn die toenemen. In de meest recente uitgave van de Veiligheidsmonitor benadrukt het CBS (2020) nogmaals wat er gaande is met de kop bij het persbericht: *'Minder traditionele criminaliteit, meer cybercrime'*. In 2019 gaf bijna 14 procent van de Nederlandse bevolking van 15 jaar en ouder aan slachtoffer te zijn geworden van traditionele criminaliteit zoals bedreiging, mishandeling, seksuele delicten, inbraak, diefstal, zakkenrollerij, beroving en vandalisme. Het aantal slachtoffers van deze traditionele criminaliteit is in 2019 echter bijna een derde lager dan in 2012. Voor cybercriminaliteit is een andere beweging zichtbaar in het slachtofferonderzoek. Waar in 2017 nog elf procent van de inwoners van 15 jaar en ouder aangaf slachtoffer van cybercriminaliteit te zijn geworden, is dit in 2019 toegenomen tot dertien procent. Het gaat dan vooral om slachtofferschap van hacken (5,5%), koop- en verkoopfraude (4,6%), cyberpesten (4,2%) en identiteitsfraude (0,5%). Als we deze inzichten uit de Veiligheidsmonitor afzetten tegen de politiecijfers uit Figuur 2, dan blijken slachtoffers verhoudingsgewijs minder aangifte bij de politie te doen bij *hacking* dan bij koop- en verkoopfraude.

Tijdens de coronacrisis dook een specifieke variant van bedrog op in de vorm van WhatsApp- of vriend-in-nood-fraude, waarbij de oplichter zich doorgaans via WhatsApp voordoet als een bekende van de ontvanger van het bericht en doet alsof er acute geldnood is. Onderzoek van de Haagse Hogeschool (van 't Hoff-de Goede & Leukfeldt, 2020) onder een representatieve steekproef van volwassen Nederlanders toonde aan dat in 2020 15 procent was geconfronteerd met een poging tot deze vorm van fraude. Daarvan maakte 5% daadwerkelijk geld over, wat goed is voor 0,7 procent van alle respondenten. Het ging daarbij vooral om kleine bedragen van onder de 50 euro (27%), tussen de 50 en 750 euro maar ook grotere bedragen van 750 tot 2500 euro (29%), 2500 euro tot 5000 euro (12%) en zelfs hogere bedragen (7%). Dat criminelen ook in Nederland gebruik maakten van de ontstane situatie in de corona-crisis en de maatregelen om de verspreiding van het virus tegen te gaan, was al vroeg duidelijk. In de volgende paragraaf verkennen we de vroege berichten over de toename van de cybercriminaliteits-dreiging waarvoor de politie en andere organisaties in het Nederlandse coronanieuws waarschuwden.

3.3 Cybercriminaliteit in het vroege, Nederlandse coronanieuws

Al op 17 maart 2020 – de eerste set coronamaatregelen van de Rijksoverheid zijn vijf dagen ervoor op 12 maart 2020 afgekondigd – werd op de website van de Nationale Politie uitgebreid bericht over cybercriminelen die misbruik zouden maken van de maatregelen rondom corona (Nationale Politie, 2020). De recent ontstane situatie zou zijn benut om persoonsgegevens van slachtoffers te verkrijgen,

1 Dataportaal van de politie geraadpleegd op 16 september 2020 via: https://data.politie.nl/?dl=3B50F#/Politie/nl/dataset/47013NED/table

bijvoorbeeld via nep-mails of nep-sms'jes, via malafide websites of nep-apps. Langs diverse wegen werden volgens het politiebericht 'besmette' links verspreid waarmee persoonlijke gegevens achterhaald kunnen worden of een computer kan worden geïnfecteerd met een computervirus of *malware*.

Ook andere vormen van cybercriminaliteit, veelal *gedigitaliseerde* criminaliteit, staken al snel extra de kop op volgens de politie, zoals oplichting door malafide webshops die corona-gerelateerde producten aanboden zoals persoonlijke beschermingsmiddelen, thuiswerk- en sportartikelen, waarbij producten wel werden betaald, maar niet geleverd. Op 1 april 2020 vermeldt *Algemeen Dagblad* dat de politie in de tussenliggende periode tien malafide webshops offline heeft gehaald die o.a. mondkapjes en zelftesten aanboden, maar na betaling niet leverden (Voskuil, 2020). Er gingen volgens het AD-bericht zelfs afpersingsmails rond waarin werd gedreigd de familie van de ontvanger te infecteren met corona als er niet zou worden betaald.

Al vroeg in de coronacrisis werd duidelijk dat de Nederlandse samenleving niet alleen plotsklaps kwetsbaar was geworden door het coronavirus, maar ook de dreiging van oplichting was toegenomen, veelal langs digitale weg. Eind april 2020 concludeerde programmadirecteur Digitalisering en Cybercriminaliteit van de Nationale Politie Theo van der Plas dat *'de cybercriminaliteit door de corona-crisis fors toeneemt'*, terwijl tegelijkertijd de criminaliteit in het algemeen daalt aldus Van der Plas in *EenVandaag* (AvroTros, 2020). Hij vult aan: *'Vooral WhatsApp-fraude en het aantal verstuurde phishing-mails nemen enorm toe in deze tijden van corona. Normaal hebben we iedere week honderd aangiften van WhatsApp-fraude. Door de coronacrisis ligt dit aantal nu op driehonderd per week.'* (Idem)

Kwetsbaren in de samenleving, met name ouderen, bleken slachtoffer te worden van gedigitaliseerde criminaliteit. Wil van Gemert van de Europese misdaadbestrijdingsorganisatie Europol zei, ook in *EenVandaag*, dat er meer dan 120.000 websites zijn die Covid-19 of corona als onderwerp hebben: 'Het merendeel is in onze ogen ontwikkeld om criminaliteit mee te plegen.' (AvroTros, 2020) Toch zijn het niet alleen individuele burgers die vaker het slachtoffer werden, ook bedrijven kregen last van 'corona-cybercriminaliteit': 'Eén op de veertien Nederlandse bedrijven heeft naar eigen zeggen sinds het begin van de coronacrisis te maken gekregen met cybercriminaliteit gerelateerd aan Covid-19. Dit blijkt uit onderzoek dat ABN Amro in mei 2020 heeft verricht onder 170 bedrijven.' (Monterie, 2020)

Internationaal zien we hetzelfde beeld in de berichtgeving, zo vraagt *Financial Times* zich af *'Why Covid-19 is a gift for cyber criminals'* (Financial Times, 2020) en wijst Deloitte ook al vroeg op *'the risks of working from home'* (Deloitte, 2020). Cybercriminelen wisselen van tactiek en maken misbruik van de angst die corona veroorzaakt. Daarbij vormt thuiswerken een bron voor nieuwe vormen van 'datadiefstal'. Een kwart van alle werknemers merkt sinds het begin van de coronacrisis een toename van frauduleuze e-mails, *spam* en *phishing*-pogingen in hun zakelijke e-mail; 26% van de respondenten in de enquête van Deloitte geeft aan dat ze momenteel in de verleiding komen om kopieën van waardevolle bedrijfsgegevens te bewaren voor het geval er een fatale aanval wordt gepleegd en het voortbestaan van het bedrijf in gevaar komt. Nog meer dan voorheen is tijdens de lockdown geboden dat bedrijven prioriteit geven aan preventieve maatregelen om het verlies van bedrijfsgegevens en intellectueel eigendom te voorkomen en het risico op bedrijfsfraude te verminderen, aldus het advies van Deloitte. (idem)

Duidelijk is dat de dreiging van cybercriminaliteit in coronatijd toenam in Nederland. In de volgende paragraaf verkennen we wat er in de internationale, wetenschappelijke literatuur bekend is over cybercriminaliteit tijdens de coronacrisis en de aanpak daarvan door de politie.

3.4 De wetenschappelijke state of the art over cybercriminaliteit en corona

Er is internationaal nog maar weinig wetenschappelijk onderzoek gedaan naar de impact van de coronacrisis op cybercriminaliteit (Collier et al., 2020). Onze zoektocht middels wetenschappelijke zoekmachines en tijdschriften met de zoektermen '(cyber)crime' en 'covid-19(corona)' en/of 'police(policing)' leverde slechts elf artikelen uit wetenschappelijke *peer reviewed* tijdschriften op. Duidelijk is al wel dat de combinatie van sociale isolatie, verstoring van dagelijkse routines, financiële tegenslagen en de blootstelling aan desinformatie die met de coronapandemie samenhangen, leidt tot ernstig geestelijk lijden waarbij slachtofferschap van cybercriminaliteit nog een flinke extra belasting kan geven (Monteith et al., 2021). Al met al tekent zich een somber beeld af waar het gaat om de sociale gevolgen van de *lockdowns* en het effect hiervan op de criminaliteit: '*The social, economic, and political consequences of lockdown, social distancing, and mass illness are becoming clearer, and evidence now suggests some large-scale transformation, at least in the short term, in patterns of crime'* (Horgan et al., 2021:5). Maar wat voor criminaliteitspatronen tekenen zich nu precies af in tijden van corona?

3.4.1 Verschuivingen in de criminaliteit als gevolg van de lockdown

Als gevolg van de maatregelen die gericht zijn op het laten afnemen van het maatschappelijk verkeer om de coronapandemie te bestrijden, wordt zichtbaar dat veel van de daarmee samenhangende criminaliteit ook opdroogt. In Schotland zag men bijvoorbeeld een daling van 18% in de aangiftecijfers, daarbij nam criminaliteit met een fysieke component af met 14% voor seksuele delicten, 26% voor winkeldiefstal en 29% voor andere diefstallen (Horgan et al., 2021). Omdat mensen minder op straat en onderweg zijn, nemen de daaraan gerelateerde vormen van criminaliteit af (Hawdon, Parti & Dearden, 2020). Maar dit betekende niet dat alle criminaliteit in de fysieke wereld stopte. Zo namen het huiselijk geweld en de meldingen van geluidsoverlast in de woonomgeving stevig toe (Hawdon, Parti & Dearden, 2020). Als gevolg van het thuiswerken en toegenomen gebruik van sociale media om sociale contacten te onderhouden steeg de gelegenheid voor cybercriminaliteit: *'(…) as persons spend more time connected to the Internet, and less time on the streets, opportunities for street violence and property crimes decrease while Internet crimes may increase'* (Buil-Gil et al., 2021:48). Het neveneffect van de strikte *lockdowns* was dat de gelegenheid voor criminaliteit van de straat naar het web verplaatste (Buil-Gil et al., 2021).

Cybercriminaliteit was al voor de coronapandemie een stevige zorg. Cybercriminaliteit staat volgens het World Economic Forum in de top vijf van grootste, wereldwijde risico's (World Economic Forum, 2019; Naidoo, 2020). Volgens de WHO is de omvang van cybercriminaliteit sinds de pandemie vervijfvoudigd (Collier et al. 2020). De jaarlijkse omvang van de schade van cybercriminaliteit wordt op 6 triljoen dollar geschat in 2021 waar dat in 2015 nog 3 triljoen dollar was (Ahamad, 2020; Naidoo, 2020). Cybercriminaliteit levert bij benadering criminele organisaties daarmee momenteel meer op dan de wereldwijde handel in drugs (Ahamad, 2020).

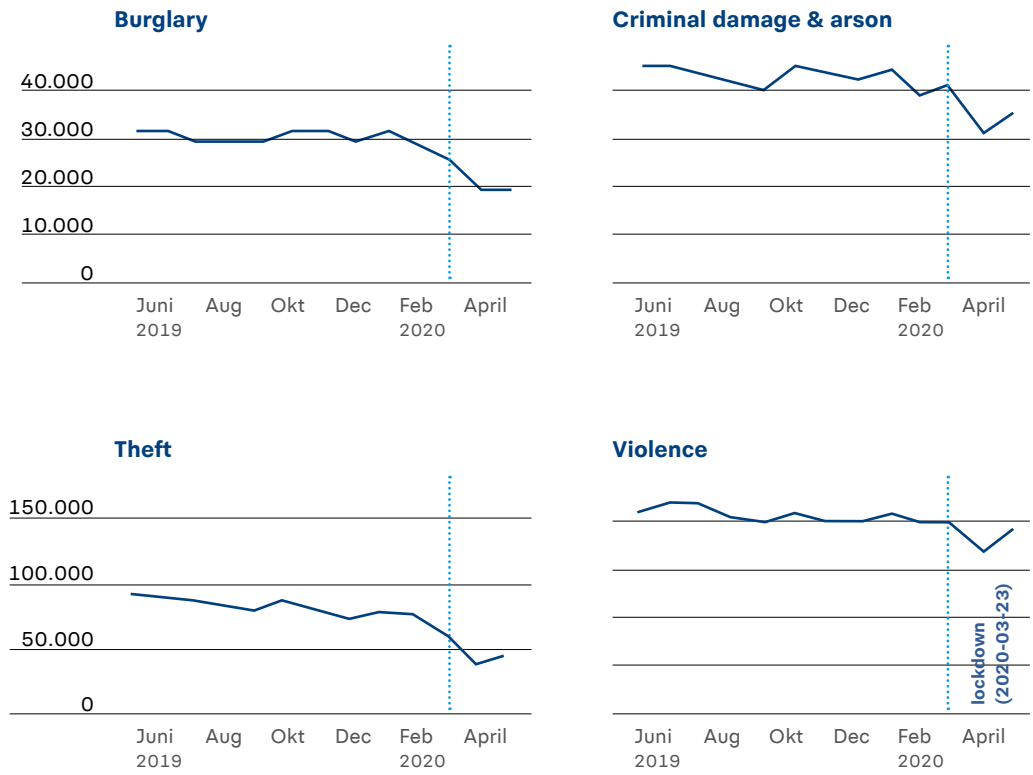
Over de vraag of cybercriminaliteit tijdens de coronapandemie en periodes van maatschappelijke *lockdowns* is toegenomen bestaat enige discussie. Op basis van een vergelijking van slachtofferschap van cybercriminaliteit in een aselecte steekproef van om en nabij de 1000 personen uit de Verenigde Staten van Amerika concluderen Hawdon, Parti en Dearden (2020) dat er maar weinig tot geen toename van slachtofferschap van cybercriminaliteit te zien zou zijn. Ander onderzoek leidt tot de tegenovergestelde conclusie, zoals hieronder duidelijk zal worden.

Een overall beeld uit Schotland

Vooral de studie van Buil-Gill en collega's (2021) geeft vanuit de strakke classificatie van politiecijfers voor gedigitaliseerde criminaliteit in Schotland een helder inzicht. Allereerst werpen we een blik op de ontwikkeling van klassieke criminaliteit in Schotland: de gestippelde lijn markeert het moment van de eerste *lockdown* in Schotland (Figuur 3). Duidelijk is dat inbraken, vandalisme, brandstichting en diefstallen afnamen. Opvallend is de lijn van geweld die vanaf de *lockdown* een daling laat zien. Deze

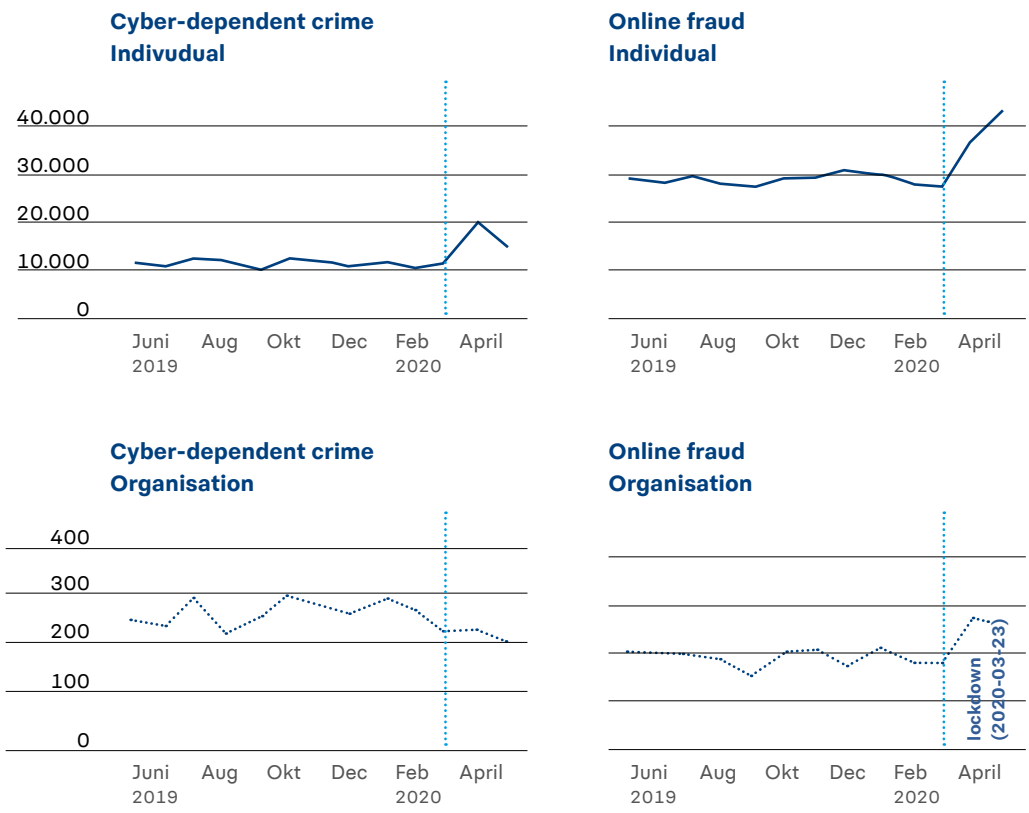
daling werd vooral verklaard door het sluiten van het uitgaansleven. Verderop in de *lockdown* klimt het geweld naar het oude niveau terug. Dit wordt verklaard door een toename van huiselijk geweld als gevolg van spanningen in gezinnen die naarmate de *lockdown* langer duurde eveneens toenamen. Als we daarnaast de cijfers voor gedigitaliseerde criminaliteit in Schotland zetten (Figuur 4), dan is een duidelijk verschil te zien met de voorgaande figuur (Figuur 3).

Figuur 3 – Ontwikkeling van klassieke criminaliteit in Schotland (Buil-Gil et al., 2021:49).



Kort na de start van de eerste *lockdown* in Schotland was duidelijk sprake van een toename in de cyber-dependent aanvallen, in de vorm van *hacking*, computer virussen en DDos-aanvallen (vooral gericht op individuen). Voor organisaties was een daling van deze typen aanvallen zichtbaar. Als het gaat om online fraude dan blijkt er voor aanvallen gericht op individuen een sterk stijgende lijn zichtbaar vanaf de *lockdown*. De fraude aanvallen gericht op organisaties namen tevens toe, zij het in lichtere mate.

Figuur 4 – Ontwikkeling van gedigitaliseerde criminaliteit in Schotland (Buil-Gil et al., 2021:55).



Toename van phishing

Vooral *phishing* bleek tijdens de coronapandemie toe te nemen (Tran, 2020). In maart 2019, vlak na de wereldwijde uitbraak van het coronavirus en het treffen van vergaande maatregelen in de bestrijding ervan, nam *phishing* naar schatting met 600% toe. *Phishing* fungeert vaak als een opstap-delict voor andere delicten als *hacking* of het verspreiden van *ransomware* (Lallie et al., 2021). Naar schatting slaagt 80% van de *phishing*-aanvallen door het gebruik van *Social Engineering* technieken (Naidoo, 2020), dat betekent dat *phishers* inspelen op de emotie van de ontvangers van hun berichten, waardoor zij minder weerstand tegen de boodschap van het bericht kunnen bieden. *Phishing* mails bevatten grofweg voor 70% *malware* en 30% zijn aanvallers uit op het ontfutselen van inloggegevens (Ahamad, 2020). Oplichters spelen in op de coronacrisis door 'COVID-19' of andere gerelateerde namen in de titels van *phishingmails* en *malware* op te nemen (Ahamad, 2020; Horgan et al. 2021). Naast individuele burgers moeten ook thuiswerkers alert zijn op *phishing*. Door het thuiswerken, zonder het reguliere bedrijfs-netwerk en in het eigen thuisnetwerk, zijn er minder mogelijkheden voor bedrijven om hun werknemers tegen *phishing* aanvallen te beschermen (Ahamad, 2020).

Nieuwe groep actieve daders

Als gevolg van de afname van de arbeidsdeelname en aanverwante stijging van de werkeloosheid zijn er waarschijnlijk meer, nieuwe gemotiveerde daders die online proberen op illegale wijze hun inkomsten te verkrijgen (Hawdon, Parti & Dearden, 2020). Dit past bij de observaties uit Schotland waar men vooral een toename van de niet tot nauwelijks technische cybercriminaliteit signaleerde (Collier et al., 2020). Vu en collega's concluderen op basis van hun longitudinale onderzoek naar cybercriminele

marktplaatsen dat er weliswaar een toename van het aantal transacties is, maar dat er als gevolg van de coronapandemie en de *lockdowns* geen sprake is van een echte transformatie van deze markt: *'The same kinds of transactions, users, and behaviours dominate (…), however volumes increase for all product categories. In terms of users, we see an uplift in numbers across most categories, but particularly in users making small numbers of sale'* (Vu et al., 2020: 563).

Nu we de verschuivingen in de criminaliteit als gevolg van de *lockdowns* in kaart hebben gebracht, werpen we een blik op potentiële verklaringen om daar in de aanpak van gedigitaliseerde criminaliteit op in te kunnen spelen.

3.4.2 Op zoek naar verklaringen aan de hand van de routine activiteiten theorie

Onderzoekers concluderen dat er als gevolg van de coronamaatregelen en hun neveneffecten meer nieuwe, kleine cybercriminelen actief zijn geworden, voornamelijk als gevolg van verveling en werkeloosheid (Vu et al., 2020; Collier et al., 2020; Horgan et al., 2021). Collier en collega's voegen daar aan toe dat nieuwe daders mogelijk meer negatieve spanning ervaren als gevolg van de pandemie en de maatregelen om deze te bestrijden, en dat zij meer tijd hebben dan voorheen om zich in cybercriminaliteit te gaan verdiepen (Collier et al. 2020; Horgan et al. 2021). Elk van deze verklaringen worden ook in eerder Nederlands onderzoek naar verklaringen voor daderschap van cybercriminaliteit aangedragen (Van der Wagen et al., 2019).

Als gevolg van de coronapandemie maar vooral als neveneffect van de getroffen maatregelen in de bestrijding van de verspreiding van het virus zijn de routine-activiteiten van nagenoeg de totale wereldbevolking in een ongekend korte tijd zeer ingrijpend veranderd (Lallie et al., 2021; Hawdon, Parti & Dearden, 2020; Monteith et al., 2021; Horgan et al. 2021). De in de criminologie klassieke routineactiviteiten theorie (Cohen & Fellson, 1979) wordt vaak op de verklaring voor gelegenheid voor cybercriminaliteit toegepast. Deze theorie omvat kortweg dat criminaliteit ontstaat waar de elementen van een gemotiveerde dader, een potentieel slachtoffer en de afwezigheid van toezicht in tijd en ruimte samenvallen. De toepassing van deze theorie op cybercriminaliteit is echter problematische vanwege het element dat een gemotiveerde dader en een potentieel slachtoffer volgens deze theorie in tijd en ruimte bij elkaar komen. Duidelijk is dat dit in de digitale omgeving niet langer in strikte zin opgaat. Dader en slachtoffer ontmoeten elkaar als het ware virtueel waarbij een dader gelijktijdig "ontmoetingen" met meerdere slachtoffers kan hebben. Online is er ook nagenoeg geen sprake van toezicht door anderen als gevolg van de sociale disorganisatie en afwezigheid van gedeelde normen en waarden (Hawdon, Parti & Dearden, 2020).[2]

Ondanks enkele beperkingen biedt de Routine Activiteiten Theorie de nodige handvatten om te verklaren wat er tijdens de coronapandemie gebeurde. De gelegenheid voor digitale fraude nam toe omdat meer mensen online gingen shoppen en er schaarste voor thuiswerk- en sportartikelen en persoonlijke beschermingsmiddelen ontstond. Door het sluiten van het uitgaansleven droogde de criminaliteit die daarmee gepaard ging op. Met het thuiswerken nam de mogelijkheid voor werkgevers om technische beveiligingsmaatregelen te treffen af. En de beweging naar sociale media om contact met vrienden, kennissen en familie te onderhouden maakte ook die platformen weer interessanter voor criminelen (Collier et al. 2020; Horgan et al. 2021).

De snelheid waarmee mensen noodgedwongen zijn overgegaan op digitale platformen om te kunnen blijven werken en contact met elkaar te houden, ging ten koste van de veiligheid (Naidoo, 2020; Horgan et al. 2021). Dit betekende ook dat digitaal minder ervaren en veiligheidsbewuste mensen

2 Meer over de toepassing van de Routine Activiteiten Theorie op cybercriminaliteit is te vinden in werk van Yar (2005), Holt en Bossler (2014), Leukfeldt (2016) en Spithoven (2020).

noodgedwongen online moesten om te blijven werken en met elkaar in contact te blijven (Hawdon, Parti & Dearden, 2020). Door *social distancing* zijn mensen meer afhankelijk geworden van ICT in hun werk, van online communicatie, betalingen, informatie-uitwisseling en dit wordt crimineel uitgebuit (Tran, 2020; Naidoo, 2020; Monteith et al., 2021; Fontanilla, 2020). Dit geldt dus zowel voor werk als voor sociale aangelegenheden (Naidoo, 2020). Als gevolg van de *lockdown* zijn mensen massaal meer online actief. Potentiële slachtoffers worden kwetsbaarder voor cybercriminaliteit door online risicovol gedrag als *'(...) downloading games and music from unknown websites, using file-sharing programs, instant messaging, opening unknown email attachments, and clicking on pop-up messages increases cyberharassment'* (Hawdon, Parti & Dearden, 2020:548). Daarnaast maakt meer online zijn, potentiële slachtoffer sowieso zichtbaar voor gemotiveerde daders (Hawdon, Parti & Dearden, 2020; Fontanilla, 2020).

Duidelijk is dat de *lockdown* neveneffecten heeft op werkpatronen, mobiliteit, consumptiegedrag en sociale samenhang (Buil-Gil et al., 2021), maar ook op de economie en uiteenlopende routineactiviteiten (Collier et al., 2020), waaronder ook culturele aspecten van het dagelijks leven. (Horgan et al., 2021). De *lockdown* heeft kortweg effect op *'(...) the rhythms of people's daily routines as patterns of work, leisure and study have changed as a result of lockdown and social distancing.'* (Collier et al., 2020:1). En dat geldt niet alleen voor het indivdu, maar op maatschappelijke en zelfs internationale schaal: *'The pandemic is reshaping the routine activities of societies en masse, leading to changes in the ecology of risk and opportunity for cybercrime.'* (Horgan et al., 2021:1).

3.4.3 Een spade dieper: Integratief model ter verklaring van de toename van cybercriminaliteit

In de verklaring van de toename van cybercriminaliteit moet echter breder worden gekeken dan alleen naar de routine-activiteiten (Naidoo, 2020). Ook Lallie en collega's (2021) stellen dat de toegenomen gelegenheid voor cybercriminaliteit het effect is van ingrijpende sociale en economische veranderingen als gevolg van de *lockdown*. Maar de effecten van de *lockdown* laten ook zien dat cybercriminelen hun modus operandi in zeer korte tijd op de nieuwe maatschappelijke omstandigheden kunnen afstemmen. Cybercriminelen spelen bijvoorbeeld in op de actualiteit door nieuwe aanvallen af te stemmen op het gewijzigde beleid (Collier et al. 2020). En dat is kenmerkend voor de techniek van *social engineering*, die voortdurend inspeelt op de actualiteit, onzekerheden en zoekgedrag van mensen (Ahamad, 2020). Cybercriminelen benutten daarmee niet alleen de technische maar ook de sociale kwetsbaarheid van hun slachtoffers (Naidoo, 2020).

Online oplichters spelen in op de publieke angst en onzekerheid die er als gevolg van de coronapandemie is (Tran, 2020; Naidoo, 2020; Lallie et al., 2021; Fontanilla, 2020, Collier et al., 2020). De toegenomen stress, angst en bezorgdheid maken mensen kwetsbaar voor hun aanvallen (Lallie et al., 2021; Fontanilla, 2020). Cybercriminelen spelen – na uitvoerige analyse van 185 online oplichtingspogingen – volgens Naidoo (2020) in op de volgende situationele kenmerken van de coronapandemie: behoefte aan sociaal contact, de overgang naar thuiswerken, toenemende werkeloosheid, beschikbaarheid van steunfondsen, behoefte aan vermaak en ontspanning, en de opkomst van corona gerelateerde goede doelen. Cybercriminelen doen zich in hun e-mails vooral voor als sociale netwerkplatformen, banken, technologiebedrijven en overheden. Omdat cybercriminelen steeds meer, sneller en flexibeler gebruikmaken van de sociale context is het lastiger voor potentiële doelwitten om aan hun aanvallen te ontkomen.

Met deze bevindingen heeft Naidoo een theoretisch model opgesteld dat naast de routine-activiteiten ook nadrukkelijk de situationele factoren van de coronapandemie omvat. Cybercriminelen hebben tijdens de coronapandemie voortdurend hun modus operandi aangepast en blijken uiterst flexibel: ze proberen steeds nieuwe technieken voor sociale beïnvloeding uit. Daarom moet er meer aandacht zijn voor de actuele, sociale context van digitale oplichting dan in onderzoek op basis van de routine-activiteiten theorie vaak het geval is (Naidoo, 2020). Maar waar begin je in de aanpak van cybercriminaliteit?

3.4.4 Naar een lokale aanpak van gedigitaliseerde criminaliteit?

Het is volgens een aantal auteurs (Collier et al., 2020; Horgan et al., 2021; Leukfeldt, Spithoven & Misana – ter Huurne, 2020) een misvatting dat cybercriminaliteit als nationaal en internationaal probleem alleen op die niveau's kan worden aangepakt: '*Too much attention has been focused on the limits of the public police capacity to respond to cybercrime, and not enough attention paid to its strengths and potential to play a unique and complementary role in tackling cybercriminaliteit. Arguably, the skills and capacities of local police will be crucial in responding to cybercrime and ensuring cyber security for all.'* Collier et al., 2020: 14). Naast dat het internet allerlei internationale contexten met elkaar verbindt, doorkruist deze ook vooral lokale samenlevingen. Het is daarmee aannemelijk dat daders ook op nationale of zelfs lokale schaal actief zijn. Het gaat daarbij specifiek om lokaal gedeelde politiek, taal en cultuur waar daders op inspelen (Horgan et al., 2021). Dit geldt vooral voor delicten als pesten en lastigvallen maar ook voor stalking en fraude die een sterk lokale context kennen (Horgan et al., 2021).

De lokale politie en haar partners zijn volgens collega's Horgan (et al., 2021) en Collier (et al., 2020) nadrukkelijk aan zet in de preventie van lokaal slachtofferschap van cybercriminaliteit. Zij zijn volgens deze auteurs de aangewezen spelers in hun lokale interactie met potentiële slachtoffers en daders op basis van hun goede contacten en diepgaande lokale kennis van doelgroepen met risicocommunicatie die aansluit bij deze doelgroepen: *'(...) police services are uniquely well-placed to engage with these forms of crime due to their existing human infrastructure and skills, deep ties to local communities, and knowledge of local issues.'* (Collier et al., 2020: 12). Hierbij gaan deze auteurs echter voorbij aan de noodzaak van een veel bredere, preventieve strategie waarin naast de lokale politie ook gemeenten, provincies, banken, werkgevers, verzekeraars, internet service providers en het maatschappelijk middenveld een rol spelen (Spithoven, 2020).

Toch hebben Horgan (et al., 2021) en Collier (et al., 2020) een punt als het gaat over de kracht van bestaande, goede relaties die lokale politiemensen met de lokale samenleving hebben: *'This would allow local policing to capitalise on the existing relationships and insights long-developed in specific localities, link up awareness messaging with its target audience(s) in more direct ways, and enhance the legitimacy of both the messages and the public police as cybercrime responders'* (Horgan et al., 2021:15). Ook kunnen lokale partners het beste de lokale aangiftebereidheid van doelgroepen stimuleren (zie ook Leukfeldt, Spithoven & Misana – ter Huurne, 2020). De aandacht van de lokale politie zou uit moeten gaan naar het verzorgen van preventieve activiteiten gericht op potentiële slachtoffers en daders en het promoten van *'digital guardianship'*. Het is daarbij echter cruciaal dat duidelijk is waar de politie verantwoordelijk voor is en waarvoor haar partnerorganisaties aan de lat staan (Collier et al., 2020; Horgan et al., 2021). En dat overzicht is nog niet aanwezig.

In de Nederlandse situatie leggen Leukfeldt, Spithoven & Misana – ter Huurne (2020) in vergelijkbare zin de nadruk op lokale preventie door de gemeenten. Dit vanuit de focus van de Nederlandse politie op haar kerntaken en de preventieve rol die gemeenten op zich hebben genomen in het tegengaan van offline veelvoorkomende en *high impact* criminaliteit, in samenhang met hun lokale partners (Terpstra & Mein, 2010; Spithoven, 2020). Nederlandse gemeenten hebben de preventie van slachtofferschap van gedigitaliseerde criminaliteit inmiddels ook als beleidsprioriteit aangemerkt (Spithoven, 2020).

De focus van de lokale aanpak van gemeenten in samenspel met partners als de politie ligt volgens Leukfeldt, Spithoven en Misana-ter Huurne (2020) op de volgende onderdelen:

I. *Stimuleren* van inwoners en bedrijven in het verzorgingsgebied om aangifte te doen en melding van slachtofferschap van cybercriminaliteit te doen.
II. *Monitoren* van de lokale ontwikkelingen in slachtofferschap en daderschap.

III. *Voorlichten* van specifieke doelgroepen onder de inwoners en bedrijven over specifieke vormen van cybercriminaliteit op basis van bestaande, lokale relaties.
IV. *Aanjagen* van lokale, brede samenwerking met partijen om meer bewustwording en zelfbeschermend gedrag onder inwoners en ondernemers te stimuleren.
V. *Opsporen* van lokale daders en dadergroepen die zich bezighouden met relatief eenvoudige vormen van cybercriminaliteit.
VI. *Frustreren* van lokale daders en dadergroepen door hen te vervolgen en potentiële daders voor te lichten over de persoonlijke consequenties wanneer zij worden gepakt.

Daarbij ligt het accent voor de onderdelen één tot en met vier in de Nederlandse setting nadrukkelijk bij de gemeente en vult de politie daarbij waar mogelijk aan, maar voor de onderdelen vijf en zes is de lokale, gebiedsgebonden politie aan zet in samenwerking met andere (organisatie)onderdelen. Gedigitaliseerde criminaliteit zou op den duur geïntegreerd moeten worden in de lokale aanpak van criminaliteit door gebiedsgebonden politiemedewerkers (Horgan et al., 2021), zo is het idee. Merk op dat intussen ook niet-strafrechtelijke interventies worden toegepast, zoals het voeren van stopgesprekken en het verhalen van financiële schade op daders.

3.5 De noodzaak van lokale verkenningen van de digitale politietaak

Maar in de complexiteit van de lokale praktijk is dit lang niet zo evident. De verwachting is echter dat na corona cybercriminaliteit als prangend vraagstuk zal aanblijven: *'Even as lockdowns ease, it is reasonable to suspect that certain far-reaching socialorganisational and economic changes, for example to working patterns and online shopping, are likely to persist well into the future.'* (Horgan et al., 2021:8). Op basis van de ontwikkeling van de criminaliteitsstatistieken tussen de *lockdowns* is tevens de verwachting dat de klassieke offline criminaliteit na de coronapandemie weer terug zal komen, omdat de gelegenheid daartoe weer toe zal nemen maar dat cybercriminaliteit daarnaast zal aanblijven (Buil-Gil et al., 2020).

Daarom is het verstandig dat de lokale, gebiedsgebonden politie zich voorbereidt: *'As society changes, police need to adapt to these new patterns in both routine activities and crime.'* (Collier et al., 2020:10). In de volgende hoofdstukken sluiten we daarom aan op de praktijk van het politiedistrict IJsselland. Daar is immers recent een eerste stap gezet in de lokale aanpak van gedigitaliseerde criminaliteit. In het volgende hoofdstuk staat de deelvraag 'Wat is het leereffect van de gebiedsgebonden medewerkers van het district IJsselland in de aanpak van gedigitaliseerde criminaliteit?' centraal. Vervolgens wordt in hoofdstuk vijf het leereffect van het digitaal flexteam opgehaald en zullen we in hoofdstuk zes de knelpunten in de huidige, lokale aanpak van gedigitaliseerde criminaliteit in dit district verkennen.

4

Lokale good practice: Centerpons & Lucky


DELL

Hoofdstuk 4

Lokale good practice: Centerpons & Lucky

In hoofdstukken 4 en 5 staat het leereffect centraal van de inspanningen die in het politiedistrict IJsselland zijn geleverd om de *digitale uitdagingen* waar het voor staat, het hoofd te bieden. Allereerst wordt in paragraaf 4.1 een korte introductie gegeven op de ervaringen met het onderzoek Lucky/Centerpons[3] dat kan worden beschouwd als een *good practice* in de lokale aanpak van gedigitaliseerde criminaliteit. In paragraaf 4.2 wordt een chronologisch stappenplan gepresenteerd, waar andere politiedistricten en cybercrimeteams zich mogelijk in de toekomst door kunnen laten inspireren.

Het gaat bij Lucky/Centerpons (hierna kortweg: 'Lucky') om een grootschalig onderzoek naar fraude via WhatsApp. Bij dit onderzoek is door het cybercrimeteam Oost-Nederland en het Basisteam IJsselland-Zuid intensief samengewerkt. Er wordt in dit hoofdstuk een nauwkeurige beschrijving gegeven van de projectmatige aanpak die is gevolgd. Het ging daarbij om een relatief nieuw vraagstuk voor politie (en justitie). Deze beschrijving bevat een flink aantal praktische *succesfactoren* die uit de casus zijn gedestilleerd: twintig maar liefst. Deze worden doorlopend aangestipt, toegelicht en tevens, waar mogelijk, aangevuld met informatie over concrete stappen die politiedistricten kunnen zetten die een vergelijkbaar project willen uitvoeren. In onderstaande box zijn de succesfactoren (en voor andere politieteams wellicht aanbevelingen) in chronologische volgorde opgenomen om de lezer alvast te prikkelen.

1. Zorg voor samenwerking tussen basisteam en cybercrimeteam en/of de districtsrecherche (DR).
2. Laat cybercrimeteam of DR focussen op de zwaardere, bovenlokaal opererende verdachten; het basisteam op de lichtere, lokaal opererende verdachten.
3. Jaag samen de lokale prioriteitstelling aan (OM, teamleiding, stuurploeg en OCP).
4. Laat je niet demotiveren door gebrek aan routine en digitale vaardigheden.
5. Maak een projectplan; wie is voor welk deel van deze zaak verantwoordelijk, wie doet wat en wat heb je van elkaar nodig?
6. Zorg vroegtijdig voor betrokkenheid van het OM, incl. de 'cyber-experts' vanuit het parket.
7. Laat de projectmedewerkers zelf meedenken over hun bijdrage aan het project en voeg dat stapsgewijs samen tot een gedragen en doordachte projectaanpak.
8. Heb oog voor de individuele motivatie en eigen 'regelruimte' van medewerkers.
9. Bepaal samen de doelstelling van het project en benoem wat kan worden bijgedragen door de deelnemers aan de samenwerking. Benoem ook wat nog ontbreekt en waar het ontbrekende stukje kan worden verkregen.
10. Reageer op signalen vanuit 'de onderbuik': verricht gerichte analyse op aangiften en meldingen over gedigitaliseerde criminaliteit in een bepaald tijdsbestek.
11. Wees je bewust van de criminele organisatiestructuren die meestal gekoppeld zijn aan gedigitaliseerde criminaliteit.
12. Wees realistisch, bepaal nauwkeurig wat je in je project kan aanpakken en wat niet (je gaat meer vinden dan je aankan.

3 Het gaat in beide gevallen om interne werktitels. 'Lucky' is de betiteling van het deelonderzoek gericht op twee verdachten vanuit het cybercrimeteam Oost-Nederland; het hieraan gekoppelde onderzoek naar een groot aantal hieraan gekoppelde verdachten vanuit het Basisteam IJsseland-Zuid heet 'Centerpons'. In de rest van dit hoofdstuk wordt gemakshalve 'Lucky' aangehouden.

13. Ga improviserend te werk bij het vinden van capaciteit, maar zet collega's in op hun expertise.
14. Organiseer een gecoördineerde, gezamenlijke 'veegweek'.
15. Benut de specialistische kennis van het cybercrimeteam vooraf bij de instructie van o.a. basisteam collega's en als vraagbaak tijdens de veegweek.
16. Stem de planning en benodigde capaciteit in een vroegtijdig stadium met elkaar af. Zorg dat ook het OM de benodigde medewerkers heeft klaarstaan voor de veegweek.
17. Neem telefoons van de pinners en *'money mules'* in beslag en analyseer o.a. chatgesprekken.
18. Evalueer gezamenlijk het verloop en de uitkomsten van het project.
19. Onderlinge verbanden tussen aangiften laten rusten!
20. Na afloop: Horizontaal leren!

4.1 Leren van het onderzoek 'Lucky'

In navolgende wordt een beschrijving gegeven van een grootschalig opsporingsonderzoek dat het basisteam IJsselland-Zuid en het cybercrimeteam van de eenheid Oost-Nederland in samenwerking hebben gedraaid: het onderzoek 'Lucky'. 'Lucky' betreft een opsporingsonderzoek naar fraude die wordt gepleegd met behulp van WhatsApp, een onderzoek met tussen de 25 en 30 verdachten. In korte tijd (ongeveer twee weken) zijn deze verdachten aangehouden en verhoord. Ze hebben allemaal een individuele strafrechtelijke afdoening gehad, variërend van voorwaardelijk sepot tot een sanctie van de strafrechter. Het cybercrimeteam richtte zich hierbij voornamelijk op twee 'hoofdverdachten' die veel van de genoemde verdachten bleken aan te sturen; uiteindelijk concentreerde het onderzoek zich op 26 verdachten.

Met dit onderzoek zijn lokaal de nodige successen behaald in de gebiedsgebonden aanpak van gedigitaliseerde criminaliteit, welke ook in de media zijn opgepakt. Dat begon met de berichtgeving over de aanhouding van maar liefst 24 verdachten van *money muling* uit de omgeving van Deventer (RTV Oost, 2020). Aansluitend werd bericht over de celstraffen die aan twee oplichters zijn uitgedeeld (Klaassen, 2020; Broersma, 2020).

De eerste succesfactor die we kunnen identificeren betreft de samenwerking tussen het basisteam en een andere rechercheafdeling: *Zorg voor samenwerking tussen basisteam en het cybercrimeteam en/of de districtsrecherche* (1). Projectmatige samenwerking als deze geeft een basisteam de kans om te wennen aan de werkzaamheden die nodig zijn en deze na verloop van tijd op te nemen in het reguliere werkproces. Het is aan te bevelen bij meerdere projecten samen te werken met een ander meer ervaren onderdeel van de politie, om de benodigde kennis en routine een stevige basis te kunnen geven binnen bijvoorbeeld het basisteam. Ook aan meer creatieve mogelijkheden kan worden gedacht, zoals *hackatons* en coaching door cybervrijwilligers.

In het geval van 'Lucky' wijst het cybercrimeteam van de eenheid Oost-Nederland er nadrukkelijk op dat een districtsrecherche (DR) in vergelijkbare gevallen ook in staat is (of zou moeten zijn) om de benodigde werkzaamheden te verrichten. 'Lucky' zou bewust zijn opgepakt door het cybercrimeteam vanwege de relatieve onbekendheid met digitale fraude zaken bij de DR, in de hoop de zaak te laten fungeren als showcase en te laten zien wat er mogelijk is. Een tweede succesfactor tekent zich af: *Laat cybercrimeteam of DR focussen op de zwaardere, bovenlokaal opererende verdachten; het basisteam op de lichtere, lokaal opererende verdachten* (2). De bovenlokaal opererende verdachten hadden een leidende en coördinerende rol. De verdachten waarop het basisteam zich richtte waren vooral *'money mules'* en *'pinners'*, die een 'veiligheidsprobleem' vormden voor het basisteam IJsselland-Zuid. De toegenomen hoeveelheid aangiften van fraude was de directe aanleiding voor de samenwerking. Hierop wordt later nader ingegaan.

Het *tackelen* van actuele vraagstukken rond bijvoorbeeld gedigitaliseerde criminaliteit is niet simpelweg een kwestie van 'beter in iets worden'. Er zijn meer zaken dan politiemensen en OM'ers om eraan te werken. Ook hangt het succes van (bijvoorbeeld) een district in de (repressieve) aanpak van cybercriminaliteit onvermijdelijk samen met de prioriteit die eraan gegeven wordt. Daarbij is bewustzijn van de werkzame mechanismen van belang. In de uiteindelijke besluitvorming door het OM spelen signalen vanuit de politie en het openbaar bestuur een belangrijke rol. Maar uiteindelijk bepaalt de 'waan van de dag' vaak waar politiemedewerkers feitelijk voor worden ingezet; zaken die op een moment in de tijd belangrijker lijken dan alle andere. Ook draagt de informatiehuishouding van de politie die niet vanzelf zicht geeft op de omvang van gedigitaliseerde criminaliteit, eraan bij dat de betekenis en impact hiervan grotendeels onzichtbaar blijven.[4] Tegelijkertijd blijven gebrek aan routine en vaardigheden voortbestaan. De keuze prioriteit te geven aan gedigitaliseerde criminaliteit lijkt dan ook vooraf te moeten gaan aan alle andere te ondernemen stappen. Een cruciale succesfactor is volgens ons: *Jaag samen de lokale prioriteitstelling aan (OM, teamleiding, stuurploeg en OCP)*(3).

Een zekere veerkracht en flexibiliteit zijn in dit stadium hard nodig. Idealiter starten activiteiten op waar het probleem zich lijkt te concentreren of waar veel aangiften binnenkomen. Analyse van aangiften is een eerste stap en van daaruit kan evt. naar een passende taakverdeling worden gezocht. Het district van de pleegplaats of waar de hoofdverdachten wonen is normaalgesproken 'aan zet', maar bij de aanpak van gedigitaliseerde criminaliteit is stringent hanteren van al deze begrippen funest. Niet afschuiven, maar 'ontschotten' en samenwerken moet de norm worden, waarbij uitwisselen van informatie en analyses cruciaal is. Een losse aangifte is in de regel onderdeel van een reeks. Maar als de patronen niet worden onderzocht omdat geen enkel disrict 'de vingers wil branden' blijft de criminele organisatie die erachter zit onopgemerkt.

We doen de volgende succesfactor er maar gelijk achteraan: *Laat je niet demotiveren door gebrek aan routine en digitale vaardigheden* (4). In de praktijk blijkt aanwezigheid van digitale vaardigheden en kennis maar tot op zekere hoogte noodzakelijk om gedigitaliseerde criminaliteit te kunnen afhandelen. En de 'koudwatervrees' nam in het geval van 'Lucky' snel af. Opvallend is in het algemeen dat er systematisch werd samengewerkt in het geval van 'Lucky'. Een succesfactor: *Maak een projectplan; wie is voor welk deel van deze zaak verantwoordelijk, wie doet wat en wat heb je van elkaar nodig?* (5) De gehanteerde systematische werkwijze die we in dit hoofdstuk beschrijven werpt vruchten af. De nauwe betrokkenheid van het OM is hierbij een belangrijke succesfactor gebleken: *Zorg vroegtijdig voor betrokkenheid van het OM, incl. de 'cyber-experts' vanuit het parket* (6). Er is gezamenlijk toegewerkt naar een 'veegweek' waarbij behalve rechercheurs en medewerkers van het basisteam, ook analisten en informatiemedewerkers paraat stonden, evenals vanuit het OM gespecialiseerde medewerkers. (Verderop komt de 'veegweek' nader aan de orde.)

In grote lijnen zijn de volgende fasen herkenbaar in de samenwerking: *beeldvorming, oordeelsvorming, besluitvorming en uitvoering*. Daarbij valt vooral op dat de deelnemers aan de samenwerking zich ieder voor zich hebben afgevraagd hoe ze hieraan het beste konden bijdragen. Wat abstracter gezegd ontstond een iteratief proces waarbij de deelnemers de eigen kring en het samenwerkingsoverleg meerdere keren afwisselden om tot een sterker eindresultaat te komen. Daarbij was sprake van een sterke motivatie en van 'persoonlijk leiderschap'. We noteren meerdere succesfactoren: *Laat de projectmedewerkers zelf meedenken over hun bijdrage aan het project en voeg dat stapsgewijs samen tot een gedragen en doordachte projectaanpak* (7). *Heb oog voor de individuele motivatie en eigen 'regelruimte' van medewerkers* (8). *Bepaal samen de doelstelling van het project en benoem wat kan worden*

4 Helaas liggen veel zaken niet fysiek op de plank, maar zijn volledig aan het oog onttrokken. Daarbij is cybercriminaliteit vrijwel niet zichtbaar op straat. Sommige aangevers melden zich bij de politie als hun zaak niet wordt onderzocht, maar ook hun onvrede blijft grotendeels onopgemerkt.

bijgedragen door de deelnemers aan de samenwerking. Benoem ook wat nog ontbreekt en waar het ontbrekende stukje kan worden verkregen (9).

De doelstelling of m.a.w. de begrenzing van het uitgevoerde opsporingsonderzoek, is volgens alle betrokkenen bij gedigitaliseerde criminaliteit nog belangrijker dan anders. In overleg met het OM is de doelstelling van 'Lucky' bepaald. Om alle benodigde activiteiten te kunnen verrichten werd afgesproken strikt binnen de afgesproken kaders te blijven, en 'restinformatie' niet verder te onderzoeken maar te delen. Uiteindelijk is een gezamenlijk beeld gevormd van de opgave. Basisteam, cybercrimeteam en OM hebben aansluitend samen een oordeel gevormd over wat er nodig zou zijn voor de feitelijke aanpak en ieders aandeel daarin. Vervolgens is tot samenwerking besloten. Een aantal stappen wordt hieronder meer chronologisch gepresenteerd en toegelicht.

4.2 Het onderzoek 'Lucky' in chronologische stappen

Stap 1 – Samenwerking tot stand brengen tussen basisteam, cybercrimeteam en OM
Voor het succes van het district IJsselland bij het intensiveren van de aanpak van cybercriminaliteit lijkt de samenwerking met het cybercrimeteam en (gespecialiseerde functionarissen van) het OM cruciaal te zijn geweest. Het OM legde prioriteit bij zogeheten vriend-in-nood-fraudes (VIN-fraudes). Dit gaf een extra impuls aan de analyse van relevante aangiften. Er waren overigens al enige tijd signalen over een toename van gedigitaliseerde criminaliteit. Vervolgens wordt overleg opgestart met het cybercrimeteam van de eenheid Oost-Nederland dat de VIN-fraudes als landelijk aandachtsgebied heeft:

> *'Op het hoogtepunt had ik hier 20 aangiften van slachtofferschap van vriend-in-noodfraude per week, in dit district. Reken maar uit hoeveel aangiften er inmiddels zijn gedaan, met schadebedragen van bijvoorbeeld €10.000,-, de impact is zeer groot.' (Medewerker basisteam IJsselland-Zuid)*

Stap 2 – Analyse van aangiften en dossiers (beeldvorming)
Met de focus op VIN-fraudes ontstond uit gerichte analyse van (o.a.) aangiften vanaf oktober 2019 binnen drie maanden het beeld dat ook binnen het werkgebied van het district meerdere verdachten zaten:

> *'We hebben met elkaar geconstateerd dat VIN-fraudes echt een probleem worden waar we iets aan moeten doen. Toen ben ik die zaken gaan verzamelen.' (Medewerker basisteam IJsselland-Zuid)*

Er lijkt in de landelijke spreiding van verdachten in fraudezaken, sprake van een verdichting in Deventer, waarbij ronselaars, 'money mules' en 'pinners' vooral lokaal actief lijken te zijn. Maar de oplichters lijken zich buiten het werkgebied te bevinden en ook landelijk actief, met steun van diverse 'hulpstructuren'.[5]

Succesfactoren: *Reageer op signalen vanuit 'de onderbuik': verricht gerichte analyse op aangiften en meldingen over gedigitaliseerde criminaliteit in een bepaald tijdsbestek* (10) *en wees je bewust van de criminele organisatiestructuren die meestal gekoppeld zijn aan gedigitaliseerde criminaliteit* (11).

---

5 De analyse van gedigitaliseerde criminaliteit wordt bemoeilijkt door de weinig eenduidige registratie van dit soort zaken in de politiesystemen: *'Wij registreren delicten op maatschappelijke klassen. F127 is er eentje, overige horizontale fraude. Daar kan heel veel onder vallen. Maar er is ook een maatschappelijke klasse die heet cybercriminaliteit maar we hebben ook verticale fraude en identiteitsfraude en ga zo maar door.'* (Medewerker basisteam IJsselland-Zuid)

Stap 3 – Nader overleg tussen basisteam en cybercrimeteam (beeldvorming/oordeelsvorming)
Het OCP van het basisteam IJsselland-Zuid trad over de bevindingen in overleg met het cybercrimeteam. In dit overleg kwam de mogelijke relatie naar voren tussen de zaak die intern bekendstaat onder de codenaam 'Lucky', over enkele verdachten met een coördinerende rol die VIN-fraudes via WhatsApp beramen, en verdachten in IJsselland (Deventer). Het doel wordt bepaald: we ontwerpen een aanpak met een beperkte focus, zodat deze haalbaar is met de beschikbare capaciteit. Dus: *Wees realistisch, bepaal nauwkeurig wat je in je project kan aanpakken en wat niet, want je gaat meer vinden dan je aankan* (12).

Stap 4 – Basisteam verklaart zich bereid tot extra inzet (oordeelsvorming)
Veelal is nog onduidelijk hoe de taken verdeeld moeten worden als het gaat om de opsporing van gedigitaliseerde criminaliteit. Op het lokale niveau zijn ook nog maar weinig opsporingsspecialisten voorhanden op dit terrein. Als de vraag rijst waar de capaciteit gevonden kan worden om het opkomende probleem van digitale fraudes in het district aan te pakken, verklaart het basisteam IJsselland-Zuid zich onder voorwaarden bereid om capaciteit in te zetten. Vanuit het 'blauw', om verdachten aan te houden, inbeslagnames te doen en aanverwante logistieke en administratieve werkzaamheden te verrichten. Daarnaast wordt onder meer capaciteit toegezegd vanuit het 'ondermijningsteam', waarin twee rechercheurs van het basisteam en twee van de districtsrecherche zijn samengebracht. Ook het cybercrimeteam stelt capaciteit beschikbaar voor de samenwerking, en zal als onderdeel daarvan degenen die van oplichting worden verdacht in de zaak 'Lucky', verhoren:

> *'Vanuit het cybercrimeteam kwamen ze met een aantal zaken en zo kregen we overlap. Ik heb gezegd: "Alles wat wij doen is het horen van de money mules en de restinformatie delen we met jullie. En als we bij elkaar zitten krijgen we meer voor elkaar." Vervolgens hebben we een selectie van de verdachten gemaakt.' (Medewerker basisteam IJsselland-Zuid)*

Succesfactor: *Ga improviserend te werk bij het vinden van capaciteit, maar zet collega's in op hun expertise* (13). Te denken valt aan de volgende taakverdeling: Basisteam: aanhouden, in beslag nemen, verhoren, logistiek en administratie rondom bijv. 'pinners' en *'money mules'*. Recherche en cybercrimeteam: in kaart brengen van verdachten, coördineren, aanhouden, in beslag nemen, verhoren, logistiek en administratie verzorgen rondom bovenlokaal opererende verdachten.

Stap 5 – 'Veegweek' voorbereiden en bemensing organiseren (uitvoering)
Ondersteund door het cybercrimeteam gaat het 'ondermijningsteam' met de voorbereiding van een 'veegweek' aan de slag. Daarbij gaat het vooral om gegevens vorderen (o.a. bij banken) en verhoren voorbereiden. De gevorderde informatie is nodig om de verhoren voor te bereiden, waarbij het doel vooraf (in overleg met het OM) moet worden vastgesteld. Met het cybercrimeteam is afgesproken van zoveel mogelijk verdachten de telefoon in beslag te nemen om deze te kunnen uitlezen. Dit vooral met het oog op vervolgonderzoek (in 'Lucky' door het cybercrimeteam). De logistiek die hieraan gekoppeld is wordt meegenomen in de voorbereiding. Het concentreren van de werkzaamheden in de tijd vergemakkelijkt het beschikbaar kunnen krijgen van de verschillende benodigde specialisten.
In samenwerking met het cybercrimeteam wordt een planning gemaakt en een team samengesteld. Uiteindelijk worden twee weken geprikt om verdachten aan te houden en te verhoren. Daarvoor worden collega's vanuit het 'ondermijningsteam', het team veelvoorkomende criminaliteit (VVC) en het cybercrimeteam aan elkaar gekoppeld. Andere basisteammedewerkers verrichten de aanhoudingen en inbeslagnames. IJsselland zorgt achteraf dat de dossiers worden opgemaakt. De samenwerking met het cybercrimeteam wordt als een belangrijke meerwaarde beschouwd:

'Het cybercrimeteam was echt onze hulplijn. En de samenwerking met hen vond ik echt de meerwaarde van het hele onderzoek. Voor mij zijn er nu ook andere werkzaamheden op cybercriminaliteit gebied uit voortgekomen. Hier zat een onderzoek achter wat het interessanter maakte, en waar de informatie van onze 26 verdachten ook voor van belang was. Het draaien van een zaak op een katvanger, dat was op zichzelf allemaal niet zo interessant en ingewikkeld.' (Rechercheur 'ondermijningsteam')

'We hebben voor vaste verhoorkoppels gezorgd. We hadden een koppel vanuit het cybercrimeteam en 1 of 2 koppels uit Deventer. En we zorgden dat er altijd voor dat iemand van de intel aanwezig was en iemand van onze analyseafdeling. We lazen mee met de verhoren terwijl die afgenomen werden en we stonden ook via de chat in live verbinding met de verhoorders, zodat op het moment dat er bepaalde namen genoemd werden, we daarop konden inspelen. De verhoorders waren vooraf niet enorm op de hoogte. Op het moment dat wij aansloegen op zaken die voor ons relevant waren konden we daar vragen over stellen natuurlijk. Op het moment dat wij verbanden zagen tussen verschillende verhoren die al eerder waren afgelegd konden we daar ook input over geven. Intel medewerkers konden natuurlijk gelijk checken in het systeem wie daar misschien bij zouden horen en om aanvullende informatie vragen.' (Rechercheur cybercrimeteam)

Succesfactoren: *Organiseer een gecoördineerde, gezamenlijke 'veegweek' waarbij informatie wordt gevorderd, verhoren worden voorbereid en verdachten evt. worden aangehouden* (14). *En benut de specialistische kennis van het cybercrimeteam vooraf bij de instructie van o.a. basisteam collega's en als vraagbaak tijdens de veegweek* (15).

Stap 6 – Afstemmen met het OM (besluitvorming/uitvoering)

Er is tijdig geconstateerd dat het op grote schaal aanbrengen van een type zaak dat ook voor het OM (meestal wordt bedoeld: ZSM) relatief nieuw is, afstemming vergt. Het OM gaf daarbij de focus van de opsporingsactiviteiten aan, zorgde voor de benodigde medewerkers en voor een juridische toelichting op het benodigde bewijs. Tegelijkertijd is het gezamenlijke doel bepaald: een succesvol strafrechtelijk vervolg in de zaken van een groot aantal verdachten, maar geen uitputtend onderzoek. Het OM zorgde dat er een 'assistent-officier' beschikbaar was; een officier van justitie, gespecialiseerd in cybercriminaliteit was raadpleegbaar als vraagbaak[6]:

'Wij hadden heel erg afgestemd van tevoren binnen welke kaders we zouden blijven: we zouden het behapbaar houden en niet steeds nader onderzoek doen, maar gaan voor een bepaalde hoeveelheid informatie. We horen de verdachten, bijvoorbeeld over witwassen en willen ze daarvoor bij ZSM aanbieden. Maar omdat we best wel veel verdachten zouden aanleveren hadden we een assistent-officier tot onze beschikking, puur voor de zaken vanuit onze veegweek. En de cyberofficier stond klaar om vraagbaak te zijn voor de assistent-officier. Daardoor is het bij ons gewoon snel verlopen. Ik merkte later dat twee zaken die we later aanbrachten, alweer veel moeilijker lagen bij het OM. We hadden andere teams gevraagd om twee verdachten namens ons te horen, en die verhoren kwamen later binnen. Dan merk je dat het gelijk weer veel moeizamer gaat. Als je het onderzoek wilt doen, zoals wij dat gedaan hebben, dan moet je echt de afstemming zoeken.' (Rechercheur 'ondermijningsteam')

6 Ook hier is zichtbaar hoe de verschillende 'partners' in de samenwerking de eigen kring en het samenwerkingsoverleg afwisselden waar nodig. Steeds bepaalt elke partner in eigen kring wat er nodig is voor een sterker eindresultaat, om daar vervolgens binnen het project duidelijke afspraken over te maken. Ook andersom kan tussen de niveaus worden gewisseld: op projectniveau wordt vastgesteld wat er nodig is en vervolgens zorgen de 'partners' ieder voor zich dat de afspraken worden ingevuld.

Succesfactor: *Stem de planning en benodigde capaciteit in een vroegtijdig stadium met elkaar af. Zorg dat ook het OM de benodigde medewerkers heeft klaarstaan voor de veegweek* (16).

Stap 7 – 'Veegweek' uitvoeren: verdachten aanhouden en verhoren (uitvoering)
De doelstelling van de veegweek was tweeledig. Politie en justitie wilden een duidelijk signaal afgeven aan jongeren die zich schuldig hadden gemaakt aan onder meer 'witwassen'. Meestal door een bankrekening ter beschikking te stellen ten behoeve van oplichtingspraktijken of door het buitgemaakte geld voor de oplichter contant op te nemen bij een geldautomaat, was hiervan sprake. De hiervan verdachte jongeren werden allemaal aangehouden zonder dat dit strikt noodzakelijk was, om het onderzoek op zich ook al enigszins een normerende functie te geven (in dat geval een voorschot op evt. straf). Waar mogelijk werden telefoons in beslag genomen. De verhoren waren primair gericht op het delict 'witwassen' en waren daarnaast bedoeld om informatie te krijgen over de ronselaars en de modus operandi.

De tweede doelstelling was dan ook de ronselaars en (het netwerk van) de oplichters aan te kunnen pakken. Het Team Digitale Opsporing (TDO) in Zwolle stond klaar om een groot aantal telefoons uit te lezen. Iedere dag was er een medewerker uit Deventer 'die toch naar Zwolle moest' die de logistiek rond de telefoons kon verzorgen. De inbeslagnames zouden maximaal een week duren. De uitgelezen data (chatgesprekken bijvoorbeeld) zijn geanalyseerd en gebruikt door het cybercrimeteam, onder meer om informatie over de mogelijke oplichters te krijgen. In de strafdossiers werd de informatie uit de verhoren en de telefoons ook gecombineerd, soms om een verklaring van verdachte onderuit te halen.

Succesfactor: *Neem telefoons van de pinners en 'money mules' in beslag en analyseer o.a. chatgesprekken* (17).

Stap 8 – Strafrechtelijk vervolg geven (uitvoering)
In samenspraak met het OM werd er in veel gevallen voor gekozen toe te werken naar een omvangrijkere ten laste legging. Daarbij werden naast 'witwassen' zoals hiervoor besproken, ook andere aspecten meegenomen, waaronder 'computercriminaliteit' zoals dat strafbaar is gesteld in het WvS. Uiteindelijk heeft het OM er overigens veelal voor gekozen niet direct een strafrechtelijke sanctie op te leggen. In die gevallen is meestal besloten tot een voorwaardelijk sepot. Daarbij ging het met name om verdachten die hun bankrekening ter beschikking hadden gesteld. Anderen, die werden verdacht van het opnemen van buitgemaakt geld bij een geldautomaat, kregen (eerder) een transactievoorstel of een dagvaarding van de officier van justitie. Bij de geïnterviewde politiemensen leven wat verschillende beelden over de strafrechtelijke afdoening die op de veegweek is gevolgd. Volgens de één zijn de voorwaardelijke sepots passend bij de meeste verdachten (zonder 'strafrechtelijke documentatie'), de ander wijt deze sepots aan een gebrek aan capaciteit bij het OM. Tegelijkertijd, zo wordt genoemd tijdens de interviews, hebben ook banken een taak bij het tegengaan van fraude en kunnen verdachten ook in dit opzicht met (ingrijpende) maatregelen te maken krijgen, zoals het niet meer kunnen verkrijgen van een bankrekening.

Het blijkt dat er verschillend wordt gedacht over de strafrechtelijke uitkomsten van het onderzoek 'Lucky'. Het is van belang om mogelijke onvrede bij de deelnemers aan de samenwerking samen te bespreken en te gebruiken om van te leren.
Succesfactor: *Evalueer gezamenlijk het verloop en de uitkomsten van het project* (18). In april-mei 2020 werd duidelijk dat er voldoende bewijs voorhanden was om de onderzochte zaken een strafrechtelijk vervolg te kunnen geven.

Stap 9 – Onderlinge verbanden tussen aangiften laten rusten (uitvoering)
Afgesproken is vermoedens over relaties tussen zaken niet nader te onderzoeken, waarbij restinformatie werd doorgespeeld naar het landelijke informatieknooppunt. Zo zijn bankrekeningnummers die onderlinge relaties vertoonden zijn doorgespeeld. Echter niet duidelijk is wat er vervolgens mee is gebeurd.

En intussen zijn er alweer andere prioriteiten. Het verdient in de meeste gevallen de voorkeur lokale analyse van aangiften te laten rusten (zie ook succesfactor 12) en in plaats daarvan landelijke analyse hiervan in te richten.

> *'Je ziet dat er in een zaak meerdere plekken zijn waar het geld naartoe gaat. Zowel naar Groningen als naar Zeeland. Dat betekent dat er iemand coördineert die we nu niet zien. Ik denk dat dit een georganiseerd verband is. In de stijl waarmee ze oplichten zien we in meerdere zaken dezelfde specifieke tekst terugkomen. We zijn er niet aan toegekomen om dat uit te diepen, maar dat is voor ons al met het blote oog te zien. Ze beginnen consequent met een bepaalde tekst en een specifieke manier waarop ze die opschrijven, dus dat valt gewoon op. Maar om dat echt diepgaand uit te zoeken gaat hier de pet te boven. We moeten daarbij echt duidelijk grenzen stellen, want anders vreet het te veel capaciteit. Dan heb je een aantal bankrekeningnummers waar door heel het land veel geld op is overgemaakt (...) en geef ik aan het landelijk informatieknooppunt. Wat ermee is gebeurd, weten we niet. Er zijn een aantal zaken in mijn werk waarvan ik het belangrijk vindt dat er iets mee gebeurt, de rest laat ik los.' (Medewerker basisteam IJsselland-Zuid)*

Succesfactor: *Onderlinge verbanden tussen aangiften laten rusten* (19).

Stap 10 – Horizontaal leren

De hierboven beschreven inspanningen rondom het onderzoek 'Lucky' verdienen navolging, gezien de grote toename van gedigitaliseerde criminaliteit. Daarom is van belang dat dergelijke *good practices* worden verspreid: *horizontaal leren* is daarbij het doel. De toename is van zodanige omvang dat de politie op elk niveau een taak heeft om gedigitaliseerde criminaliteit te voorkomen en tegen te gaan. Een extra aanwijzing in deze richting is het feit dat volgens geïnterviewde politiemensen ook al langer bekende criminelen de omschakeling naar het wereldwijde web hebben gemaakt bij het plegen van misdaden. Kennis van de lokale situatie en van de digitale dimensie van criminaliteit zijn daarmee beide cruciaal geworden voor goed gebiedsgebonden politiewerk. De aanpak van gedigitaliseerde criminaliteit zal in het reguliere werkproces dan ook steeds belangrijker worden. Daarbij vormt de beschreven projectmatige aanpak een goede basis om medewerkers binnen politiedistricten in te werken in de thematiek. Communicatie, extern maar ook intern, is hierbij van groot belang.

Extern wil de politie vanzelfsprekend duidelijk maken hoe burgers en bedrijven kunnen voorkomen slachtoffer te worden van gedigitaliseerde criminaliteit, en dat daders door politie en justitie worden 'aangepakt'. Intern gaat het erom kennis en kunde, maar ook de motivatie om gedigitaliseerde criminaliteit aan te pakken te verhogen. Bij de interne communicatie daarover is van belang aandacht te besteden aan de vraag hoe benodigde kennis en ondersteuning te verkrijgen zijn. In het beschreven project bleek aan de externe communicatie meer aandacht te zijn besteed dan aan de interne, maar beide zijn belangrijk.

> *'Als je dit niet aanpakt wordt het echt onbeheersbaar. Wij kiezen er gewoon voor om er iets aan te gaan doen en aan de buitenwereld mee te geven dat we dat doen. In het wereldje zelf gaat het ook wel rond: "De politie doet niks met dit soort zaken". Maar we stonden wel mooi in de krant dat er 26 zaken naar justitie zijn gegaan en nu zijn er twee verdachten die 4,5 jaar krijgen. Dat komt wel uit onze koker en we laten zien: "Iemand oplichten moet je hier in Deventer niet doen."' (Medewerker basisteam IJsselland-Zuid)*

Succesfactor: *Horizontaal leren* (20).

5

Het leereffect van het digitaal flexteam

Hoofdstuk 5

Het leereffect van het digitaal flexteam

Binnen het district IJsselland is het *digitaal flexteam* al voor de coronacrisis ingezet op het tegengaan van gedigitaliseerde criminaliteit. Het lijkt, hoe bescheiden ook, een slimme en strategische keuze te zijn geweest die niets te vroeg kwam: de politie pakt een heel groot deel van de aangiften van gedigitaliseerde criminaliteit niet op, terwijl de criminaliteit zich op grote schaal van de straat naar het web lijkt te verplaatsen. Tijdens de coronacrisis heeft gedigitaliseerde criminaliteit zich een nog sterkere positie verworven. Daarmee is bijdragen aan de bestrijding hiervan een uiterst actueel thema voor alle niveaus binnen de politieorganisatie. Om deze reden wordt in deze paragraaf de opbrengst of het 'leereffect' van IJssellands' digitaal flexteam beschreven. Waar houdt het team zich mee bezig en waar loopt men tegenaan?

Circa twee jaar geleden heeft het politiedistrict IJsselland besloten het 'flexteam' in te zetten voor het aangaan van de digitale uitdagingen waar het district voor staat. De flexibel in te zetten capaciteit die standaard beschikbaar is voor elk district, en die meestal voor het vormen van 'heterdaadteams' wordt ingezet, is door IJsselland benut om relatief onbekend terrein te verkennen. Medewerkers die meer ervaring op wilden doen met 'digitale' werkzaamheden konden onderdeel worden van het digitaal flexteam. Hieronder wordt aandacht besteed aan de volgende thema's: in paragraaf 5.1 verkennen we de doelstelling en samenstelling van het digitaal flexteam; in paragraaf 5.2 de achtergrond en ontwikkeling van de medewerkers; in paragraaf 5.3 waar het digitaal flexteam tegenaan loopt en in paragraaf 5.4 behandelen we het 'grenswerk door het digitaal flexteam'.

5.1 Doelstelling en samenstelling van het digitaal flexteam

Uit gesprekken met enkele medewerkers blijkt dat het digitaal flexteam van IJsselland niet zo gauw een digitale uitdaging uit de weg gaat. Er wordt aan een brede doelstelling gewerkt: *het district 'digitaal vaardig' maken*. Zo wordt behalve op het versterken van de aanpak van gedigitaliseerde criminaliteit ook ingezet op het vergroten van de aanwezigheid van het district op sociale media en *webcare*. Dit laatste is onder meer gericht op de kwaliteit van de dienstverlening. Al met al is sprake van een nogal ambitieuze, mogelijk te ambitieuze taakstelling. Realistische verwachtingen zijn dan ook belangrijk om van het digitaal flexteam een succes te maken, beseft ook de Operationeel Expert van het team:

> *'Het ideaal is dat elke collega digitaal vaardiger is geworden als wij worden geëvalueerd. Maar dat is een utopie. Je zit met verschillen tussen medewerkers. Onze collega's zijn niet op digitale vaardigheden geselecteerd. Uiteindelijk moeten we een aantal specialisten overhouden die andere collega's verder kunnen helpen.'*

Over de invoering van taakaccenthouders *social media* en/of cybercriminaliteit voor de basisteams worden gesprekken gevoerd. Ook hier valt ons op dat er vooralsnog geen keuzes worden gemaakt. Intussen worden medewerkers van het district ondersteund en geïnstrueerd door het digitaal flexteam en geeft het bekendheid aan digitale thema's. Na een korte oriëntatiefase zijn meerdere concrete initiatieven van de grond gekomen. Er zijn uiteenlopende activiteiten die bij de 'doelstelling' passen. Zo houdt het digitaal flexteam zich behalve met (ondersteuning bij) de afhandeling van zaken met een digitale component ook bezig met diverse andere taken, zoals het trainen van basisteams in het gebruik van sociale media, het maken van een instructiefilm voor OCP's om duidelijk te maken hoe ze trends kunnen signaleren en het samenstellen van een 'handleiding' voor het opnemen van aangiften van cybercriminaliteit. Op basis van een top 4 van meest voorkomende typen zaken zijn standaard vragensets gemaakt

die aan aangevers kunnen worden gestuurd. De bedoeling hiervan is aangevers alle relevante 'digitale' informatie te laten aanleveren die relevant kan zijn voor de opsporing. Tevens is er aandacht voor de interne communicatie over het digitaal flexteam. Bewustwording van de digitale dimensie van het (basis)politiewerk en het verspreiden van kennis zijn daarbij de belangrijkste speerpunten.

Het digitaal flexteam wordt aangestuurd door een Operationeel Expert en bestaat voornamelijk uit basisteammedewerkers, van wie sommigen bij Intake & Service werkzaam zijn. Voor een deel van hun tijd zijn ze inzetbaar voor het digitaal flexteam. De meeste beschikken niet over opmerkelijke digitale vaardigheden of opleiding. Ook valt op dat slechts weinigen beschikken over ruime ervaring in de opsporing. Er zitten ten tijde van dit onderzoek (vrijwel) geen rechercheurs in het digitaal flexteam. Terwijl ervaring in de opsporing wel behulpzaam is bij een deel van de taken van dit team. Daarover later meer.

Hoewel men op een tamelijk brede taakstelling is uitgekomen voor het digitaal flexteam, is wel sprake van een inhoudelijke focus waar het gaat om de afhandeling van zaken. In eerste instantie richtte het team zich voornamelijk op vriend-in-nood-fraude, overeenkomstig de focus van het cybercrimeteam van Eenheid Oost-Nederland. Toch is de vraag of in het algemeen een duidelijkere focus op gedigitaliseerde criminaliteit meer zou opleveren, met een daarbij passende gerichte inzet van ervaren medewerkers, middelen en opleiding.

5.2 Achtergrond en ontwikkeling van de medewerkers

Een groot deel van de collega's in het district IJsselland zou nog behoorlijk terughoudend omgaan met de steeds belangrijker wordende digitale component van hun werk. Zo voelt een groot deel van de basisteammedewerkers zich volgens de mensen van het digitaal flexteam nog niet opgewassen tegen het werken aan zak van gedigitaliseerde criminaliteit. Ook het incorporeren van het gebruik van *social media* in het dagelijkse politiewerk stuit nog op weerstand. Hoewel sommige informatie wel te vinden is, binnen bijvoorbeeld *politiekennisnet* en *e-learnings*, maakt lang niet iedereen daar gebruik van. Tegelijkertijd blijkt de beschikbaarheid van opleidingen en uitgewerkte handleidingen binnen de politie nog beperkt. Deze combinatie van factoren is het digitaal flexteam een doorn in het oog. De leden van het flexteam zijn dan ook graag bereid nieuwe kennis en vaardigheden op te doen, om die vervolgens aan collega's te kunnen doorgeven. Sommigen menen in de praktijk al de rol van *taakaccenthouder* te vervullen, die in hun ogen een vaste plek verdient in elk basisteam.

De redenen die de leden van het flexteam hadden om daarin van start te willen gaan, blijken tamelijk uiteenlopend. Wat hierbij opvalt is dat affiniteit, veel meer dan voorkennis of opleiding doorslaggevend is. Ook worden sommige medewerkers van het digitaal flexteam simpelweg gemotiveerd door het grote belang van de digitale opgave voor de politie. Zo geven meerdere medewerkers aan de hoge prioriteit die wordt gegeven aan het afhandelen van winkeldiefstallen en overlastmeldingen niet te kunnen onderschrijven. In hun ogen is het niet passend meer dat de basisteams en ZSM hier veel tijd in stoppen, terwijl tegelijkertijd aangiften van gedigitaliseerde criminaliteit 'op de plank blijven liggen'. Via onder meer Marktplaats-oplichting en vriend-in-nood-fraude worden slachtoffers op grote schaal 'binnen een paar minuten opgelicht voor duizenden Euro's', zoals één van de medewerkers het verwoordde. Ook zijn er flexteam-leden die affiniteit met de opsporing hebben en daarin graag verder willen. Anderen voelen zich geroepen om voor het digitaal flexteam te gaan werken vanwege affiniteit met *social media*, 'techniek' en ICT. Professionele betrokkenheid en verantwoordelijkheidsgevoel spelen ook een rol, zoals bij een medewerker Intake & Service die zag dat nog onvoldoende werd ingespeeld op aangiften met een digitale component. Er was in haar ogen afstemming nodig, evenals bijscholing van collega's: reden genoeg voor haar om zich hiervoor in te zetten binnen het digitaal flexteam. Ten tijde van dit onderzoek had de bijscholing al concreet vorm gekregen: er was een handboek gemaakt en de betreffende collega's werden via instructievideo's en speciale bijeenkomsten bijgeschoold door het digitaal flexteam.

Voor de leden van het digitaal flexteam wordt geprobeerd een passende opleiding samen te stellen. Veelal verkrijgt het digitaal flexteam kennis via gespecialiseerde onderdelen, vooral het cybercrime-team op eenheidsniveau en het (landelijk georganiseerde) Team Digitale Opsporing (TDO). Die fungeren als 'hulplijnen'; de mensen van het digitaal flexteam kunnen erop terugvallen. Ook wordt een zogeheten OSINT-opleiding gevolgd, onder meer gericht op het gebruiken van (voornamelijk) openbare bronnen, zodanig dat er geen herleidbare digitale sporen op het internet worden achtergelaten door de politie. Het doel is ook hier weer om de opgedane kennis door te geven aan bijvoorbeeld wijkagenten. Overigens kunnen politiemensen niet of nauwelijks steunen op digitale kennis vanuit de politie-opleiding, die tot ontsteltenis van de mensen van het digitaal flexteam nog steeds weinig zou inspelen op de opkomst van cybercriminaliteit. Naast de genoemde kennisbronnen is men dan ook afhankelijk van 'werkend leren'. De pioniers van het flexteam die wij gesproken hebben zijn nieuwsgierig en gaan zelf op zoek naar informatie: *'Als ik bijvoorbeeld niet weet wat spoofing is, zoek ik daar een filmpje over op YouTube.'* Ook worden nieuwe dingen gewoon uitgeprobeerd: *'Ik heb een telefoon gekregen met een alias erop en daarmee kunnen wij op verschillende social media kanalen en op darkweb. Daar ga ik binnenkort gewoon eens in duiken. Ik weet nog niet of we daar zaken van kunnen maken, maar ik ga het monitoren.'* Onduidelijk is of het hier gaat om ongeoorloofde 'fake accounts'.

Nog onduidelijk is in hoeverre de expertise van de flexteam medewerkers (en van andere medewerkers van de basisteams) zich kan ontwikkelen. Het flexteam beperkt zich vooralsnog tot de simpelere zaken: *'de geldezel, de Tikkie-fraude, laag in de criminele organisatie.'* Daarbij bestaat nog de mogelijkheid om meer met de basisteams samen onderzoeken uit te gaan voeren:

> *'Bijvoorbeeld: In een wat groter onderzoek komen we erachter dat er twintig rekeningen zijn. Al die twintig eigenaren moeten gehoord worden als verdachte. Dat moet dan door de basisteams gebeuren. Vervolgens wordt het allemaal weer bij ons neergelegd om te analyseren wat er uit die informatie komt. Dan kunnen we weer een stapje verder. Dat zou misschien kunnen gebeuren door de basisteams: we zijn een stap verder, kunnen jullie nog wat getuigen horen of een verdachte horen? En uiteindelijk zal je vanuit het flexteam zelf een aantal verdachten moeten gaan horen. Als het te specifiek wordt, dan is het gewoon niet meer haalbaar om dat door de basisteams te laten doen. (...) Wat allemaal haalbaar is zal de praktijk moeten uitwijzen. Op de eenvoudige handelingen zal je stappenplannen moeten maken, zoals ze er ook zijn over hoe ik een PV moet opmaken bij een blaastest.' (Medewerker digitaal flexteam)*

Er kan aan zaken worden gewerkt zonder dat kennis van alle 'technische details' nodig is, zo blijkt:

> *'Hoe je gegevens veiligstelt en hoe dingen digitaal allemaal in elkaar zitten weet je een beetje. Het is meer algemene kennis die van belang is over de feiten die ze plegen, vooral tijdens verhoren, en die kennis heb ik wel. We hebben digitale specialisten binnen de politie en die hebben hun eigen taak.'*

Van belang is hierbij op te merken dat de medewerkers van het flexteam een bijzondere positie hebben: zij krijgen de gelegenheid zich enigszins te specialiseren. Voorlopig zijn de basisteams in het algemeen nog minder ver. Een medewerker van het flexteam schetst wat in zijn ogen haalbaar zou moeten zijn voor een basisteam, op termijn (waar het gaat om vriend-in-nood-fraudes):

'Het is een lastig te zeggen wat er op termijn kan op basisteamniveau. Omdat wij hier nu ruimte en tijd voor krijgen. Ook krijgen we een opleiding. Maar een deel van de zaken zou zeker door de basisteams gedraaid kunnen worden. Maar heb je echt expertise nodig en ga je grote onderzoeken draaien, dan zou ik een specialisme aanraden. Willen ze de hele organisatie blootleggen en afhandelen, dan denk ik eerder aan een specialistisch team, want dan ga je over de grenzen van de eenheid. Dan kom je in Amsterdam of Den Haag bijvoorbeeld en dan heb je wellicht het cyberteam wel nodig, want die hebben daar veel beter contact mee. Maar een whatsapp-fraude, tot op zekere hoogte durf ik wel te zeggen dat ik die zaak kan draaien op het basisteam. Dan pakken we de loopjongens en misschien degene die daarboven zit. Wil je daarna kijken naar de verbinding met de initiator en de rest van het netwerk, dan zal verdachte's telefoon uitgelezen moeten worden of moeten gegevens gevorderd. Ook dan zit je wel al meer richting een specialistisch team te denken. Je hebt ook al snel analisten nodig die we bij het basisteam niet hebben.'

Al met al lijkt nog wat onduidelijk te zijn waarop het digitaal flexteam zich uiteindelijk dient voor te bereiden. Een stip aan de horizon ontbreekt: de taakstelling en de bezetting van het digitaal flexteam zijn nog tamelijk breed en niet helder. Waarom geen ervaren rechercheurs aan boord? Welke rol gaat de districtsrecherche spelen en hoe verhoudt zich dat tot de rol van het digitaal flexteam? Wat wordt de focus in de toekomst? Hoe ziet de 'digitale' werkvoorraad er precies uit en wat is de taakverdeling tussen de verschillende districtelijke onderdelen? Welk resultaat moet behaald? Waar dienen capaciteit, opleiding en investeringen uiteindelijk op te worden gericht? Opmerkelijk in dat verband is dat de rol van het flexteam bij het in het vorige hoofdstuk beschreven project slechts 'zijdelings' is geweest, opnieuw een indicatie dat de koers nog niet helder is uitgezet waar het gaat om de digitale opgave in het district.

5.3 Waar loopt het digitaal flexteam tegenaan?

De vraag waar het digitaal flexteam in haar korte bestaan zoal 'tegenaan is gelopen', is nogal breed. We streven dan ook niet naar volledigheid maar zullen hier (in willekeurige volgorde) een aantal zaken aandacht geven die de moeite waard kunnen zijn, bijvoorbeeld voor andere districten met een vergelijkbare opgave en/of bij de eventuele doorontwikkeling van het digitaal flexteam binnen het district IJsselland. Vanzelfsprekend komen hieronder nogal uiteenlopende zaken kort aan de orde:

- Over de *webcare*-diensten bestond de nodige ontevredenheid binnen de basisteams. Met die onvrede is snel iets gedaan door het digitaal flexteam. De *webcare*, ofwel de externe communicatie en dienstverlening via online kanalen, werd door veel uitvoerende politiemensen binnen het district niet ervaren als *core business*. De werkzaamheden hadden in hun ogen te weinig relatie met de eigen hoofdtaken. Uiteindelijk is gekozen de *webcare* over te dragen aan het Regionaal Service Centre (RSC). Zo kwam capaciteit vrij en ook lijkt *online politiewerk* hierdoor wat gemakkelijker 'aan de man' te brengen binnen de basisteams, doordat een 'digitale frustratie' is weggenomen.

- Het digitaal flexteam wilde snel in kaart hebben wat de opgave is als het gaat om aangiften van cybercriminaliteit: hoeveel komen er daarvan binnen en hoeveel worden er afgehandeld? Het bleek lastig om die vraag te (laten) beantwoorden. De oorzaak daarvan ligt in de niet-eenduidige registratie: er werd onder meerdere 'maatschappelijke klassen' gerubriceerd, waardoor relevante zaken niet snel te verzamelen waren. Een aangifte kon bijvoorbeeld onder 'computervredebreuk' of 'cybercriminaliteit' worden geregistreerd, maar ook onder 'horizontale fraude', waar ook fraudezaken zonder digitale component onder gevat kunnen worden. Goed overzicht krijgen vergt dan ook veel analyse- en leeswerk. Door het digitaal flexteam is initiatief genomen hierin verbetering aan te brengen. Er is een handleiding gemaakt die onder meer duidelijk maakt onder welke maatschappelijke klassen aangiften met bepaalde kenmerken geregistreerd dienen te worden.

De bedoeling is de registratie overeenkomstig de werkwijze van de cybercrimeteams te laten verlopen.

- De teamleden zijn nog volop in ontwikkeling, maar hebben wel al enkele zaken opgepakt. Daarbij is een aantal knelpunten naar voren gekomen. Onder meer de parttime inzetbaarheid van medewerkers van het flexteam en hun nog beperkte ervaring in de opsporing leverden problemen op. Zo blijkt de combinatie wijkagent en digitaal flexteam in het concrete opsporingswerk belemmeringen op te leveren. Om een zaak van begin tot eind goed te kunnen volbrengen, is een tamelijk complexe planning nodig, waaraan ook vastgehouden moet worden. Om evt. toezeggingen richting de aangever na te kunnen komen, maar ook omdat bijvoorbeeld gevorderd beeldmateriaal van banken slechts enkele weken beschikbaar blijft. Ook moeten weleens meerdere keren 'vorderingen' worden gedaan, hetgeen een flinke uitdaging oplevert. De planning en het schriftelijke werk dat hieraan vastzit blijkt, zeker zonder opgebouwde routine, problemen op te leveren. Als daarin iets misloopt kan dat bijvoorbeeld tot gevolg hebben dat een verhoor dat al door de recherche is ingepland, niet door kan gaan. Slechts zelden kan men binnen een paar dagen over gevorderde informatie of bijvoorbeeld camerabeelden beschikken.

- De bedoeling van het digitaal flexteam is om zich uiteindelijk te richten op het geven van ondersteuning aan de basisteams en de districtsrecherche, bij 'digitale' zaken. Het is nog niet duidelijk welke typen zaken door het basisteam, de districtsrecherche en door het cybercrimeteam opgepakt dienen te worden. Ook lijkt nog onduidelijk wat de rol van het digitaal flexteam daarbij precies zou moeten worden:

  'We willen alles met gedigitaliseerde criminaliteit ondersteunen. Je kunt dat breed zien: uitlezen telefoons, BOB-aanvragen doen, verdachtenverhoor voorbereiden, verdachten horen, werkmap klaarmaken, dossier maken. We zijn zeer actief en houden de handen niet op de rug.' (Operationeel Expert digitaal flexteam)

- Het flexteam ziet dat de politie op het lokale niveau tegen de geografisch gebonden verantwoordelijkheden aan loopt. 'De verdachte komt niet altijd uit de stad waar het feit is gepleegd', stelt een medewerker van het flexteam vast: 'Als je naar de aanpak van cybercriminaliteit kijkt, kom je erachter dat de politie in Nederland een heleboel eilandjes heeft gecreëerd.' In zaken waarin verdachte(n) elders woonachtig zijn, wordt in de regel weinig geïnvesteerd, omdat zeer de vraag is of de zaak met succes is over te dragen aan een ander team elders in het land. In het verlengde hiervan ligt de constatering dat leidinggevenden terughoudend zijn aan zaken van gedigitaliseerde criminaliteit te beginnen, omdat verdachten veelal aan een groot aantal aangiften/zaken zijn te koppelen. Het onderzoek naar die verdachte wordt dan als te omvangrijk ingeschat t.o.v. de beschikbare capaciteit in het team. De kans dat er ook elders geen prioriteit aan kan worden gegeven is groot, is meestal de verwachting: 'Je hoort er vaak niks meer van.' En zo blijft het erbij (de 'veegweek' uit het vorige hoofdstuk uitgezonderd):

  'Als je de rekening opvraagt heb je al een verdachte en een woonplaats en je kunt vervolgens wellicht beelden en telefoongegevens opvragen, maar dat is weer extra werk en dat doet men dan in de regel niet. En niemand krijgt een keer carte blanche van zijn chef van: nou ga je die zaak maar draaien ook al kost het capaciteit. Dat hebben ze in Deventer wel één keer gedaan. Dat is die zaak met die 26 verdachten. Daar bereik je ook het nieuws mee, het werd groot uitgepakt. Ik heb het idee dat dat vaker kan.' (Medewerker digitaal flexteam)

- De relatief beperkte prioriteit die aan de aanpak van gedigitaliseerde criminaliteit wordt gegeven, ook binnen het district IJsselland, kan niet door het digitaal flexteam worden gecompenseerd. Op de *mismatch* tussen aanbod van zaken en (de voor dit thema) beschikbare capaciteit is nog geen

antwoord gevonden. Ook is nog geen sprake van een uitgewerkte aanpak van gedigitaliseerde criminaliteit binnen het district IJsselland. Zo is bijvoorbeeld duidelijk geworden dat er in het district veel *money mules* zitten (zie vorig hoofdstuk), maar is de opsporing in dergelijke zaken nog geen dagelijks werk. Ook is er nog geen concreet voornemen om die groep op een alternatieve wijze 'aan te pakken'. Er wordt wel over gesproken, maar men is er ten tijde van dit onderzoek nog niet toe overgegaan gecoördineerd 'stopgesprekken' met van *moneymuling* verdachte personen te voeren. Ook is nog niet duidelijk of wijkagenten of anderen deze gesprekken dan zouden moeten voeren.

- Alle betrokkenen geven aan dat er nog winst te behalen is door simpelweg meer prioriteit te geven aan de aanpak van *gedigitaliseerde criminaliteit*. Het thema krijgt volgens het flexteam langzamerhand meer prioriteit van het OM. Ook ervaart men binnen de politie meer bewustzijn van de grote toename van gedigitaliseerde criminaliteit. De oprichting van het digitaal flexteam is hiervan een mooi voorbeeld, maar men vindt de prioriteitstelling nog onvoldoende aansluiten bij de opgave die er is. Niet alleen kan meer recht worden gedaan aan de grote impact die een deel van de zaken heeft op slachtoffers, ook moet er nog veel meer ervaring mee worden opgedaan.

- Het digitaal flexteam ziet veelvuldig dat collega's nog maar weinig zicht hebben op de genoemde impact en op het verschijnsel van *gedigitaliseerde criminaliteit*. Tegelijkertijd is sprake van negatieve beeldvorming rondom dit thema. Onterecht lijkt de gedachte bij veel collega's te leven dat zaken met een digitale component door hen onmogelijk opgepakt kunnen worden. Terwijl de complexiteit van een belangrijk deel van de zaken van gedigitaliseerde criminaliteit beperkt is.

- De vraag is of een voldoende groot aandeel van de zaken onderzoekbaar blijft. Wanneer verdachten niet met hun naam of andere herleidbare kenmerken gekoppeld kunnen worden aan bijvoorbeeld gebruikte servers en telefoonnummers, dan wordt de opsporing erg lastig op basisteamniveau en ook voor de huidige bezetting van het flexteam:

  'Een aantal dingen kan ik wel zelf. Een website of een IP-adres herleiden. Als je die door het systeem heengooit kun je achterhalen door welke server dat ding gehost wordt. Dan ben je weer een stapje verder en dat is misschien net genoeg om weer een beginnetje te hebben aan een onderzoek.' (Medewerker digitaal flexteam)

- Er is technische ondersteuning (bijvoorbeeld bij uitlezen van telefoons en computers) en ook ondersteuning bij kennisvragen lijkt ruim voorhanden, o.a. vanuit het cybercrimeteam en het Team Digitale Opsporing (TDO). De ervaren collega's van deze afdelingen raden ook regelmatig af om verder onderzoek te doen in bepaalde complexe situaties. Dat is mooi, en tegelijkertijd roept het vragen op over de toegevoegde waarde van het digitaal flexteam.

- De ontwikkelingen gaan in hoog tempo. Hoewel het digitaal flexteam flinke inspanningen levert om zelfstandig de opsporing van gedigitaliseerde criminaliteit op te kunnen pakken, is intussen door het cybercrimeteam van de eenheid Oost-Nederland initiatief genomen een deel daarvan te coördineren. Daarbij gaat het om de zogeheten *vriend-in-nood-fraudes* (VIN-fraudes). Het flexteam heeft hieraan ook medewerking toegezegd. Ten tijde van dit onderzoek is de inzet dat er landelijk overzicht wordt gecreëerd, waarbij onderzoek wordt gedaan naar een aantal verdachten. Het cybercrimeteam zorgt dat beschikbare informatie wordt gebundeld en geanalyseerd en dat de benodigde informatie wordt gevorderd bij derden, om te voorkomen dat dubbel werk wordt gedaan. (Niet zelden worden door verschillende onderdelen van de politie gegevens gevorderd over dezelfde verdachten.) Vervolgens zullen de 'pakketjes' met informatie naar (onder meer) de basisteams worden gestuurd. Het flexteam is enthousiast en wil graag ondersteunen:

'Als er bijvoorbeeld voldoende informatie voorhanden is om een verdachte aan te houden en te verhoren, dan is dat een klus die prima bij de basisteams past. Die zitten op korte afstand en kunnen daar tussendoor veel in doen. Een standaard voorblad opmaken bij een zaak, ik denk dat zulke dingen prima passen bij een basisteam.' (Medewerker flexteam)

- Het verkrijgen van de benodigde middelen en opleidingen is een knelpunt voor het team. Zelfs laptops bleken moeilijk te verkrijgen voor het nieuwe team.

- Er is behoefte aan meer werkafspraken en een vaste officier of contactpersoon bij het OM. Hierin is ten tijde van dit onderzoek nog niet voorzien.

- Hoewel een deel van het flexteam graag bereid is om voorlichting te geven over de gevaren van cybercriminaliteit, leeft binnen het team ook de gedachte om preventie vooral aan andere (landelijke) partijen over te laten. Het flexteam komt hier niet veel aan toe. Er wordt steeds meer bekendheid aan de genoemde risico's gegeven, en dat gebeurt toch het meest effectief op landelijk niveau via de massamedia, zo wordt ook geconstateerd. Daarbij is men van opvatting dat ook commerciële partijen zoals banken, een belangrijke rol te vervullen hebben om criminaliteit te helpen voorkomen en consumenten over risico's voor te lichten.

5.4 Grenswerk door het digitaal flexteam

Nog niet duidelijk is of de aanpak van het digitaal flexteam blijft en hoe zittende politiemensen in IJsselland zich in de toekomst op de digitale politietaak zullen voorbereiden. Duidelijk is wel dat de aanpak van gedigitaliseerde criminaliteit en de benodigde digitale professionalisering in het algemeen nog aandacht vragen op lokaal niveau. Betrokkenen geven nadrukkelijk aan dat er meer prioriteit aan gegeven moet worden. Daarnaast is ondersteuning nodig met opleidingen, faciliteiten en de invoering van nieuwe functies (bv. taakaccenthouders). Ook is bij dit voor de politie relatief nieuwe werkveld *gedigitaliseerde criminaliteit* nog veelvuldig de vraag hoe de verantwoordelijkheden verdeeld zijn en zouden moeten worden.

Nog vaak is onduidelijk waar de grens van de eigen verantwoordelijkheid ligt en die van een ander politieonderdeel begint, vandaar boven deze slotparagraaf het kopje: *grenswerk*. Vooralsnog lijkt het verstandig om de onduidelijkheid onder ogen te zien en dik gemarkeerde grenzen op de kaart te vermijden, maar: Hoe moeten de grenslijnen eruit komen te zien? En hoe moet in dit verband tegen de veelal bovenlokale aard van gedigitaliseerde criminaliteit worden aangekeken? Welk aandeel van het werk behoort een politiedistrict op zich te kunnen nemen?

Het zijn vragen die nog regelmatig voor verkramping lijken te zorgen binnen de politie. In het volgende hoofdstuk wordt hierop nader ingegaan. Deze paragraaf over het digitaal flexteam van het district IJsselland willen we graag afsluiten met een positieve constatering. Het team toont aan dat binnen de politieorganisatie (wel degelijk) veel potentie aanwezig is om de nieuwe digitale uitdagingen aan te gaan, ook lokaal. Daarbij is het team graag bereid nieuwe vormen van samenwerking aan te gaan, om de veelal bovenlokale aard van gedigitaliseerde criminaliteit het hoofd te kunnen bieden. Ook daarover meer in het volgende hoofdstuk waarin we ons richten op de knelpunten in de huidige lokale aanpak van gedigitaliseerde criminaliteit van het district IJsselland.

6

Knelpunten: informatievoorziening, samenwerken & opleiden


POLITIE

Hoofdstuk 6

Knelpunten: informatievoorziening, samenwerken & opleiden

In dit onderzoek staan de algehele leerervaringen centraal van het politiedistrict IJsselland dat bezig is zich aan te passen op de digitale politietaak. In dit stadium gebeurt dit nog enigszins op de tast. Er is dan ook nog alle gelegenheid om op de opgedane leerervaringen te reflecteren en na te denken over de vraag wat de politie op het lokale niveau van basisteams en districten nodig heeft om de nieuwe digitale taak in de toekomst beter aan te kunnen.

In dit hoofdstuk worden enkele belangrijke (dreigende) knelpunten in de huidige aanpak van gedigitaliseerde criminaliteit van het district IJsselland belicht, waarop onze reflectie in het volgende en laatste hoofdstuk grotendeels gebaseerd zal zijn. Daarbij worden in dit hoofdstuk de belangrijkste (dreigende) knelpunten verder uitgewerkt, deels op basis van bevindingen die al in voorgaande hoofdstukken zijn beschreven. In paragraaf 6.1 wordt op belangrijke vragen omtrent informatievoorziening ingegaan. In paragraaf 6.2 worden enkele samenwerkingsverbanden opgesomd die het lokale niveau helpen bij het kunnen vervullen van de nieuwe digitale politietaak. Tot slot gaat paragraaf 6.3 in op knelpunten ten aanzien va het ontwikkelen van digitale kennis en vaardigheden, op de mate waarin dat nodig is en op de vraag hoe die kennis beter beschikbaar gemaakt kan worden: een cruciale randvoorwaarde om een *realistische*, lokale digitale ambitie te kunnen vaststellen.

6.1 Informatievoorziening

Bij het relatief nieuwe aandachtsgebied *gedigitaliseerde criminaliteit* komen in de uitvoering diverse vraagstukken naar voren die aan informatievoorziening zijn gerelateerd. In deze paragraaf willen we hier meer zicht op krijgen: Waar loopt men in het district IJsselland tegenaan en hoe kunnen problemen worden opgelost? De volgende vragen komen hierbij aan bod: Welke knelpunten komen naar voren bij de analyse van informatie? Hoe dient bij gevallen van gedigitaliseerde criminaliteit het aangifteproces te verlopen en hoe kan dit verbeterd worden? Hoe zit het met het ‘eigenaarschap’ van informatie? Gezien de (zeer) beperkte omvang van dit onderzoek verwachten we geen complete beschrijving te geven: ons doel is slechts een eerste indruk te geven van de huidige stand van zaken, voornamelijk vanuit het perspectief van het politiedistrict IJsselland.

6.1.1 Analyse

In het vorige hoofdstuk werd beschreven hoe het digitaal flexteam aanliep tegen de weinig eenduidige registratie van gedigitaliseerde criminaliteit. Gebleken is dat dezelfde typen aangiften onder meerdere ‘maatschappelijke klassen’ gerubriceerd worden, waardoor relevante zaken niet snel te verzamelen zijn. Zo kan een aangifte onder ‘computervredebreuk’ of ‘cybercriminaliteit’ worden geregistreerd, maar er zijn nog meer categorieën waar zaken met een digitale component onder vervat kunnen worden. Verder is het van belang bijvoorbeeld telefoonnummers en bankrekeningnummers op de juiste wijze in te voeren. Door de hele politieorganisatie heen een eenduidige registratiewijze volgen is volgens alle betrokkenen cruciaal om de informatie die beschikbaar is goed terug te kunnen vinden en gebruiken.

Een nieuw BVH-systeem is in voorbereiding dat de ervaren knelpunten (deels) kan oplossen. Binnen het district IJsselland is alvast initiatief genomen om de invoer te uniformeren (zie ook volgende kopje ‘aangifte opnemen’). Deze verbeterslag is volgens betrokkenen binnen het digitaal flexteam nodig om aangiften van cybercriminaliteit en relevante politie-informatie optimaal doorzoekbaar te maken

en gemakkelijk aan elkaar te kunnen koppelen. Van een uniforme werkwijze binnen de politie, waarbij medewerkers heldere instructies krijgen over invoeren en zoeken van politie informatie, lijkt rondom gedigitaliseerde criminaliteit geen sprake. Een landelijke analyse van de verschillende relevante soorten gegevens (over gedigitaliseerde criminaliteit) en de gewenste daarop aansluitende invoerroutines kan winst opleveren. Ten tijde van het onderzoek worden door het cybercrimeteam Oost-Nederland pragmatische noodgrepen gebruikt, zoals het draaien van geautomatiseerde *queries* door beschikbare aangiften om vormen van gedigitaliseerde criminaliteit in beeld te krijgen en kansrijke zaken uit te filteren. Op uitvoerend niveau is men van opvatting dat met het oog op de benodigde aanpak van gedigitaliseerde criminaliteit, op een grootschalige aanpassing van de informatiehuishouding van de politie niet langer kan worden gewacht.

Hieronder wordt beschreven hoe het aangifteproces binnen het district IJsselland tegen het licht is gehouden. Ook hiermee kan een bijdrage worden geleverd aan het verbeteren van de informatie-voorziening rond gedigitaliseerde criminaliteit.

6.1.2 Aangiften opnemen

De start van veel opsporingswerk wordt gevormd door de aangifte. Alle betrokkenen in dit onderzoek lijken doordrongen van het feit dat de kwaliteit van de aangifte in belangrijke mate de efficiëntie en effectiviteit van het opsporingswerk bepaalt. Als informatie hier niet wordt verzameld of niet goed wordt geregistreerd, kan dat grote invloed hebben op het vervolg, onder meer aangezien (digitale) informatie niet altijd traceerbaar blijft bij de aangever. Ook heeft een aangifte waarin gegevens ontbreken een lagere kans om opgepakt te worden, doordat er minder aanknopingspunten zijn voor onderzoek. Tevens is de kans lager dat een aangifte met succes wordt gekoppeld aan een ander (lopend) onderzoek, wanneer bepaalde gegevens ontbreken. Uit de interviews komt een aantal aspecten naar voren die bij gedigitaliseerde criminaliteit (extra) van belang blijken te zijn.

Binnen het district IJsselland werd het opnemen van aangiften van gedigitaliseerde criminaliteit en de kwaliteit daarvan een aandachtspunt onder druk van de grote toename hiervan tijdens de corona-crisis. Het effect van de (eerste) *lockdown* werd lokaal al na twee weken zichtbaar. Het digitaal flexteam maakte werk van het inventariseren van de knelpunten en van de instructie van collega's binnen de basisteams die aangiften opnemen. Een medewerker Intake & Service, tevens lid van het digitaal flexteam:

> *'Wij hebben ons laten inplannen op alle basisteams voor een soort bijspijkermoment. Op dat moment laten wij aan de hand van een filmpje zien hoe er gestandaardiseerd gewerkt kan worden met ons handboek. We hebben natuurlijk alles digitaal maar ze krijgen het ook persoonlijk mee in een boekje, zodat ze het ook meteen gaan toepassen. We hebben afgesproken met de teamchefs dat ze daar ook flink bovenop gaan zitten, dat dit ook gebeurt.'*

Voorafgaand is een handboek voor het opnemen van aangiften gemaakt gericht op een Top 4 van de meest voorkomende 'digitale criminaliteitsvormen'. Dit handboek wordt intussen ook al buiten het district IJsselland toegepast. Intake & Service collega's is gevraagd naar knelpunten. Daar kwam uit dat men niet goed wist welke specifieke vragen er gesteld moeten worden bij aangiften van cybercriminaliteit en dat men graag bijgeschoold zou willen worden op 'digitaal gebied'. Deze inspanningen moeten ertoe leiden dat in voorkomende gevallen volgens een stappenplan wordt gevraagd naar de standaard benodigde informatie bij zaken met een digitale component: telefoonnummers, e-mail adressen, bankrekeningnummers, etc.

Ook is het besparen van tijd van de betreffende medewerkers in de basispolitiezorg en bij Intake & Service een doelstelling, vanwege de recentelijk toegenomen hoeveelheid aangiften. Door met een

gestandaardiseerde (internet)aangifte te werken kan het aangifteproces efficiënter verlopen en wordt er door elke medewerker van Intake & Service naar de juiste informatie gevraagd. Daarbij wordt de aangever gevraagd een deel van de vragen aan te vullen met digitale gegevens. Vervolgens wordt de aangeleverde informatie op een gestandaardiseerde wijze verwerkt, zodat deze goed wordt geregistreerd.

Mede onder invloed van de coronamaatregelen werd deze manier van werken erg belangrijk. De medewerkers van Intake & Service zagen een grote, mogelijk blijvende verandering in hun werkwijze optreden: in veel zaken bleek het contact met aangevers op afstand tot tevredenheid te kunnen verlopen (ook internetaangifte doen op het bureau is mogelijk). De drempel voor verhoor op afstand en voor digitaal of telefonisch aangifte doen, is al met al verlaagd zo wordt gemeend. Al werd tijdens de interviews ook aangetekend dat de (ervaren) impact bij criminaliteitsslachtoffers, ook bij gevallen van gedigitaliseerde criminaliteit, een belangrijk aandachtspunt moet (kunnen) blijven. Ook werd opgemerkt dat de inrichting van het aangifteproces kan worden beschouwd als een uitdrukking van de prioriteit die gedigitaliseerde criminaliteit krijgt. Mogelijk kunnen basisteams een bijdrage leveren aan effectieve opsporing door sneller op meldingen te reageren, en in de toekomst vaker onmiddellijk na de telefonische melding ter plaatse (digitaal) aangifte op te nemen. Een medewerker van het cybercrime-team van de Eenheid Oost-Nederland:

> *'Er wordt regelmatig flink wat geld buit gemaakt. Je ziet ook een flinke impact op slacht-offers. We doen er alleen niks mee, want wat gebeurt er? Zo'n slachtoffer belt de politie en die moet vervolgens nog drie dagen wachten met aangifte doen. Waarom zouden we niet een auto daarheen sturen en ter plaatse de aangifte opstellen en de juiste gegevens veiligstellen zodat je meteen aan de slag kunt? Tuurlijk, ik snap dat we weinig capaciteit hebben maar het is wel interessant om het te onderzoeken en te ontdekken, wat zo'n werkwijze kan opleveren.'*

Gezien de grote verwevenheid van zaken van gedigitaliseerde criminaliteit, werd er door deze rechercheur ook voor gepleit bij de aangifte al te checken of gegevens daaruit ook elders in lopend onderzoek voorkomen. Hetgeen tegelijkertijd een pleidooi inhoudt voor het opvoeren van het aantal functionarissen binnen de politie dat zaken aan elkaar kan koppelen met behulp van BlueView – om de opsporing effectiever te maken en dubbel werk te voorkomen; bijvoorbeeld het veelvuldig vorderen van dezelfde banktransactiegegevens:

> *'We zijn nog te vaak met dezelfde dingen bezig. Er komt bijvoorbeeld een rekeningnummer naar voren in de aangifte. BlueView zou gewoon beschikbaar moeten zijn voor welk team dan ook binnen politie Nederland. Zodat als ze een rekeningnummer hebben, ze dat in Rotterdam kunnen invoeren en kunnen zien: daarmee is mogelijk al een vordering gedaan in Maastricht. Dan kun je meevaren op de vordering die Maastricht heeft gedaan, dat scheelt weer een vordering. Dat is al iets kleins waar ze mee aan de slag kunnen gaan, bij de basis-teams die aangiften opnemen.'*

6.1.3 Afbakening

Uit de gevoerde gesprekken binnen het district IJsselland en met het cybercrimeteam Oost-Nederland komt helder naar voren dat er belemmeringen zijn voor het aanpakken van zaken van gedigitaliseerde criminaliteit door basisteams en districtsrecherche. Vermoedelijk spelen een kennisachterstand en onbekendheid met de impact van zaken van gedigitaliseerde criminaliteit daar een rol bij. Ook de formele prioriteitstelling vanuit het OM is van invloed (geweest) (zie voorgaande hoofdstukken). Echter ook in de mate waarin zaken van gedigitaliseerde criminaliteit aansluiten bij de manier waarop werkzaamheden lokaal worden afgebakend schuilt een belemmering. Passend bij de lokale prioriteiten worden keuzes gemaakt over de inzet van de beschikbare capaciteit. Op het lokale niveau blijkt het lastig om te beginnen aan digitale zaken of daar prioriteit aan te geven, op het moment dat er keuzes gemaakt moeten worden.

Allereerst lijkt de hoeveelheid aangiften van gedigitaliseerde criminaliteit, ten tijde van dit onderzoek tamelijk overweldigend. Zo is (landelijk) sprake van een zeer groot aantal aangiften van digitale fraude en tegelijkertijd van een grote hoeveelheid niet-geanalyseerde, onoverzichtelijke informatie. Dit leidt ertoe dat er verlegenheid ontstaat bij het aanpakken van deze relatief nieuwe stroom. De hoeveelheid zaken met een digitale component is dermate groot dat de discussie over welk politieonderdeel zich daarmee het beste zou kunnen bezighouden onder grote druk staat. Begrijpelijkerwijs leidt dit eerder tot defensieve reacties dan tot initiatief van onderop. Veelgehoord is de reactie: *'We hebben onze handen al vol aan de high impact crimes'* waarbij onder meer geweld een belangrijke rol speelt.

Zoals eerder vermeld speelt het feit dat cybercriminaliteit niet 'gebiedsgebonden' is, eveneens een belangrijke rol. Wanneer een slachtoffer aangifte doet in district X dan lijkt de kans dat de dader zich daar ook bevindt veel kleiner dan bij veel andere, meer klassieke vormen van criminaliteit. Waar aangiften binnenkomen, zegt bij gedigitaliseerde criminaliteit betrekkelijk weinig. Ook dit is een belangrijke factor die ervoor zorgt dat bij de afbakening van werkzaamheden gedigitaliseerde criminaliteit gemakkelijk afvalt. Een aangifte oppakken betekent een relatief grote kans op het moeten overdragen van de zaak, omdat de verdachte die in beeld komt veelal buiten het eigen werkgebied woont. Volgens geïnterviewde politiemensen is de kans groot dat overgedragen zaken, alsnog terzijde worden gelegd wegens capaciteitsgebrek; het ontvangende team heeft vaak al zijn eigen prioriteiten zo blijkt in de praktijk. Een medewerker van het cybercrimeteam Oost-Nederland reageert als volgt op het ineffectieve rondschuiven met zaken: *'Eigenlijk zou je er naartoe moeten dat het basisteam waar het slachtoffer woonachtig is, verantwoordelijk is en blijft voor de zaak.'* In zijn visie ontbreekt een mechanisme om de schaal van veiligheidsproblemen lokaal inzichtelijk te maken.

De politie is in belangrijke mate geografisch georganiseerd en dit lijkt een nadelig effect te hebben bij de reactie van de politie op gedigitaliseerde criminaliteit. Hierbij speelt ook de onderlinge verwevenheid van zaken van gedigitaliseerde criminaliteit een rol. Met behulp van digitale hulpmiddelen kunnen op grote schaal slachtoffers worden gemaakt, verspreid over het land en zelfs over de hele wereld. In tegenstelling tot bijvoorbeeld een mishandeling in het uitgaansleven of zelfs een oplichtingszaak in de 'offline wereld', is een zaak van gedigitaliseerde criminaliteit (juist als het om een relatief eenvoudige zaken gaat) veelal gerelateerd aan een groot aantal andere gepleegde feiten en ook aangiften. Het maakt beslissers op lokaal niveau terughoudend te kiezen voor het oppakken van zaken van gedigitaliseerde criminaliteit, voor zover de formele prioriteitsstelling (sterk gericht op de klassieke *high impact crimes*) daar al de ruimte voor biedt.

Gebiedsgebonden politiewerk heeft echter wel degelijk een rol in het tegengaan van gedigitaliseerde criminaliteit. Zoals eerder vermeld signaleren basisteams ook weleens dat min of meer 'bekende criminelen' gebruik zijn gaan maken van digitale hulpmiddelen of zijn overgeschakeld naar gedigitaliseerde vormen van criminaliteit. De wijkagent en andere politiemensen met een lokale informatiepositie zullen hierop in moeten (leren) spelen. Daarbij ligt voor de hand dat politiemensen ook lokaal in staat gesteld moeten worden kennis en vaardigheden op peil te brengen en ervaring op te doen met de afhandeling van zaken van gedigitaliseerde criminaliteit. Duidelijk is dat de overschakeling van de straat naar het web plaatsvindt, maar in welk tempo is op basis van dit onderzoek niet aan te geven. Wat ons betreft is dit een belangrijke vraag die nadere analyse dan wel onderzoek verdient.

In de volgende paragraaf wordt ingegaan op beproefde en mogelijk nog te ontwikkelen vormen van samenwerking die basisteams en districtsrecherche met elkaar en vooral met andere onderdelen van de politie aan kunnen gaan. Hiermee lijken antwoorden gevonden te kunnen worden gevonden op een aantal van de knelpunten die hier zijn besproken.

6.2 Samenwerking bij de aanpak van gedigitaliseerde criminaliteit

Gezien de aard van gedigitaliseerde criminaliteit lijkt samenwerking, ook intern, cruciaal. In deze paragraaf zullen we deze stelling onderbouwen aan de hand van de praktijken die tot op heden zijn 'ontwikkeld' en die we hebben kunnen signaleren in dit onderzoek (6.3.1). Het gaat hierbij om eenvoudige vormen van samenwerking en het zoeken van 'hulplijnen', maar ook om meer complexe en in onze ogen zelfs bijzondere vormen van samenwerking. In 6.3.2 wordt ingegaan op vormen van samenwerking die nog verder versterkt kunnen worden.

6.2.1 Beproefde samenwerkingsvormen

De politieorganisatie dient vanzelfsprekend een bonte verzameling van verschillende kennisdomeinen 'in huis' te hebben; forensisch, financieel, digitaal, om enkele voorbeelden te noemen. Daarbij kunnen specialistische teams vanzelfsprekend een partje van de werkvoorraad voor hun rekening nemen, maar specialisten kunnen ook ondersteuning bieden aan andere onderdelen. Deze 'hulplijn'-constructie speelt in de aanpak van gedigitaliseerde criminaliteit (voorlopig) een enorm belangrijke rol; *learning by doing* wordt zo een reële optie. Tijdens ons onderzoek kwamen we diverse voorbeelden tegen, waarvan de belangrijkste hieronder kort worden genoemd. Daaronder ook belangrijke externe relaties:

- Het OM beschikt over specialisten die de politie kunnen helpen inzicht te verkrijgen in benodigde stappen in opsporingsonderzoeken, juist waar nog weinig kennis aanwezig is over een bepaald type zaak. Zo beschikt het OM over een 'cyberofficier' die bijvoorbeeld met een basisteam bespreekt wat er nodig is voor een succesvol strafrechtelijk vervolg van een 'marktplaatsfraude';
- Ook ZSM vervult een ondersteunende rol bij het ontwikkelen van een aanpak in zaken van gedigitaliseerde criminaliteit. Zo zou een standaard werkwijze zijn ontwikkeld voor *money mules*, die landelijk beschikbaar is gesteld;
- Het cybercrimeteam van de eenheid Oost-Nederland is op diverse manieren beschikbaar voor de basisteams en de districtsrecherche als samenwerkingspartner (zie hoofdstuk 4) en als 'hulplijn'. Zo is ondersteuning gegeven aan medewerkers Intake & Service bij het opnemen van aangiften (*'Daar hebben we ontzettend van geleerd'*). De ervaring binnen het cybercrimeteam is dat basisteams met ondersteuning goede resultaten kunnen boeken, mits de 'discussie over het vrijmaken van capaciteit' goed is verlopen. Overigens zijn nog wel grote verschillen zichtbaar in motivatie en kennis van de basisteams die door het cybercrimeteam worden ondersteund;
- Een belangrijke 'hulplijn' is ook het Team Digitale Opsporing. Hier kunnen medewerkers van de basisteams en de districtsrecherche terecht voor concrete ondersteuning (ook ter plaatse) en met uiteenlopende vragen. Zo wordt genoemd dat het TDO 'wat dieper kan graven in telefoons en computers', maar er is ook juridische (ervarings)kennis aanwezig bij het TDO. Die brede oriëntatie wordt op prijs gesteld: *'Er kan met ze gespard worden.'* Zo wordt ook soms afgeraden bepaalde zaken of onderzoekshandelingen lokaal op te pakken;
- Opvallend is de nog beperkte inzet op preventie, maar ook de nog beperkte samenwerking tussen het district IJsselland en de (lokale) overheid. Volgens meerdere betrokkenen is hier nog meer aandacht voor nodig.

In de basisteams zelf valt op dat nog niet is voorzien in een structurele inbedding van de 'hulplijn'-constructie; het inzetten van *taakaccenthouders digitaal* lijkt daarbij een voor de hand liggende optie. Zoals in voorgaand hoofdstuk is geconstateerd vervullen de leden van het digitaal flexteam momenteel al min of meer deze rol binnen het district IJsselland, maar die is vooralsnog van tijdelijke aard en veel geïnterviewde politiemensen steunen de gedachte van invoering van een taakaccenthouder.

6.2.2 Samenwerking verder versterken

Intussen is meermalen benoemd hoezeer gedigitaliseerde criminaliteit in zijn aard vertakt is, waarbij

criminele netwerken die op dit terrein actief zijn regelmatig een grote geografische spreiding hebben. Om te zorgen dat cybercriminaliteit toch kan worden opgepakt op het districtelijke niveau zijn er al diverse stappen gezet om tot een effectievere aanpak te komen, vaak via samenwerking. Tot besluit van deze paragraaf worden hier de door het cybercrimeteam Oost-Nederland (deels nog te nemen en uit te breiden) stappen beschreven in de versterking van de samenwerking binnen de politie.

Waar het gaat om het specifieke aandachtsgebied van dit team (als gevolg van een landelijke onderverdeling van aandachtsgebieden), de vriend- in-nood-fraudes, is ten tijde van dit onderzoek een nieuwe, veelbelovende werkwijze opgestart om in te spelen op een aantal specifieke kenmerken van gedigitaliseerde criminaliteit en op de (nog beperkte) spankracht in de districten om aan de aanpak hiervan bij te dragen. Allereerst heeft het team initiatief genomen (uitsluitend gestandaardiseerde, digitale) aangiften te verzamelen en analyseren. Daarbij worden verbanden gelegd en bundels van zaken gevormd. Ten behoeve van deze zaken worden gegevens gevorderd bij derden, o.a. op basis van verkregen bankrekeningnummers. Vervolgens worden verschillende aangiften gebundeld, als blijkt dat er overeenkomsten zijn die mogelijk in de richting van dezelfde verdachte wijzen. De ontwikkelde aanpak stelt het cybercrimeteam in staat om de gebundelde aangiften als 'werkpakket' bij de districten uit te zetten waar de verdachten woonachtig zijn. Daarbij kan het cybercrimeteam de criminele netwerken overzien en coördinerend opereren bij het oprollen van de netwerkstructuren, evt. in samenwerking met meerdere politiedistricten. Deze werkwijze op basis van bijzondere opsporingsbevoegdheden (Titel V van het Wetboek van Strafvordering) is na verloop van tijd stopgezet door het OM. Er zou onvoldoende sprake zijn geweest van onderzoek naar ernstige misdrijven in georganiseerd verband. Voor de politie betekent dit dat er, in overleg met het OM, gezocht moet worden naar een alternatief. Praktisch gezien gaat het erom in een vroegtijdig stadium verschillende 'kleine zaken' aan elkaar te koppelen, gebruik te maken van de bevoegdheden die hierbij passen (wellicht cf. Titel IV Sv) en toch mogelijkheden te vinden om gebundeld gegevens te vorderen, bijvoorbeeld waar hetzelfde telefoonnummer in verschillende aangiften voorkomt. Van het OM vergt dit medewerking en aanpassing van het werkproces en mogelijk van ICT-systemen, aangezien volgens één van de geïnterviewde politiemensen *'geautomatiseerd parketnummers aangemaakt moeten worden'*. De gewenste werkwijze vraagt volgens de geïnterviewden om herinterpretatie van juridische kaders en/of om herinrichting van (digitale) werkprocessen. Waarbij van het OM een actieve, oplossingsgerichte houding wordt verwacht.

Het lijkt nuttig om de monitoring van de ontwikkeling van gedigitaliseerde criminaliteit, op basis van een aangescherpte registratiediscipline of door extractie van ontwikkelingen uit bestaande cijfers, landelijk vorm te geven. Daarnaast lijkt het de gespreksdeelnemers nuttig om het opsporingsonderzoek bij gedigitaliseerde criminaliteit landelijk te coördineren, gezien de aard ervan en de (nog) beperkte spankracht op districtelijk niveau om landelijk opererende criminele netwerken aan te pakken. Met de beschreven werkwijze wordt voorkomen dat politiemensen binnen de districten op basis van onvolledige of juist dezelfde informatie, veelvuldig dezelfde gegevens vorderen bij derden. Tegelijkertijd wordt het rondschuiven met zaken door het land op deze manier voorkomen. Aan het einde van de looptijd van dit onderzoek kwam naar voren dat het OM de goedkeuring aan de hier beschreven wijze van grootschalige vordering van gegevens introk. Hierover meer in het volgende hoofdstuk.

Overigens zijn er nog wel (technische) verbeterpunten. Ten tijde van dit onderzoek is er nog geen duidelijkheid over de taakverdeling tussen districtsrecherches en basisteams. Daarbij lijkt ook de prioriteitstelling nog een rol te spelen, evenals soms een gebrek aan kennis en routine. Meer technisch: men kan bij het vorderen van informatie over telefoonnummers (nog) geen geautomatiseerde werkwijze volgen. De procedures bij het verkrijgen van gegevens over bankrekeningnummers zouden nog niet bij alle partijen zijn geautomatiseerd. Ook vormt de informatiehuishouding binnen de politie een belemmering voor de beschreven aanpak: het cybercrimeteam heeft meerdere *work-arounds* ontwikkeld, onder meer om de benodigde informatie te kunnen analyseren en om te voorkomen dat aangevers geautomatiseerd het bericht ontvangen dat de aangifte terzijde wordt gelegd, terwijl die juist

in de ‘werkpakketten’ wordt betrokken.

6.3 Versterken van digitale kennis en vaardigheden

Het werkterrein van politiemensen is voortdurend in verandering. De aanpassing op maatschappelijke trends en ontwikkelingen in de criminaliteit vragen dan ook constant om aandacht, op alle niveaus van de politieorganisatie, en tevens van bestuurders en politiek. In deze paragraaf wordt kort ingegaan op het versterken van digitale kennis en vaardigheden op districtelijk niveau. In hoeverre is dat nodig? Wat zijn de ervaringen hiermee tot dusverre, en wat lijkt er nodig in de nabije toekomst? Ons uitgangspunt is dat elk niveau in de politieorganisatie een bijdrage zal moeten leveren aan de invulling van de digitale politietaak. Een belangrijk deel van ons leven speelt zich tegenwoordig *online* af. Dat betekent voor politiemensen dat ze daarop afgestemd moeten raken en ook invulling moeten gaan geven aan de behoeften die burgers hebben aan online dienstverlening. In dit onderzoek ligt de focus primair bij gedigitaliseerde criminaliteit, die enorm in opkomst is. Echter, ook waar het hierom gaat is nog niet glashelder op welke typen werkzaamheden basisteams en districtsrecherche zich dienen te prepareren. Toch proberen we in deze paragraaf enkele inzichten te geven over het versterken van digitale kennis en vaardigheden, gericht op het tegengaan van gedigitaliseerde criminaliteit.

6.3.1 Lokale initiatieven

Allereerst valt op dat geïnterviewde functionarissen de kennis onder collega’s over (de opsporing) van gedigitaliseerde criminaliteit laag inschatten. Zo wordt regelmatig genoemd dat men weinig kennis heeft over opsporingsmogelijkheden. Praktische, technische en juridische kennis laat nog te wensen over. In de tweede plaats lijkt er gebrek aan effectieve coördinatie te zijn op het prepareren van politiemensen op de digitale politietaak. Zo is nog weinig sprake van een systematische kennisoverdacht en training van politiemensen binnen het district, maar ook in de politieopleiding is er volgens de direct betrokkenen in IJsselland nog maar nauwelijks aandacht voor cyber: een effectief landelijk ‘masterplan’ ontbreekt ten tijde van dit onderzoek (al is een landelijk initiatief wel in voorbereiding, zie par 7.3.4). Het digitaal flexteam zag dan ook diverse mogelijkheden om deze leegte op te vullen. Er is (positief geformuleerd) veel ruimte voor lokaal initiatief, maar kennisontwikkeling heeft daardoor nog geen structureel karakter, het gaat eerder om ad hoc *on-the-job-learing* (voor degenen die de stap durven zetten), korte cursussen en een themadag van het cyber- en flexteam. Een ander voorbeeld is dat er een handleiding is gemaakt door het digitaal flexteam, bedoeld om (voornamelijk) de medewerkers van Intake & Service te helpen bij het opnemen van aangiften met een digitale component (zie ook het vorige hoofdstuk).

6.3.2 Lokale behoefte aan kennis

Zoals eerdere hoofdstukken duidelijk maakten wordt in de praktijk zichtbaar hoe ondanks specialistische teams, het cybercrimeteam op eenheidsniveau en het team hightech crime landelijk, een belangrijk deel van de aangiften niet opgepakt kunnen worden. Tegelijkertijd heeft de praktijk ook geleerd dat er genoeg zaken van gedigitaliseerde criminaliteit zijn die in principe op het districtelijke niveau ‘gedraaid’ kunnen worden: met de complexiteit van deze zaken valt het best mee, waardoor men hierin toch de gewenste resultaten kan boeken (evt. met gebruikmaking van een ‘hulplijn’ zoals het TDO of cybercrimeteam). De ‘vriend-in-nood-fraude’ en de ‘marktplaats-fraude’ zijn hiervan de bekende voorbeelden, maar naar verwachting zijn er meer te vinden. Er ontbreekt echter nog wel kennis en ervaring bij districtsrecherche en basisteams. In combinatie met de nog beperkte prioriteit die aan gedigitaliseerde criminaliteit wordt gegeven, leidt deze onbekendheid met de thematiek ertoe dat veel aangiften (die wel bij voornamelijk het basisteamniveau zouden passen) nog blijven liggen.

Aan welke kennis bestaat behoefte? Er is om te beginnen behoefte aan meer juridische kennis. Zo is tijdens de interviews aangegeven dat veel collega’s binnen de politie wetsartikelen over digitale delicten en de opsporing daarvan niet of slecht kennen. Ook zou men beter in de gelegenheid gesteld moeten worden om op de hoogte te blijven over ontwikkelingen in de criminaliteit, in technische ontwikkelingen

en (aanverwante) opsporingsmethoden. Zo zouden slechts weinig medewerkers binnen het district weten of en hoe digitale bewijstukken veiliggesteld kunnen worden, zoals bijvoorbeeld een mailbox of een mobiele telefoon.

Tegelijkertijd ligt ook het peil van digitale vaardigheden in het algemeen gemiddeld nog (lang) niet hoog genoeg volgens de geïnterviewde politiemedewerkers. Men is ervan overtuigd dat hier nog het nodige aan moet gebeuren. Denk hierbij onder meer aan computervaardigheden en het gebruik van sociale media. Wij vinden het overigens moeilijk te bepalen in hoeverre hier sprake is van (negatieve) beeldvorming. De reacties tijdens de interviews waren weleens om somber van te worden, maar vermoedelijk is ook hier sprake van een normaalverdeling, waarbij de meeste politiemensen wel degelijk over gemiddelde tot goede vaardigheden beschikken, enkelingen zeer veel kennis en vaardigheden hebben ontwikkeld en eveneens enkelingen over zeer weinig digitale vaardigheden beschikken. Nadere beschouwing van de feitelijk aanwezige en benodigde vaardigheden en een gerichte strategie volgen lijken verstandig, waarbij bijvoorbeeld een bepaald basisniveau gehaald moet gaan worden en daarnaast een kleine selectie een 'expertrol' krijgt. Tegelijkertijd, zoals ook hierboven en in eerdere hoofdstukken al duidelijk naar voren kwam, blijken samenwerking en het inzetten van 'hulplijnen' mogelijkheden te bieden om het potentieel aan (lokale) politiemensen dat snel inzetbaar is bij het tegengaan van gedigitaliseerde criminaliteit snel te benutten. Echter, zonder een plan om kennis en ervaring op te doen zullen de grenzen eerder in zicht komen.

6.3.3 Ervaringen met opleidingsmogelijkheden tot nu toe

Opvallend is dat onder meer binnen het digitaal flexteam nog maar vrij beperkt opleidingen worden aangeboden aan de medewerkers (zie ook hoofdstuk 5). Daar ligt vermoedelijk een belangrijke kans; gemotiveerde medewerkers de kans geven om een bij hun rol passende opleiding te volgen. Overigens hebben wij van de beschikbaarheid van opleidingen geen duidelijk beeld gekregen, mede doordat er binnen het district nog geen uitgewerkt opleidingsplan voorhanden is, ook niet binnen het digitaal flexteam.

Een politiedistrict klaarstomen op de digitale politietaak van de toekomst lijkt een kwestie van lange adem te zijn, waarbij de zoektocht nog maar net van start is gegaan. De taakverdeling is zelfs nog niet in potlood geschreven, de opleidingsbehoefte die daarbij past ontbreekt dan ook nog en vervolgens kan nog blijken dat het opleidingsaanbod nog niet (helemaal) voldoet. Opmerkelijk is wel dat enkele leden van het digitaal flexteam aangeven ook zelfstandig in staat te zijn om de benodigde kennis te verzamelen (zie hoofdstuk 5), daarbij geholpen met beschikbare kennisbanken van de politie maar ook door bijvoorbeeld filmpjes op YouTube. Ook lijkt *on-the-job-learning* voor een deel van de politiemensen in de basisteams een begaanbare route, waarbij wel gewaakt moet worden dat kennis ook de kans krijgt om te beklijven. Van belang is werkzaamheden regelmatig terug te laten keren, zodat er routine ontstaat, eenmaal verworven kennis niet de kans krijgt weg te zakken en kortom geïnvesteerde (leer)tijd niet verloren gaat. Daarbij blijkt uit de praktijk dat kennis overdragen in een klein team of kleine groepjes, het beste werkt: zo wordt voorkomen dat collega's overspoeld raken en zo in hun 'koudwatervrees' worden bevestigd.

Belangrijk te vermelden tot slot is dat de politieopleiding nog maar weinig in de behoefte lijkt te voorzien: volgens de geïnterviewde politiemedewerkers in dit onderzoek is er binnen de opleiding nog maar weinig aandacht voor het nieuwe verschijnsel *gedigitaliseerde criminaliteit* en vinden ze dat toekomstige politiemedewerkers in het algemeen slecht worden voorbereid op de digitale aspecten van hun (toekomstige) werk.

7

De lokale, digitale stap voorwaarts en het landelijke niveau

Hoofdstuk 7

De lokale, digitale stap voorwaarts en het landelijke niveau

In dit hoofdstuk maken we de balans op, beantwoorden we de hoofdvraag, geven we aanbevelingen aan de politiepraktijk en doen we suggesties voor vervolgonderzoek. Hierbij vertrekken we vanuit de gezamenlijke, lokale visie op de aanpak van gedigitaliseerde criminaliteit in het district IJsselland: deze verkennen we in de eerste paragraaf. Vervolgens behandelen wij de actuele, lokale ambities van het district in de aanpak van gedigitaliseerde criminaliteit in paragraaf 7.2. Paragraaf 7.3 gaat in op ontwikkelingen op landelijk niveau (zie ook paragraaf 2.4). In paragraaf 7.4 beantwoorden we de hoofdvraag van dit onderzoek aan de hand van de deelvragen, gevolgd door aanbevelingen op het lokale, eenheids- en landelijke niveau om het Gebiedsgebonden Politiewerk in samenspel met andere (organisatie)onderdelen meer toe te rusten op het effectief aanpakken van gedigitaliseerde criminaliteit. We sluiten af met enkele suggesties voor vervolgonderzoek.

7.1 De IJssellandse visie op de lokale aanpak van gedigitaliseerde criminaliteit

Hoe de medewerkers van het district IJsselland tegen de lokale aanpak van gedigitaliseerde criminaliteit aan kijken is duidelijk geworden in een tweetal groepsgesprekken. Deze gesprekken hebben we gevoerd met medewerkers van twee basisteams, van het digitaal flexteam, de districtsrecherche en het cybercrimeteam Oost-Nederland.

De eerste *lockdown* had een duidelijk effect op het werk van de medewerkers van het district IJsselland. Naast het *up-to-date* blijven van de geldende maatregelen om deze te kunnen handhaven en een praktische zoektocht naar voldoende mondkapjes, desinfectie gels, middelen om te kunnen thuiswerken en een overgang naar de digitale Teams omgeving, werd duidelijk dat ook veranderingen in de criminaliteit lokaal aandacht gingen vragen. Zo was het opdrogen van de offline criminaliteit en de toename van online criminaliteit tijdens de eerste *lockdown* voor de collega's van Service en Intake aan de frontdesk duidelijk merkbaar.

Over de verschuiving naar online criminaliteit in de eerste *lockdown* was iedereen het wel eens, maar over wie er achter die verschuiving zitten bestaan nog de nodige vraagtekens. Het ligt niet voor de hand dat de lokale inbreker ineens online actief is geworden. Die wacht gewoon tot hij de volgende kraak kan zetten, zo is de gedachte. Men verwacht eerder dat er al een aantal mensen ervaring had en dat die groep actiever is geworden. Waarbij vermoedelijk 'extra handjes' in de uitvoering nodig waren en dus meer geldezels en ronselaars moesten worden ingeschakeld. Men verwacht na de *lockdown* al snel terug te gaan naar een situatie die vergelijkbaar is met die van voor de coronacrisis. Maar daarbij wordt wel aangetekend te verwachten dat cybercriminaliteit op een hoog niveau zal blijven.

Dit beeld – dat cybercriminaliteit een blijvende rol zal spelen en naast het oude, vertrouwde politiewerk erbij is gekomen – moet volgens onze gespreksdeelnemers nog wel breder binnen het district bekend worden. Daarmee kwamen de gespreksdeelnemers, behalve op de noodzaak van het aanpassen van het selectiviteitskader en de lokale prioriteiten ook terug op de onbekendheid met cybercriminaliteit in de organisatie. Dat er nog niet wordt doorgepakt op cyberzaken is vooral het gevolg van de relatieve onbekendheid van het fenomeen in combinatie met de beleidsprioriteiten. Daarbij knaagt het soms bij collega's op straat dat capaciteit die eerst op straat werd ingezet of voor de opsporing van 'veelvoorkomende criminaliteit', tegenwoordig wordt ingezet op het tegengaan van cybercriminaliteit.

Het is volgens de gespreksdeelnemers van belang om na te denken over prioritering en capaciteit, zodat meer ervaring opgedaan kan worden met de aanpak van cybercriminaliteit. Hierbij wordt door de medewerkers die al wat ervaring hebben aangetekend dat "gewoon beginnen" aan een cyberzaak er niet bij is. Misschien daalt de offline criminaliteit wel in zijn algemeenheid, maar dat betekent niet dat het minder druk is binnen het district: er moeten nog steeds op dagelijkse basis keuzes over de inzet van de beschikbare mensen worden gemaakt. Er moet prioriteit aan worden gegeven en worden afgestemd met andere onderdelen binnen de politieorganisatie. Als het basisteam in beweging komt op de *money mules*, dan levert dat al snel informatie op over de hogere lagen van een criminele organisatie. Dat betekent werk voor de districtsrecherche en/of het cybercrimeteam. Maar ook voor hun werk is lang niet altijd de capaciteit beschikbaar waar het gaat om zaken met een digitale component.

De relatieve onbekendheid met cybercriminaliteit, het selectiviteitskader, lokale prioriteiten, en de capaciteitsproblemen werken belemmerend voor het aanpakken van cybercriminaliteit. Daarnaast is ook de huidige informatiepositie op dit thema een knelpunt, zo blijkt tijdens de gevoerde gesprekken. Zo geeft de geografisch georiënteerde werkwijze van de politie en dito registratie in onder meer BVH 'kortsluiting' op de geografisch onbegrensde aard van cybercriminaliteit. Er ligt vanuit de beperkte informatiepositie en capaciteit in het district, zo is de heersende opvatting tijdens de gesprekken, vooral een taak op eenheidsniveau en bij landelijke politieonderdelen bij de bestrijding van gedigitaliseerde criminaliteit. Daar zou men onder meer informatie en aangiften bij elkaar moeten brengen en de eerste opsporingsslag moeten doen, voordat het lokale niveau aan het werk kan. Waar (op kleine schaal) aangiften van gedigitaliseerde criminaliteit worden opgepakt, blijkt regelmatig dat op meerdere plekken in het land dezelfde informatie wordt gevorderd bij derden en ook dat dergelijke aangiften vaak aan elkaar gelinkt kunnen worden. Daardoor wordt een opsporingsonderzoek al gauw veel te omvangrijk, onder de huidige omstandigheden.

Er is een probleem dat het verdient aangepakt te worden, maar het werk moet wel behapbaar blijven. Het uitgangspunt van gecentraliseerde opsporing van cybercriminaliteit en decentrale opvolging wanneer er verdachten in beeld zijn, krijgt veel steun van de gespreksdeelnemers. Daarbij wordt door alle gespreksdeelnemers onderstreept dat er serieus geïnvesteerd zal moeten worden in de (extra) digitale politietaak, daarbij rekening houdend met de al bestaande capaciteitsproblemen: de opsporing van cybercriminelen vraagt – naast het klassieke, lokale politiewerk – te veel capaciteit. Maar in combinatie met gecentraliseerde analyse van informatie en coördinatie van de opsporing, zien onze gespreksdeelnemers wel een duidelijke rol voor de basisteams en de districtsrecherche. Deze rol is allereerst signalerend, want lokale professionals hebben kennis van de lokale situatie en bijvoorbeeld zicht op kwetsbare jongeren die ten prooi kunnen vallen aan oplichters en ronselaars. Zij kunnen goed helpen in het vormen van een lokaal beeld, helpen prioriteiten te stellen, een rol spelen in de preventie en tevens in (de ondersteuning van) opsporingsonderzoeken.

Bekendheid met de lokale situatie kan helpen wanneer verdachten in het opsporingsproces in beeld zijn, onder meer bij het in kaart brengen van hun netwerk en verblijfslocaties. Verdachten zitten nu eenmaal ergens lokaal in een wijk en zijn soms al 'bekenden' van de politie. De toegevoegde waarde van lokale kennis wordt tijdens de gesprekken beaamd door het cybercrimeteam. Het ziet onder meer een belangrijke rol voor gebiedsgebonden collega's in het meedenken in het stellen van prioriteiten in de opsporing.

7.2 De ambities in de aanpak van gedigitaliseerde criminaliteit in IJsselland

In gesprek met de districtsleiding werd duidelijk dat het district de prioriteit op het aanpakken van gedigitaliseerde criminaliteit wil behouden en de aanpak ervan – binnen de grenzen van de huidige capaciteit en mogelijkheden – verder wil versterken. Daarbij wordt aangetekend dat de klassieke criminaliteit in de fysieke wereld tijdens de tweede *lockdown* alweer snel terug was op het niveau van

voor de *lockdowns*. Dit versterkt de lokale verwachting dat gedigitaliseerde criminaliteit na corona niet in plaats van deze klassieke criminaliteit zal komen, maar er vermoedelijk bij zal komen. Desalniettemin is het volgens de districtsleiding zaak om lokaal in te blijven zetten op de bestrijding ervan.

Na de zomer van 2021 zal de inzet van het digitaal flexteam worden geëvalueerd. Hoewel er discussie mogelijk is over de capaciteit die dit team lokaal vraagt, is het binnen het district vooralsnog wel de plek waar men werkend leert in de aanpak van gedigitaliseerde criminaliteit. De ambitie is uitgesproken om de opsporende rol van dit team te versterken (hoewel er momenteel geen ervaren rechercheurs deel van uitmaken).

De districtsleiding gaf aan zowel de goede wil als de worsteling van het district in de omgang met gedigitaliseerde criminaliteit te herkennen zoals deze in dit rapport is opgetekend. Maar de ambitie blijft om op lokaal niveau gebiedsgebonden collega's mee te nemen in de noodzaak om gedigitaliseerde criminaliteit aan te pakken. Ook kan worden geconstateerd dat ondanks de lokale successen zoals deze in voorgaande zijn beschreven, op de werkvloer nog een gelaten houding heerst waar het gaat om de mogelijkheden om tegen gedigitaliseerde criminaliteit op te treden. Voor een deel van het personeel van het district ligt de nadruk op het leren en uitproberen binnen het digitaal flexteam, om vervolgens de rest van de organisatie mee te nemen in deze leerervaringen. De motivatie van de uitvoerende politiemedewerker om met gedigitaliseerde criminaliteit aan de slag te gaan, behoeft nog aandacht volgens de districtsleiding.

Er wordt vooral onder de leidinggevenden van de verschillende onderdelen van het district nog terughoudend gereageerd, want de aanpak van gedigitaliseerde criminaliteit is nieuw. Het kost nog relatief veel tijd en energie van personeel om ermee vertrouwd te raken. Iedere zaak die rondom gedigitaliseerde criminaliteit wordt opgepakt, betekent dat een andere, klassieke criminaliteitszaak blijft liggen. Dat is waar volgens de districtsleiding het gebrek aan een integrale prioriteitsstelling en beperkte affiniteit en ervaring met gedigitaliseerde criminaliteit zich op de werkvloer wreken. Volgens de districtsleiding speelt iets vergelijkbaars bij het lokale bevoegd gezag. Burgemeesters zouden niet de noodzaak ervaren van *'ook lokaal op gedigitaliseerde criminaliteit in beweging te komen'*. Het wordt ervaren als een abstracte en vooral internationale dreiging en er is weinig inzicht in effecten die lokaal te bereiken zijn. Dit is ook waarover de districtsleiding met de regionale burgemeesters, het Openbaar Ministerie en andere partners het gesprek wil aangaan. Echter, eerst moet landelijk het nodige aan de informatiepositie ten aanzien van gedigitaliseerde criminaliteit en de coördinatie van dit type zaken gebeuren, voor men op lokaal niveau echt kan doorpakken.

In het kort gelden voor de districtsleiding de volgende prioriteiten:

I. Inzetten van de basisteams op de opsporing van de faciliterende laag in het lokale criminele netwerk in de vorm van geldezels en ronselaars;
II. Als district het digitaal flexteam verder laten leren en meer collega's van de basisteams en andere onderdelen van het district laten betrekken bij de aanpak van dit nieuwe thema;
III. Het capaciteitsvraagstuk binnen het district opnieuw tegen het licht houden. De dagelijkse prioritering is nog erg gefocust op de klassieke, offline criminaliteit terwijl de realiteit duidelijk is veranderd: gedigitaliseerde criminaliteit is *here to stay*. Ook in IJsselland. Steeds zijn *high impact crimes* (HIC) leidend; gedigitaliseerde criminaliteit valt daar niet onder. Om dit aan te passen wordt door de districtsleiding met de operationele leiding en het bevoegd gezag verder gesproken.

Afsluitend werd door de districtsleiding aangegeven dat de noodzaak om tot een landelijke optimalisering van de informatiehuishouding en coördinatie rondom gedigitaliseerde criminaliteit te komen, sterk wordt herkend. Daarbij juicht men vanuit dit district een heroriëntatie op de geografische focus in de aanpak van cybercriminaliteit van harte toe. Idealiter wordt ook stevig geïnvesteerd in de preventie van slachtofferschap, aldus de districtsleiding, maar de vraag is hoeveel ruimte hiervoor ontstaat in de

toekomst. Een belangrijk vraagstuk is ook hoe preventie vorm te geven. Via voorlichting of eerder in de vorm van niet-strafrechtelijke afdoening en 'verstoren' van activiteiten van criminelen.

7.3 De digitale stap voorwaarts in de landelijke context

Hoewel het zwaartepunt van deze studie op het lokale niveau in de politieorganisatie ligt, heeft voorgaande duidelijk gemaakt dat het ook nuttig is om te verkennen welke relevante ontwikkelingen zich op landelijk niveau afspelen waar het gaat om de 'digitale stap voorwaarts'. Een belangrijk vraagstuk binnen de politie is hoe de politieorganisatie als geheel kan inspelen op de veelal bovenlokale aard van gedigitaliseerde criminaliteit. Onderstaand staat de vraag centraal hoe door direct betrokkenen binnen de politie wordt aangekeken tegen de wijze waarop hiermee omgegaan zou moeten worden. Het gaat hier om een korte verkenning en nadrukkelijk niet om een evaluatie van de prestaties tot dusverre. Tijdens een vijftal interviews zijn de volgende deelaspecten aan de orde gesteld, die hierna achtereenvolgens besproken zullen worden:

- Registratie van gedigitaliseerde criminaliteit
- Analyse, coördinatie en prioritering van zaken
- Rol voor het lokale niveau
- Voorbereiding van landelijk initiatief

7.3.1 Registratie van gedigitaliseerde criminaliteit

Op welke manier moet gedigitaliseerde criminaliteit worden geregistreerd? Welke specifieke omstandigheden spelen hier een rol bij? Wat is er nog voor nodig om registratie van gedigitaliseerde criminaliteit en het vervolg hierop te verbeteren? Deze vragen komen in deze subsectie aan bod.

Tijdens de interviews komen verschillende onderdelen van het registratievraagstuk naar voren. Allereerst is gebleken, zoals eerder in dit rapport al naar voren kwam, dat het registratiesysteem BVH met daarin een categorisering op basis van 'maatschappelijke klassen' (een indeling die sterk uitgaat van de strafbare feiten in het Wetboek van Strafrecht) in de praktijk onvoldoende mogelijkheden biedt om de ontwikkeling van verschillende vormen van gedigitaliseerde criminaliteit te monitoren. Daarnaast komt ook aan bod de behoefte aan een gestandaardiseerd aangifteproces waarbij ook geborgd is dat zoveel mogelijk digitale gegevens en bestanden worden geregistreerd en veiliggesteld.

Goede registratie en analysemogelijkheden zijn van groot belang. Zo stelt één van de geïnterviewde politiemensen dat onvoldoende onderscheid wordt gemaakt tussen *cybercrime* en gedigitaliseerde criminaliteit. *Cybercrime* – meer specifiek *hacken*, *ransomware*, DDoS-aanvallen en stelen en helen van data – deze verschijnselen eisen in zijn ogen te veel aandacht in de beeldvorming. De bulk van de gepleegde misdaad zou worden gevormd door *cyber-enabled crime*, online gedigitaliseerde criminaliteit: oplichting, fraude, *phishing*.

> *'Het probleem dat wij zelf creëren, is dat we niet helder krijgen waar we voor zijn. Media, politiek en politie werken langs elkaar heen. Waar we echt last van hebben is de enorme hoeveelheid gedigitaliseerde criminaliteit, maar dat wordt te weinig beseft.'*

Ook uit de andere interviews komt naar voren dat het verschijnsel gedigitaliseerde criminaliteit nog een positie moet verwerven in de prioriteitsstelling op de verschillende niveaus in de organisatie, ten opzichte van *cybercrime* waar het team *high tech* zich op richt, maar vooral ten opzichte van *offline* delicten. Er zou een norm moeten komen voor de aanpak hiervan, waarbij de prioriteiten lokaal mede bepaald kunnen worden maar zaken van gedigitaliseerde criminaliteit niet langer van tafel kunnen vallen.

Bij het registratieprobleem in BVH betekent concreet dat er onvoldoende mogelijkheden zijn gericht op trends in te spelen en daar medewerkers op in te zetten – althans wanneer uitsluitend gebruikgemaakt

zou worden van BVH. Intussen zijn alternatieven gevonden, waarbij analyses worden uitgevoerd op de internetaangiften. Aangiften die via internet binnenkomen zijn (ook) in een apart systeem raadpleegbaar en kunnen kennelijk in een aparte database worden geanalyseerd. Aangiften die door politiemensen zijn opgenomen worden hierbij niet meegenomen. Het is dan ook van belang dat (zolang het huidige BVH in gebruik is) bijvoorbeeld door het toevoegen van 'kenmerken' aan de aangifte in BVH, classificatie van de binnengekomen aangiften alsnog mogelijk te maken, zodat op trends kan worden ingespeeld. Evenzeer is volgens de geïnterviewde politiemensen van belang om 'digitale' aangiften goed te protocolleren zodat bij gevallen van gedigitaliseerde criminaliteit de benodigde gegevens worden opgenomen en veiliggesteld.

Een andere mogelijkheid die ook bij de landelijke spelers wordt genoemd is het aangifteproces bij gevallen van cybercriminaliteit geheel te baseren op de internetaangifte. De internetaangifte zou een positieve invloed hebben op de aangiftebereidheid, vanwege de laagdrempeligheid en het gemakkelijk kunnen *uploaden* van benodigde gegevens en bestanden (denk ook aan transactieoverzichten, appjes, screenshots e.d.). Genoemd wordt ook dat politiemensen desgewenst (met de aangever op het bureau) kunnen assisteren bij het invullen. Een punt van zorg hierbij is dat politiemensen in de basisteams en in het bijzonder de intakemedewerker protocollen en instructies moeten krijgen en maar tot op zekere hoogte 'belastbaar' zijn met detailkennis. Hulplijnen kunnen hierbij dan ook van belang zijn. Er lijkt meer gerichte aandacht nodig: coördinatie en onderzoek, om te kijken wat er nodig is en hoe verbeteringen landelijk kunnen worden doorgevoerd.

7.3.2 Analyse, coördinatie en prioritering

Cybercrime en zeker gedigitaliseerde criminaliteit is dermate in opkomst dat deze verschijnselen helaas een zekere alledaagsheid hebben gekregen: er zijn heel veel slachtoffers en veel daders. Op alle niveaus in de politieorganisatie zal hierop een antwoord gevonden moeten worden, en niet eenmalig, maar structureel, waarbij de bovenlokale aard van de opkomende vormen van criminaliteit aanleiding geven niet langer uitsluitend de klassieke geografische taakverdeling binnen de politie te volgen. Deze constateringen zijn in deze rapportage al meermalen opgeschreven, maar ze vormen ook duidelijk de rode draad door de vijf interviews waarin het landelijke perspectief centraal stond.

De geïnterviewde functionarissen vinden het van groot belang dat de eenheden snel politiemensen ter beschikking stellen voor landelijke initiatieven. Ook is men eensgezind over de noodzaak de informatiehuishouding, opleidingen, werving en prioritering van zaken ondersteunend te maken aan de nieuwe uitdagingen. Hetzelfde geldt voor de verwachtingen van de recherche-afdelingen in de districten: allen vinden dat deze meer moeten gaan doen. Daarbij is het van groot belang capaciteit, kennis en vaardigheden te versterken op het lokale niveau, zodat de cybercrimeteams zich meer dan nu op criminele samenwerkingsverbanden kunnen richten.

Ook werd in dit rapport reeds ingegaan op de voordelen van centrale analyse, dossiervorming en vordering van gegevens bij derden. De banken zouden er zelfs op hebben gewezen dat gegevens zo vaak dubbel worden gevorderd door verschillende onderdelen van de politie. Coördinatie en uitvoering van activiteiten gericht tegen gedigitaliseerde criminaliteit op landelijk niveau bieden veel voordelen, zo maken meerdere geïnterviewde functionarissen duidelijk. Zij denken dan ook dat dit principe voorlopig belangrijk zal blijven. De bovenlokale aard van gedigitaliseerde criminaliteit en ook centrale afstemming met overheidspartners en het bedrijfsleven, zoals met de bankensector of het bedrijf achter *marktplaats.nl*, spelen hierbij een rol. Er zijn concrete toepassingen ontwikkeld die 'je op landelijk niveau niet meer kunt loslaten' zo wordt opgemerkt tijdens de interviews: *'Verwijzingsportaal 2.0 zorgt behalve voor NAW-gegevens ook voor vordering van historische bankgegevens en met 3.0 ook beeldmateriaal. Dat kan je niet meer loslaten.'*

Knelpunten zijn er ook. In de afgelopen jaren is het LMIo (Landelijk Meldpunt Internetoplichting) de coördinatie gaan doen bij oplichtingszaken via 'online handelplaatsen' zoals marktplaats.nl, webwinkels en sociale media. Daarbij is initiatief genomen dossiers voor te bereiden aan de hand van online binnengekomen aangiften. Deze aangiften kwamen niet bij de politie-eenheden binnen. Voordat een dossier door het LMIo naar één van de eenheden werd gestuurd, moest worden voldaan aan één of meer van de volgende criteria. Er zou minimaal sprake moeten zijn van tien aangiften, van tenminste 5000,- euro geleden schade en/of van een minderjarige verdachte. Echter, de aangeleverde zaken bleken als 'extra werk' te worden beschouwd, omdat de internetaangiften niet meetelden in het zaakvolgsysteem BOSZ. De interne urenverantwoording leverde kortom een knelpunt op voor de dossiers die het LMIo graag onderzocht wilde hebben. Ten tijde van dit onderzoek is besloten tot een pilot waarin wordt geprobeerd een oplossing te vinden voor dit probleem van het 'ongevraagd verstrekken van dossiers' vanuit het LMIo. Daarbij is gezocht naar een manier om ook administratief de eenheden verantwoordelijk te maken voor dossiers die landelijk worden voorbereid. Meerdere aandachtspunten lijken hierbij van belang, aangezien het in de praktijk lastig is gebleken eenheden verantwoordelijkheid te laten dragen voor digitale fraudezaken. Welke rol is weggelegd voor strafrechtelijk onderzoek en wanneer kunnen aangevers beter worden geholpen met een civielrechtelijke oplossing (verhalen schade), en wat is de rol van de politie daarbij? Welke prioriteit wordt aan de opsporing van digitale fraudezaken (die voldoen aan de criteria) gegeven? Welke rol spelen internetaangiften en aan het bureau binnengekomen aangiften?

Uit de gevoerde gesprekken komt naar voren dat de politie lokaal, ook los van de gewenste landelijke coördinatie, nog beter kan inspelen op gedigitaliseerde criminaliteit. Zo is het onmogelijk om alle zaken die binnenkomen te onderzoeken en te voorzien van een strafrechtelijke reactie. Gezien de aard van een deel van de criminaliteit ligt het 'monitoren' van verdachten en het inzetten van uiteenlopende niet-strafrechtelijke interventies voor de hand. Gedacht kan worden aan het voeren van zogeheten stopgesprekken: "Je kunt strafvervolging voorkomen door te stoppen met je criminele activiteiten." Ook kan de politie zich ervoor inzetten dat de geleden schade wordt verhaald op de dader. Vanzelfsprekend kunnen politiedistricten met hun kennis van de lokale situatie hier een belangrijke rol in spelen, waarbij volgens één van de geïnterviewde functionarissen cruciaal is dat een gecoördineerde aanpak wordt gehanteerd, waarbij zo nodig onderzoek en vervolging daadwerkelijk worden ingezet. Een belemmerende factor lijkt de financieringsgrondslag voor het OM te zijn: buitengerechtelijke afdoening zou daardoor niet standaard op medewerking van het OM kunnen rekenen. Maar tijdens de interviews zijn diverse mogelijkheden genoemd, waarmee in de praktijk al ervaring wordt opgedaan, waar het gaat om 'online handelsfraude'.

> *'De landelijke pilot 'Reprimande voor minderjarige verdachten' is interessant, we zien dat je daarmee ook achter de voordeur kunt komen. Je kunt ook denken aan buitengerechtelijke afdoening, waarbij terugbetaling mogelijk is en loopt via het CJIB. Je kunt ook denken aan een directe aansprakelijkheidsstelling. Een externe partij krijgt dan info uit politiedomein, om civielrechtelijk aan de slag te gaan, via de deurwaarder.'*

Door betrokkenen wordt ervaren dat cybercrime en vooral gedigitaliseerde criminaliteit nog onvoldoende op de agenda staan, waarbij bestaande beleidskaders, prioriteiten en ICT-systemen lijken tegen te werken. Maar niet alleen binnen politie en OM is het nog een gevecht om de bakens te verzetten, ook daarbuiten. Zo zijn meerdere van de geïnterviewde betrokkenen weinig positief over de actiegerichtheid van gemeenten. Er zou veel over slachtofferpreventie worden gesproken, maar gemeenten komen nog maar mondjesmaat tot concrete inzet. Terwijl met preventie (ook in de vorm van nazorg) veel bereikt lijkt te kunnen worden. Tegelijkertijd lijkt de politie slimmer om te kunnen gaan met het inschakelen van partners. Van effectieve netwerken waarin de politie kan aangeven welke ontwikkelingen er plaatsvinden en vervolgens een integrale aanpak wordt vastgesteld, lijkt landelijk en lokaal nog weinig sprake.

'Ik denk dat dit eigenlijk de kern is. Landelijk zijn campagnes nodig. Maar lokaal kan je ook dingen doen, door bijvoorbeeld slachtoffers van gedigitaliseerde criminaliteit specifiek preventie advies te geven. Daar kunnen gemeenten op inspelen. Zij kunnen ook beveiligingsbedrijven inzetten die burgers helpen hun devices te beveiligen.'

'Ook moeten we de manier waarop we met partners omgaan verbeteren. De VNG stelt nog steeds dezelfde vragen. De gemeente blijft achterover zitten met de vraag wat ze moeten doen. Scholen en bejaardenhuizen, ze hebben allemaal een rol. Ook in het bedrijfsleven zie je echt een ontwikkeling. Denk aan de ransomware waar bedrijven mee te maken kunnen krijgen. Criminelen leggen de bedrijfsvoering stil en vervolgens maken bedrijven een economische afweging. De aangiftebereidheid is heel laag en op grote schaal worden bitcoins betaald. Ook daar moet echt iets gebeuren.'

Benadrukt wordt dat ook na verloop van tijd 'gecoördineerde actie' op landelijk niveau nodig blijft, ook als de districten zelfstandig meer actief zijn geworden in de bestrijding van gedigitaliseerde criminaliteit. Opvallend is overigens dat tijdens de interviews regelmatig over de rol van gemeenten wordt gesproken, terwijl ook de rijksoverheid een taak zou kunnen hebben. Zo wordt gesproken over een *'rapid intervention team'* dat snel kan inspelen op nieuwe vormen van cybercrime, zowel repressief als preventief: *'We hebben rapid intervention nodig. Er zitten allemaal achterdeurtjes in WhatsApp en er komen steeds weer vormen van account-take over bij.'*

Tegelijkertijd wordt geconstateerd dat van een eenduidige landelijke aanpak nog geen sprake is: het LMIo vormt hier de uitzondering op de regel, maar is slechts verantwoordelijk voor een deelaspect. Het analyseren van informatie en het leggen van verbanden op landelijk niveau zou kunnen bijdragen aan het stoppen van criminele samenwerkingsverbanden, zoals in het voorbeeld van de vriend-in-nood-fraude. Op eenheidsniveau zouden analisten nog niet over dezelfde mate van inzicht beschikken als de cybercrimeteams en het LMIo. Daarbij kan een 'centrale hub' het interne overleg stimuleren over onder meer aanpassing van de politieopleiding, en tevens overleg voeren met externe partijen.

'Met de dossiers en werkpakketten voor de districten bewegen we ons nog in de onderlaag van het criminele circuit, van de geldezels vooral. Maar er zitten ronselaars en cashers achter en leidersfiguren. Het criminele verband blijft tot op heden eigenlijk nog buiten schot. Dat is vreemd. Landelijk moet je gecoördineerde actie hebben: verhoren helpen uitmelken, ronselaars in beeld brengen en laten verhoren, om zo het verband proberen bloot te leggen. Dit gaat niet gebeuren in de districten; dit vraagt focus en capaciteit. Bovendien zijn netwerken landelijk of internationaal en daar heb je een effectieve aanpak voor nodig. (...) Je hebt een coördinatie mechanisme nodig: een centrale hub. We kunnen het samenvoegen van zaken automatiseren, we doen dat nu nog handmatig ten behoeve van de werkpakketten. (...) Daarbij kan je opvragen van ontbrekende gegevens in de online aangifte ook landelijk organiseren. Via het verwijzingsportaal banken kan je naam en bankrekeningnummer opvragen en telefoonnummer kun je opvragen, die gegevens moet je vervolgens toetsen met GBA. Dan heb je een aangifte die compleet is. Vervolgens wil je met die gegevens pakketjes maken. Dit hele proces van samenvoegen en veredelen van informatie zou het beste in een centrale hub kunnen gebeuren. Om vervolgens het pakketje naar het district te sturen waar de verdachte woont. Je hebt de hub ook nodig voor de aansturing van de lokale aanpak en voor een aantal PPS'en.'

'De banken zitten op een heel goed spoor, zelfs (...) zijn goed bezig met een portal. De banken zijn in hun mindset bijgedraaid. Zij zien dat ze onderdeel zijn van het maatschappelijk probleem. De providers zien dat nog niet zo, die zetten in op hun dienstverlening voor de burger; een goed netwerk. Dat burgers erin trappen is niet hun

probleem. Daar ligt het gevoelig, hosting en netwerk. Dat met behulp van het netwerk fraude wordt gepleegd, daar vinden ze zichzelf niet verantwoordelijk voor. Zij kijken eerder naar het hosting bedrijf en verwijzen terug naar de vrijheid van de eindgebruiker.'

7.3.3 Rol voor het lokale niveau

'Als we doen wat we deden gaan we het niet redden: gedigitaliseerde criminaliteit zal dan onze achilleshiel blijven. Onze systemen en mensen zijn er niet op berekend. Dit is wat anders dan klassiek opsporingswerk. Ook de politie moet digitaliseren. We hebben een ander type rechercheur nodig bijvoorbeeld. Het profiel van de wijkagent en de agent op straat moeten we herzien. Als de samenleving zo digitaliseert als nu, moet je je daarop aanpassen, ook al blijft een groot deel van het werk hetzelfde. Die digitale dimensie komt er wel bij. Je hebt meer digitale specialisten nodig om digitale zaken te draaien. Dat is een flinke slag die we moeten maken.'

De hedendaagse samenleving is gedigitaliseerd, speelt zich deels online af en ook gedigitaliseerde criminaliteit heeft zijn intrede gedaan. De reikwijdte en impact hiervan betekenen dat ook op het lokale niveau de politie belangrijke aanpassingen zal moeten doen. Dit is de grote lijn in dit rapport en deze wordt ook volop bevestigd door de interviews met sleutelfiguren op landelijk niveau, zoals bovenstaand citaat duidelijk maakt. Zo is al aandacht nodig voor digitalisering in de opleiding van zittende en aankomende politiemensen. Ook in de werving zou rekening gehouden moeten worden met benodigde digitale vaardigheden, dat geldt voor elk niveau in de politieorganisatie. Daarbij wordt gemeend dat landelijk beleid nodig is om op lokaal niveau af te dwingen dat ook gedigitaliseerde criminaliteit een rol gaat spelen in de selectie van zaken. Op lokaal niveau kan een belangrijke bijdrage worden geleverd door de nieuwe 'bulk' van zaken op te pakken, waarbij in eerste instantie verdachten van relatief eenvoudige feiten verhoord kunnen worden. Van belang is ook zittende politiemensen ervaring en kennis te laten opdoen, en in staat te stellen om samen te werken met onder meer de cybercrimeteams en (op te richten) landelijke onderdelen.

Een andere wijze van omgaan met opsporingsinformatie speelt telkens een belangrijke rol tijdens de gevoerde gesprekken. Daarbij zorgt de digitale politietaak voor een duidelijk ervaren achterstand in de ontwikkeling van de informatiehuishouding.

'Onze organisatie is gebouwd op de situatie van acht jaar geleden, toen de nationale politie werd ingevoerd. Je ziet eigenlijk dat we nu bij de aanpak van nieuwe vormen van criminaliteit helemaal geen lange termijn plannen kunnen maken.'

7.3.4 Landelijk initiatief in voorbereiding

Uit de gevoerde gesprekken bleek ook dat er op landelijk niveau het nodige staat te veranderen ten aanzien van de registratie, maar ook de analyse en coördinatie van gedigitaliseerde criminaliteitszaken. De nieuwe 'bulk' aan gedigitaliseerde criminaliteit in de vorm van onder meer oplichting, fraude, ID-fraude, illegale webshops en *phishing* staat daarbij centraal. Daarbij wordt ingezet op een landelijk coördinatiepunt en *taskforces* op eenheidsniveau. Het landelijk coördinatiepunt zal afzonderlijk binnenkomende aangiften op het gebied van gedigitaliseerde criminaliteit samenvoegen en de eerste stappen zetten in de opsporing. Daarbij valt te denken aan het achterhalen van de te-naam-gestelde bij rekeningen, het vorderen van transactiegegevens en IP-adressen. Het centrale overzicht dat dit team verwerft zal moeten voorkomen dat zaken niet of moeizaam worden opgevolgd, doordat ze in de eenheid van de aangever achterblijven of van de ene kant naar de andere kant van het land worden gestuurd, met vertraging rondom af- en inboeken als gevolg. Doelstelling is aangiften gebundeld naar de eenheid te sturen waar de verdachte woont. Ook de landelijke aanpak en informatiepositie wil men versterken. Zo wordt ingezet op het 'uitfilteren' van de gedigitaliseerde criminaliteitszaken uit de veelvoud aan

gebruikte feitcodes. De bemensing van dit landelijke team wordt geregeld door elke eenheid een aantal medewerkers aan te laten leveren die *dedicated* voor dit team aan de slag kunnen. Hiervoor zou intussen bij de leiding van de politie-eenheden voldoende draagvlak zijn vanwege de omvang die gedigitaliseerde criminaliteit heeft gekregen.

Met deze voorgenomen, aangescherpte focus op landelijk niveau wordt ook de rol van het lokale niveau in de aanpak van gedigitaliseerde criminaliteit duidelijker. De ervaring leert dat er lokaal kennis is over daders en dadernetwerken in steden, buurten en wijken. Deze kennis kan worden benut met ondersteuning van het op te richten landelijke team. Zo kan een 'werkpakket' worden samengesteld. Dit betreft een bundeling van zaken tegen één of meerdere verdachten uit het lokale verzorgingsgebied. Dit kan worden ingestoken op het niveau van het basisteam, de VVC-afdeling of de districtsrecherche. Over de opvolging die wordt gegeven aan deze werkpakketten zijn nog duidelijke afspraken nodig. Dit initiatief impliceert ook een informatiestroom vanuit het lokale niveau terug naar het landelijke niveau: wanneer zaken worden opgepakt genereert dit nieuwe informatie die kan worden benut om verder zicht op de daders en dadernetwerken te verkrijgen. Met deze voorgenomen werkwijze wordt landelijk voortgebouwd op de goede ervaringen die er o.a. ook in het district IJsselland zijn opgedaan, die eerder in dit rapport zijn beschreven.

Diverse opvattingen van de geïnterviewde sleutelfiguren veronderstellen telkens versterking en coördinatie op landelijk niveau, en bijvoorbeeld voortgang in de ontwikkeling van nieuwe politie-ICT (zoals BVH). Ter illustratie enkele voorbeelden:

> *'De politie is nu inmiddels 8 jaar geleden Nationale Politie geworden en opgedeeld in 10 toch wel autonome eenheden. Er staat wel NP boven, maar we werken nog steeds met verschillende informatiesystemen en BVH. Onze systemen helpen het niet om cybercrime aan te pakken.'*

> *'EU-wetgeving voor telecombedrijven heeft echt te lang stilgestaan. We hebben deels te maken met de goodwill van providers dat ze met ons en het OM samenwerken. Bij digitale criminaliteit in de vorm van een oplichting trekken ze echt niet alle registers open. Er zijn een aantal partners, maar waar het gaat om wetgeving moet er wat gebeuren. Ook moet er een goede afweging worden gemaakt over mogelijkheden anoniem te blijven. Mag je anoniem op internet blijven? En hoe moet het met de pre-paid kaartjes voor de mobiel?.'*

> *'We moeten de voordelen van de digitale aanpak laten zien: mede aan de hand van LMIo-zaken heb je soms opeens reden om binnen te stappen in een pand en een slag te slaan in de bestrijding van een netwerk dat ook offline actief is. Het is onderdeel van het werk!'*

> *'We zijn een pilot gestart met verkoopfraude en vriend-in-nood, via een privaatrechtelijk spoor, aanvullend op het strafrechtelijke. Vooral voor gevallen waar je geen antwoord hebt vanuit de opsporing. Daar zijn we ook mee bezig en deze voorbeelden moeten we uitbouwen en verspreiden.'*

7.4 Beantwoording van de onderzoeksvragen

Tegen de achtergrond van de hierboven beschreven visie op de aanpak van gedigitaliseerde criminaliteit in het district IJsselland en de ambities van de districtsleiding, is het tijd om de onderzoeksvraag te beantwoorden: *'Hoe kan het Gebiedsgebonden Politiewerk in het district IJsselland in samenspel met andere (organisatie)onderdelen meer worden toegerust op het effectief aanpakken van gedigitaliseerde criminaliteit?'* Onze conclusie trekken wij door de subconclusies bij de deelvragen bij elkaar op te tellen.

7.4.1 Beantwoording van de eerste deelvraag: Internationale state of the art

De eerste deelvraag van dit onderzoek luidde: *'Wat is er in de internationale en nationale literatuur bekend over de ontwikkeling van gedigitaliseerde criminaliteit tijdens de coronacrisis en over hoe deze vormen van criminaliteit effectief kunnen worden aangepakt?'* We zien een brede dreiging uitgaan van zowel cybercriminaliteit in enge zin – waarin digitale systemen zowel het middel als het doel zijn – als van gedigitaliseerde criminaliteit. In deze laatste variant, ook wel *cyber-enabled* criminaliteit genoemd, is vooral de categorie bedrog en diefstal prominent. Hierbij spelen oplichters in op de sociaalpsychologische beïnvloedbaarheid van hun doelwit via principes van *social engineering*. Steeds gaat het gaat om al langer lopende trends waarop de coronacrisis een versterkend effect heeft.

Ook in de processen verbaal van de Nederlandse politie was al voor de coronacrisis – met een geautomatiseerde zoekslag van het CBS – een flink aandeel *cyber-enabled* bedrog en valsheidsmisdrijven zichtbaar. Naar verwachting is dit aandeel tijdens de coronacrisis alleen maar verder toegenomen. Vooral de opkomst van WhatsApp of vriend-in-nood-fraude springt daarbij in het oog, maar ook werd al vroeg in de coronacrisis door de Nederlandse politie gewaarschuwd voor een toename van de dreiging van *phishing*, malafide webshops en *malware*. Dat geldt niet alleen voor individuele burgers maar ook zeker voor bedrijven.

De internationale, wetenschappelijke *state of the art* over de coronacrisis, cybercriminaliteit en wat de politie daaraan zou kunnen doen, maakt duidelijk dat als gevolg van de *lockdowns* er internationaal een daling zichtbaar is in de traditionele criminaliteit en een stijging van cybercriminaliteit, waarbij vooral *phishing* toeneemt en een nieuwe groep daders als gevolg van verveling, werkeloosheid en negatieve spanning, in de cybercriminaliteit actief is geworden. Hoewel verklaringen veelal worden gezocht in de routineactiviteiten theorie, geeft het werk van Naidoo (2020) ook andere nuttige inzichten. Aan de hand van een integratief theoretisch model en een empirische toetsing langs honderden voorbeelden van corona-gerelateerde cybercriminaliteit stelt hij vast dat de situationele factoren van de pandemie en *lockdown* als extra element op de routineactiviteiten theorie moet worden toegevoegd, om de dynamiek van cybercriminaliteit in deze bijzondere tijd te kunnen begrijpen.

De collega's Horgan (et al., 2020) en Collier (et al, 2020) zien een grote potentiële bijdrage van de lokale politie en lokale partners in de aanpak van cybercriminaliteit. De nadruk wordt gelegd op lokale voorlichting van potentiële slachtoffers via bestaande, goede relaties en het opsporen en verstoren van lokale daders en dadergroepen. De verwachting is internationaal dat na de coronacrisis cybercriminaliteit zal blijven voorkomen in de huidige omvang en daarmee naast de traditionele criminaliteit zal komen te staan, wanneer het maatschappelijk verkeer weer toeneemt. Daarbij zal de politie ook lokaal een verschil kunnen maken, maar hoe precies, en welke kennisbasis en ervaring zij nodig hebben en tegen welke praktische knelpunten zij vervolgens aanlopen, blijft onderbelicht.

7.4.2 Beantwoording van de tweede deelvraag: het leereffect van GGP-ers

Dat is waar onze tweede deelvraag *'Wat is het leereffect van de gebiedsgebonden medewerkers van het district IJsselland in de aanpak van gedigitaliseerde criminaliteit?'* direct aanvulling op de internationale *state of the art* biedt. Het grootschalig onderzoek naar fraude via WhatsApp via het onderzoek 'Lucky' betrof een intensieve samenwerking van het basisteam IJsselland-Zuid en het cybercrimeteam Oost-Nederland. Met een voorwaardelijk sepot in de zaken van 24 *money mules* en celstraffen voor twee oplichters, is deze lokale aanpak van gedigitaliseerde criminaliteit als *good practice* aan te merken. Hieruit zijn maar liefst twintig succesfactoren gedestilleerd die ten behoeve van de deelconclusie zijn onderverdeeld in de categorieën randvoorwaarde, samenwerking, draagvlak, taakverdeling en uitvoering:

Samenwerking	Draagvlak	Taakverdeling	Samenwerking
• Projectmatige samenwerking tussen basisteam en cybercrimeteam en/of de districtsrecherche; • Maak een gezamenlijke doelstelling voor het project; • Realistische, nauwkeurige doelstellingen; • Maak een projectplan; • Planning en benodigde capaciteit in een vroegtijdig stadium afstemmen; • Zorg het OM de benodigde medewerkers heeft klaarstaan voor de veegweek; • Organiseer een gecoördineerde, gezamenlijke 'veegweek'; • Evalueer het verloop en de uitkomsten van het project.	• Zorg vroegtijdig voor betrokkenheid van het OM; • Jaag samen de lokale prioriteitstelling aan; • Laat de projectmedewerkers zelf meedenken over hun bijdrage aan het project; • Heb oog voor de individuele motivatie van medewerkers; • Na afloop: Horizontaal leren!	• Laat cybercrimeteam of DR focussen op de zwaardere, bovenlokaal opererende verdachten en het basisteam op de lichtere, lokaal opererende verdachten; • Benut de specialistische kennis van het cybercrimeteam vooraf bij de instructie van o.a. basisteam collega's en als vraagbaak tijdens de veegweek.	• Reageer op signalen vanuit 'de onderbuik'; • Wees je bewust van de criminele organisatiestructuren die meestal gekoppeld zijn aan gedigitaliseerde criminaliteit; • Ga improviserend te werk bij het vinden van capaciteit, maar zet collega's in op hun expertise; • Neem telefoons van de pinners en money mules in beslag en analyseer o.a. chatgesprekken; • Laat onderlinge verbanden tussen aangiften rusten.

Randvoorwaarde: Laat gebrek aan routine en digitale vaardigheden niet demotiveren!

7.4.3 Beantwoording van de derde deelvraag: leereffect van het digitaal flexteam

De derde deelvraag luidde vervolgens: *'Wat is het leereffect van het digitaal flexteam van het district IJsselland in de aanpak van gedigitaliseerde criminaliteit?'*

Tijdens de coronacrisis heeft gedigitaliseerde criminaliteit zich een nog sterkere positie verworven. Daarmee is bijdragen aan de bestrijding hiervan een uiterst actueel thema voor alle niveaus binnen de politieorganisatie. Binnen het district IJsselland is het digitaal flexteam al voor de coronacrisis ingezet op het tegengaan van gedigitaliseerde criminaliteit.

De aanpak van gedigitaliseerde criminaliteit en de benodigde digitale professionalisering in het algemeen, lijken flink wat aandacht te kunnen gebruiken. Binnen het digitaal flexteam krijgen basis-teammedewerkers de mogelijkheid om zich op dit vlak te ontwikkelen. Daarbij is complicerend dat ze in de opsporing nog vrij onervaren zijn. Uit de ervaringen van het digitaal flexteam blijkt verder dat er nog relatief weinig prioriteit aan gedigitaliseerde criminaliteit wordt gegeven. Daarnaast heeft

men ondersteuning nodig met opleidingen, faciliteiten en de invoering van nieuwe functies (bv. taakaccenthouders of digitale wijkagenten).

Ten tijde van dit onderzoek is nog niet duidelijk of de aanpak van het digitaal flexteam blijft, en hoe zittende politiemensen in IJsselland zich in de toekomst de digitale politietaak eigen zullen moeten maken. Dit onderzoek kan niet duidelijk maken of een apart districtelijk team te verkiezen is boven het integreren van digitale zaken in het werk van de basisteams en districtsrecherches (ondersteund door bijv. een taakaccenthouder). Er zijn meerdere opties waar ervaring mee opgedaan kan worden en het lijkt nuttig ervaringen intern uit te wisselen en te (laten) evalueren. Interessant is daarbij de vraag hoe kennis het beste vastgehouden kan worden in de organisatie en tevens hoe die kennis het beste te verspreiden.

Bij dit voor de politie relatief nieuwe werkveld gedigitaliseerde criminaliteit is nog veelvuldig de vraag hoe de verantwoordelijkheden verdeeld zijn en zouden moeten worden, onder meer tussen basisteam en districtsrecherche. Ook blijkt nog vaak onduidelijk te zijn waar de grens van de eigen verantwoordelijkheid ligt en die van een ander politieonderdeel begint. Vooralsnog lijkt het verstandig om de onduidelijkheid onder ogen te zien en dik gemarkeerde grenzen op de kaart te vermijden, maar: hoe moeten de grenslijnen eruit komen te zien? En hoe moet in dit verband tegen de veelal bovenlokale aard van gedigitaliseerde criminaliteit worden aangekeken? Welk aandeel van het werk behoort een politiedistrict op zich te kunnen nemen? Het zijn vragen die – ondanks de motivatie om gedigitaliseerde criminaliteit aan te pakken – nog regelmatig voor verkramping lijken te zorgen.

Het digitaal flexteam van IJsselland toont intussen aan dat binnen de politieorganisatie wel degelijk veel potentie aanwezig is om de nieuwe digitale uitdagingen aan te gaan, ook lokaal. Daarbij is het team graag bereid nieuwe vormen van samenwerking aan te gaan, om de veelal bovenlokale aard van gedigitaliseerde criminaliteit het hoofd te kunnen bieden. Ook krijgt het digitaal flexteam kennis via gespecialiseerde onderdelen, vooral het cybercrimeteam op eenheidsniveau en het (landelijk georganiseerde) Team Digitale Opsporing (TDO).

7.4.4 Beantwoording van de vierde deelvraag: knelpunten in de huidige, lokale aanpak

De vierde deelvraag luidde *'Welke knelpunten ontstaan er in de huidige, gebiedsgebonden aanpak van gedigitaliseerde criminaliteit door het district IJsselland?'*

Hierbij komen uit onze gesprekken met de medewerkers van het district IJsselland drie thema's bovendrijven: (I) de informatievoorziening rondom gedigitaliseerde criminaliteit; (II) de samenwerking binnen de politieorganisatie en met partners en (III) de digitale kennis en vaardigheden van politiemedewerkers. We lopen onderstaand de bevindingen per thema kort en bondig langs.

Ten aanzien van de informatievoorziening is er sprake van de volgende knelpunten in de huidige, lokale aanpak van gedigitaliseerde criminaliteit in het district IJsselland:

- Er ontbreekt een landelijke, eenduidige registratiewijze en monitoring waardoor men noodgedwongen kunstgrepen moet doen om lokaal tot een overzicht van de aangiften en verdachten rond gedigitaliseerde criminaliteit te komen;
- De kwaliteit van de aangiften rond gedigitaliseerde criminaliteit moet landelijk worden aangescherpt;
- Bij het oppakken van aangiften rond gedigitaliseerde criminaliteit moet landelijk standaard worden afgesproken dat men de verwevenheid met andere zaken checkt via zaakkenmerken alvorens verder te gaan, er wordt nu veel dubbel werk verzet (o.a. vorderen gegevens);
- Er is landelijk sprake van een zeer groot aantal aangiften van digitale fraude en van een grote hoeveelheid aan onoverzichtelijke informatie, ook vanwege gebrek aan een eenduidige registratiewijze;
- Waar aangiften binnenkomen, zegt bij gedigitaliseerde criminaliteit betrekkelijk weinig. De

grotendeels geografische taakverdeling binnen de politie werkt hier duidelijk nadelig. Een aangifte oppakken betekent een relatief grote kans op het moeten overdragen van de zaak, omdat de verdachte die in beeld komt veelal buiten het eigen werkgebied woont.

De volgende knelpunten spelen ten aanzien van de organisatie van het werk in IJsselland en de samenwerking binnen de politieorganisatie:
- Het wordt lastig gevonden op lokaal niveau prioriteit te geven aan gedigitaliseerde criminaliteit omdat daar de capaciteit voor zou ontbreken;
- Daarbij wordt een zekere krampachtigheid zichtbaar als gevolg van het feit dat cybercriminaliteit vaak sterk vertakt is, opsporingsonderzoek wordt daardoor al gauw te omvangrijk en/of moet overgedragen worden;
- Basisteams signaleren soms dat min of meer 'bekende criminelen' gebruik zijn gaan maken van digitale hulpmiddelen of zijn overgeschakeld naar gedigitaliseerde vormen van criminaliteit. De wijkagent en andere politiemensen met een lokale informatiepositie moeten hier nog op in leren spelen;
- In de basisteams zelf valt op dat nog niet is voorzien in een structurele inbedding van de 'hulplijn'-constructie in de aanpak van gedigitaliseerde criminaliteit. Het inzetten van taakaccenthouders gedigitaliseerde criminaliteit of digitale wijkagenten lijkt daarbij een voor de hand liggende optie;
- Er is er nog geen duidelijkheid over de taakverdeling bij de aanpak van gedigitaliseerde criminaliteit tussen districtsrecherches en basisteams;
- Gezien de complexiteit, verwevenheid en geografische spreiding van veel gedigitaliseerde criminaliteitszaken is samenwerking in de aanpak ervan (voorlopig) cruciaal, met onder meer het cybercrimeteam en het Team Digitale Opsporing (TDO).

Rondom de digitale kennis en vaardigheden van politiemedewerkers spelen in het district IJsselland de volgende knelpunten:
- De praktische, technische en juridische kennis in de aanpak van gedigitaliseerde criminaliteit laat nog te wensen over;
- Er is nog weinig sprake van een systematische kennisoverdracht en training van politiemensen binnen het district, waar het gaat om gedigitaliseerde criminaliteit;
- Ook in de politieopleiding is er nog maar nauwelijks aandacht voor gedigitaliseerde criminaliteit;
- Deze onbekendheid met de (nieuwe) digitale politietaak leidt ertoe dat veel aangiften die wel bij het basisteamniveau en de districtsrecherche zouden passen nog blijven liggen.

7.4.5 Beantwoording van de vijfde deelvraag: de bijdrage van GGP

De vijfde en laatste deelvraag luidde *'Hoe kan Gebiedsgebonden Politiewerk in het district IJsselland bijdragen aan het effectief aanpakken van gedigitaliseerde criminaliteit in samenwerking met andere onderdelen van het district IJsselland, de eenheid Oost-Nederland en het nationale niveau?'*

Een politiedistrict klaarstomen op de digitale, lokale politietaak van de toekomst lijkt een kwestie van lange adem te zijn, waarbij de zoektocht nog maar net van start is gegaan. Het is van belang om werkzaamheden regelmatig terug te laten keren, zodat er routine ontstaat en eenmaal verworven kennis niet de kans krijgt weg te zakken en kortom geïnvesteerde (leer)tijd niet verloren gaat. De onderlinge taakverdeling is nog niet beschreven, de opleidingsbehoefte die daarbij past ontbreekt nog en vervolgens kan nog blijken dat het opleidingsaanbod nog niet voldoet. Er is nog weinig sprake van een systematische kennisoverdracht en training van politiemensen binnen het district. Deze heeft in voorkomende gevallen nog het karakter van ad hoc *on-the-job-learning.*

Dit ad hoc leren past overigens bij het continue zoeken dat gebiedsgebonden politiewerk impliceert. Volgens Terpstra (2018) gaat dit politiewerk 'op lokaal niveau primair (...) om begrenzen, beschermen en bekrachtigen'. Het gaat ook 'om het stellen en bewaken van de norm, het beschermen van burgers tegen het kwaad, en het bewaken en herstellen van orde en vrede, maar dan vooral op lokaal niveau'.

Dit betekent dat de lokale politie steeds met haar samenwerkingspartners en inwoners zoekt naar een passende aanpak van lokale problemen. Meurs en Creulen (2017) wijzen in dit kader treffend op een noodzakelijke onderzoekende houding en een morele betrokkenheid, die wij in het district IJsselland zeker hebben mogen aantreffen.

Op basis van de opgedane leereffecten in het district IJsselland en de door ons gevoerde gesprekken hebben wij de onderstaande potentiële rol voor het gebiedsgebonden poltiewerk in de aanpak van gedigitaliseerde criminaliteit kunnen afleiden. Daarbij stellen we eerst de algemene contouren van het gebiedsgebonden politiewerk nog even scherp. Gebiedsgebonden politiezorg richt zich volgens Terpstra en collega's (2016) op de uitvoer van (I) noodhulp; (II) wijkwerk; (III) Intake & Service en (IV) de afhandeling van veel voorkomende criminaliteitszaken. Van der Torre, Tops en Van Valkenhoef (2018) leggen in hun uitleg van gebiedsgebonden politiezorg naast de noodhulp, de nadruk op lokale opsporing en interventies om erger te voorkomen. Helsloot en collega's (2012) merken ten aanzien van het wijkwerk terecht op dat de functie van het gebiedsgebonden politiewerk zich vooral in samenwerking met andere partners afspeelt. Wanneer we deze contouren van het gebiedsgebonden politiewerk toepassen op het vraagstuk van gedigitaliseerde criminaliteit (waarbij zoals in voorgaande veelvuldig aan de orde is gesteld, deze vorm van criminaliteit intussen *veelvoorkomend* is te noemen) ontstaat het volgende overzicht van functies:

I. Vanuit o.a. *Intake & Service* lokaal ondersteunen bij (digitale) aangifte en melden van slachtofferschap van gedigitaliseerde criminaliteit
II. Vanuit het *wijkwerk* signaleren van lokaal actieve daders, dadergroepen en criminele netwerken die zich bezighouden met gedigitaliseerde criminaliteit en
III. Vanuit het *wijkwerk* en Intake & Service signaleren van lokaal slachtofferschap;
IV. Vanuit het *wijkwerk* met partnerorganisaties lokaal agenderen van het vraagstuk van gedigitaliseerde criminaliteit om tot een samenhangende, preventieve aanpak te komen;
V. Vanuit het *wijkwerk en interventie* ondersteunen van partnerorganisaties als de gemeenten, bij preventieve activiteiten ten aanzien van digitaal slachtoffer- en eventueel daderschap;
VI. Vanuit *veelvoorkomende criminaliteit* (aangestuurd door andere organisatieonderdelen (zoals bijvoorbeeld de cybercrimeteams, districtsrecherche en Landelijk Meldpunt Internet Oplichting)) opsporen van lokaal actieve daders of eventueel overzichtelijke dadergroepen waar het gaat om technisch relatief eenvoudig te onderzoeken zaken, die in vrij grote getale voorkomen (zoals geldezels);
VII. Vanuit i*nterventie* (aangestuurd door andere organisatieonderdelen) voeren van stopgesprekken met *first offenders* van relatief kleine zaken van gedigitaliseerde criminaliteit om verdere ontwikkeling in de gedigitaliseerde criminaliteit tegen te gaan;
VIII. Vanuit *opsporen* ondersteunen van de cybercrimeteams (en andere organisatieonderdelen) met advies en lokale kennis wanneer zij lokale daders, dadergroepen of criminele netwerken in zicht hebben en ondersteunen bij het aanhouden en verhoren van deze verdachten.

De rol van het gebiedsgebonden politiewerk in de aanpak van gedigitaliseerde criminaliteit zal met het oog op het voortbestaan van de klassieke criminaliteit en de lokale noodhulpfunctie, weliswaar bescheiden en complementair maar ook zeker betekenisvol kunnen zijn. Samengevat omvat de potentiële rol van het gebiedsgebonden politiewerk in de aanpak van gedigitaliseerde criminaliteit naar onze mening de volgende activiteiten per GGP-functie:

Service & Intake	Wijkwerk	Interventie	Veel voorkomende criminaliteit	Ondersteunen opsporing
• Signaleren van lokaal slachtofferschap	• Signaleren van lokaal actieve daders, dadergroepen en criminele netwerken; • Lokaal agenderen en tot integrale, preventieve aanpak komen	• Ondersteunen van partnerorganisaties bij preventieve activiteiten; • Voeren van stopgesprekken met *first offenders.*	• Opsporen van lokaal actieve daders of eventueel overzichtelijke dadergroepen.	• Andere organisatieonderdelen ondersteunen met advies en lokale kennis t.a.v. lokale daders, dadergroepen of criminele netwerken en ondersteunen bij het aanhouden en verhoren.

De uitvoering van lokale, digitale politietaken betreft in onze ogen een taak van het basisteam als geheel, in nauwe samenwerking met het district, de eenheid en landelijke diensten. Daarbij vervullen de leidinggevenden van de basisteams een cruciale rol. Geadviseerd wordt om capaciteit vrij te maken om in deze nieuwe, digitale politierol te groeien. Daarbij is het van belang om afstemming en samenwerking te zoeken met andere onderdelen binnen het district (zoals de districtsrecherche en andere basisteams) en de eenheid (zoals het cybercrimeteam). Toch moet naar onze mening de allereerste vervolgstap *niet op lokaal niveau* worden gezet. Hierover in de onderstaande beantwoording van de hoofdvraag meer.

In de gesprekken is ook een eventuele toekomstige rol van lokale noodhulp bij gedigitaliseerde criminaliteit ter sprake gekomen, opgevat als het uitbrengen van acuut handelingsadvies in een dreigende situatie van gedigitaliseerde criminaliteit, bijvoorbeeld wanneer verliezen van grote geldbedragen aan de orde kan zijn of bij digitale delicten waarbij anderszins sprake is van een hoge impact op het slachtoffer. Ook acute 'slachtofferhulp' kan in dit soort gevallen tot het werk gerekend worden. Hiervan zien wij in principe een meerwaarde, maar deze hoeft in onze ogen niet vanzelfsprekend op het lokale niveau of (in alle gevallen) bij de politie te worden ondergebracht. Dit kan ook en soms beter op afstand, meer gecentraliseerd plaatsvinden met het oog op de specialistische kennis en is afhankelijk van de toekomstige opvatting van de politietaak. Het is ook denkbaar dat de politie doorverwijst. Daarnaast nemen nu ook verzekeraars een rol op zich, zoals bijvoorbeeld in het geval van Cyberhulp van Univé verzekeringen.

7.4.6 Beantwoording van de hoofdvraag

Nu elk van de deelvragen is beantwoord, zullen wij nu de hoofdvraag van dit onderzoek beantwoorden. De hoofdvraag luidde: *'Hoe kan het Gebiedsgebonden Politiewerk in het district IJsselland in samenspel met andere (organisatie)onderdelen meer worden toegerust op het effectief aanpakken van gedigitaliseerde criminaliteit?'* Duidelijk is dat er door het district IJsselland stevig is ingezet op het opdoen van een eerste leereffect in de aanpak van gedigitaliseerde criminaliteit. Daarbij zijn al de nodige horden genomen: draagvlak organiseren, expertise vergroten en kennis verspreiden, informatie verzamelen en de informatiepositie verbeteren, verdachten in kaart brengen en verhoren. Het is duidelijk dat men in dit district op gedigitaliseerde criminaliteit in beweging is gekomen. Maar hoe kan dit *effectiever*?

Daarbij ligt de sleutel naar succes ligt zoals hierboven aangegeven naar onze mening niet in eerste

instantie op het lokale niveau (van dit district). Het op lokaal niveau goed kunnen invullen van de nieuwe, digitale politietaak kost tijd. En de benodigde investering past niet zomaar in de huidige situatie van de politie, waarin capaciteitsgebrek aan de orde van de dag is. Daarbij is in onze ogen de landelijke politiek aan zet. Het oppakken van de digitale politietaak, ook op lokaal niveau, moet niet de zoveelste extra taak worden, zonder aanvullend budget (vgl. Terpstra, Five & Salet, 2019). Ook de lokale politiek en het bevoegd gezag zullen een uitspraak moeten doen over de prioriteit die zij geven aan de aanpak van gedigitaliseerde criminaliteit. Tegelijkertijd lijken de initiatieven die in deze studie centraal stonden vrij uitzonderlijk te zijn. Dat is zorgelijk omdat we in een snel veranderende wereld leven waarin een meer adaptieve benadering nodig is, waarbij vroegtijdig op ontwikkelingen wordt ingespeeld, ook lokaal.

Niet alleen het basisteam van de politie, het district of de eenheid zijn aan zet. De aanpak van gedigitaliseerde criminaliteit is niet uitsluitend gebiedsgebonden en zelfs niet uitsluitend een politietaak. Er zal met name rond preventie samengewerkt moeten worden met een veelvoud aan veiligheidspartners en het maatschappelijke middenveld (vgl. Leukfeldt, Spithoven & Misana-ter Huurne, 2020; Spithoven, 2020). Daarbij liggen preventie en opsporing voor een belangrijk deel op eenheids- en landelijk niveau. Hierin voorzien is deels te beschouwen als een voorwaarde voor een effectieve aanpak lokaal. Maar de lokale kennis van de lokale samenleving bij de basisteams en districtsrecherche biedt in het effectief aanpakken van gedigitaliseerde criminaliteit wel degelijk een belangrijke meerwaarde, op diverse vlakken. Daarbij valt te denken aan preventie, signalering, prioritering en opsporing, maar ook aan meer praktische zaken als het aanhouden van verdachten, in beslag nemen van *devices* en administratieve afhandeling. Om de lokale bijdrage optimaal te kunnen benutten zullen eerst de volgende stappen moeten worden gerealiseerd:

1. Bewustwording van de noodzaak om gedigitaliseerde criminaliteit als politie, ook lokaal, te helpen voorkomen en aan te pakken op basis van de omvang en impact van slachtofferschap;
2. Het vergroten van praktische, technische en juridische kennis in de aanpak van gedigitaliseerde criminaliteit door middel van structurele kennisoverdracht aan zittend en nieuw personeel;
3. Prioriteit aan gedigitaliseerde criminaliteit toekennen op alle niveaus binnen de politieorganisatie in samenspraak met het OM en het lokaal bevoegd gezag;
4. Het organiseren en structureel behouden van capaciteit voor de aanpak van gedigitaliseerde criminaliteit;
5. Het lokaal actief krijgen van taakaccenthouders voor gedigitaliseerde criminaliteit of digitale wijkagenten om een voortrekkersfunctie binnen de basisteams en een lokaal aanspreekpunt voor andere organisatieonderdelen te hebben.

Ook ontbeert er op landelijk niveau een gedegen en toegankelijke informatiehuishouding. Onder meer de cybercrimeteams – die voor alle duidelijkheid bijzonder goed werk verrichten – werken momenteel met veel praktische noodgrepen. Om optimaal effect te hebben op gedigitaliseerde criminaliteit zou de politie idealiter moeten inzetten, op basis van een geoptimaliseerde informatiepositie en -huishouding, op ten eerste de preventie van verder slachtofferschap, grotendeels via partnerorganisaties. Ten tweede is inzet nodig op landelijke regie van de repressieve activiteiten door politie en justitie. We zien daar een belangrijke rol weggelegd voor de cybercrimeteams, elk met hun eigen inhoudelijke accenten.

Het cybercrimeteam Oost-Nederland is ten tijde van dit onderzoek een veelbelovende werkwijze opgestart om in te spelen op de specifieke kenmerken van gedigitaliseerde criminaliteit. Allereerst heeft het team initiatief genomen (uitsluitend gestandaardiseerde, digitale) aangiften te verzamelen en analyseren. Vervolgens werden gegevens gevorderd bij derden, o.a. op basis van verkregen bankrekeningnummers. Daarna werden verschillende aangiften gebundeld, indien deze in de richting van dezelfde verdachte wezen. De ontwikkelde aanpak stelde het cybercrimeteam in staat om de gebundelde aangiften als ‘werkpakket’ bij de districten uit te zetten waar de verdachten woonachtig zijn. Daarbij was doelstelling de criminele netwerken te kunnen overzien en coördinerend te opereren bij het oprollen van de netwerkstructuren, in samenwerking met meerdere politiedistricten en basisteams.

Na verloop van tijd oordeelde het OM dat de gehanteerde juridische grondslag niet (langer) voldeed. Een soortgelijke werkwijze wordt door LMIo toegepast op een andere juridische grondslag. Samen met het OM zal naar een effectieve en juridisch houdbare oplossing gezocht moeten worden, zodat bundelen en coördineren van zaken landelijk (evt. door een cybercrimeteam) doorgang kan vinden.

7.5 Faciliteren van de lokale, digitale stap voorwaarts

Om als gebiedsgebonden politie op lokaal niveau een stap voorwaarts te kunnen zetten in de aanpak van gedigitaliseerde criminaliteit doen wij de volgende, samenhangende en meer gedetailleerde aanbevelingen.

7.5.1 Overall aanbevelingen: prioriteit, capaciteit en samenwerking

Wij zien naast de noodzaak voor prioritering[7] van gedigitaliseerde criminaliteit, evenals Jansen et al. (2020) - een dringende noodzaak om te investeren in bewustzijn en kennis onder politiemedewerkers ten aanzien van de omvang en maatschappelijke impact van gedigitaliseerde criminaliteit. Op elk van de lagen van de politieorganisatie moeten medewerkers ervan worden doordrongen dat de gedigitaliseerde criminaliteit 'erbij is gekomen' en op termijn onderdeel zal zijn van het dagelijks politiewerk. Ook moet er in onze ogen structurele capaciteit gericht op de aanpak van gedigitaliseerde criminaliteit worden vrijgemaakt en nieuw personeel worden aangenomen met specifieke interesse en kennis van gedigitaliseerde criminaliteit. Dit hoeven geen klassiek opgeleide politiemensen te zijn, het kunnen ook specialisten zijn die geen functie op straat vervullen. Daarnaast ligt er een noodzaak om de samenwerking over de districts- en eenheidsgrenzen te stimuleren. Zorg daarbij voor vaste aanspreekpunten bij partnerorganisaties.

7.5.2 Aanbevelingen op landelijk niveau: online aangifte en versterking van informatiehuishouding

Om meer effect op lokaal niveau te kunnen sorteren zien wij een noodzaak om allereerst op landelijk niveau aan de slag te gaan. Stimuleer het doen van internetaangifte onder slachtoffers van gedigitaliseerde criminaliteit. Werk daarbij met sterke voorrang aan een verbeterde, landelijke informatiehuishouding ten aanzien van gedigitaliseerde criminaliteit op basis van een aangescherpte registratiediscipline en een eenduidige extractie van gedigitaliseerde criminaliteit uit aangiften om de ontwikkeling van dader- en slachtofferschap nauwgezet te kunnen volgen en zo een antwoord op de wendbaarheid van cybercriminelen te kunnen vormen. Versterk hierbij tevens de samenwerking met andere organisaties die ook signalen over deze ontwikkeling ontvangen zoals de Fraudehelpdesk, banken en verzekeraars. Maak daarnaast ook landelijke werkafspraken over het uitwisselen van gedigitaliseerde criminaliteitszaken tussen eenheden en teams in het land.

7.5.3 Aanbevelingen op lokaal niveau: focus op de lokale facilitators

Zorg allereerst ook lokaal voor prioriteitsstelling op gedigitaliseerde criminaliteit in samenspel met de burgemeester en het Openbaar Ministerie. Draag als lokale politie actief bij aan lokale, preventieve interventies en enthousiasmeer de gemeente om hierin het voortouw te nemen. Heb in de lokale, repressieve aanpak van gedigitaliseerde criminaliteit vooral aandacht voor de lokaal actieve daders en dadergroepen. Richt je daarbij op de onderste lagen (bijv. de geldezels, ronselaars e.d.). Sein daarbij op tijd de districtsrecherche in dat zij mogelijk informatie uit deze zaken omtrent de facilitators kunnen gebruiken om de initiators op te sporen. Zoek dus actief de afstemming met collega's van andere onderdelen en eenheden. Gebruik vooral de kracht van de lokale kennis van gebiedsgebonden politiemedewerkers om zicht te houden op de lokale ontwikkelingen onder bekende daders en dadergroepen die richting gedigitaliseerde criminaliteit opschuiven of daar al mee bezig zijn.

7.5.4 Aanbevelingen op eenheids- niveau: uitrafelen van lokale netwerken

7 Onder meer in het selectiviteitskader en de prioriteitsstelling van lokale driehoeksoverleggen.

Waar de basisteams zich kunnen richten op de facilitators van gedigitaliseerde criminaliteit - de geldezels en ronselaars - kunnen de districtsrecherche en de cybercrimeteams zich richten op de opsporing van de initiators: de oplichters en fraudeurs. Bevorder daarbij in toenemende mate de samenwerking rondom gedigitaliseerde criminaliteit tussen de basisteams, de districtsrecherche en de cybercrimeteams en vul deze aan met de kennis en ervaring van andere teams als de DDR en DRIO. Werk hierbij op eenheidsniveau aan een uitgewerkte strategie voor de aanpak van gedigitaliseerde criminaliteit. Richt daarbij de analisten van de DRIO bij een verbeterde, landelijke informatiehuishouding ten aanzien van gedigitaliseerde criminaliteit op de evolutie van regionaal dader- en slachtofferschap en laat hen de informatiegestuurde aanpak van facilitators en initiators aanjagen.

7.6 Aanbevelingen voor vervolgonderzoek

Afsluitend doen wij de volgende aanbevelingen voor vervolgonderzoek:

1. De rol van Gebiedsgebonden Politiewerk in de aanpak van gedigitaliseerde criminaliteit is nog volop in ontwikkeling. Er zijn aanwijzingen dat lokale kennis kan bijdragen aan versterking van de aanpak. Breng deze ontwikkelingen in kaart, leer ervan en stimuleer innovatie in de lokale aanpak.

2. De overschakeling van de wijk naar het web vindt al plaats, maar met welk tempo is op basis van dit onderzoek niet aan te geven. Wat ons betreft is dit een belangrijke vraag die nader onderzoek verdient, evenals de vraag of de aanpassingen in de werkwijzen bij de politie snel genoeg gaan en effect sorteren.

3. Onderzoek hoe de politieorganisatie als geheel kan investeren in de informatiepositie- en huishouding ten aanzien van (onder meer) gedigitaliseerde criminaliteit en hoe dit kan leiden tot een meer effectieve, (landelijk) gecoördineerde aanpak, waarbij met partnerorganisaties kan worden ingezet op preventie van slachtofferschap.

4. Onderzoek de praktische, technische en juridische kennis van politiemedewerkers, benodigd voor de aanpak van gedigitaliseerde criminaliteit en breng het verschil in kaart met de minimaal benodigde kennis waar Jansen et al. (2020) een mooie basis voor hebben gelegd. Wij sluiten ons aan bij hun oproep om een bredere visie op het opleiden van zittend personeel ten aanzien van gedigitaliseerde criminaliteit en de aanpak daarvan.

5. Onderzoek hoe gebiedsgebonden politiemedewerkers in samenwerking met lokale partnerorganisaties optimaal invulling kunnen geven aan de preventie van slachtofferschap en daderschap van gedigitaliseerde criminaliteit en aan het bestrijden van lokaal actieve daders, dadergroepen en criminele netwerken. Besteed daarbij, behalve aan gedigitaliseerde vormen van bedrog en diefstal ook aandacht aan gedigitaliseerde vormen van geweld.

Geraadpleegde literatuur

- Ahmad, T. (2020). *Corona virus (covid-19) pandemic and work from home: Challenges of cybercriminaliteits and cybersecurity.* Available at SSRN 3568830: https://dx.doi.org/10.2139/ssrn.3568830
- AvroTros (2020). *Opvallende stijging aangiftes van online fraude tijdens coronacrisis: 'Vooral kwetsbaren en ouderen zijn slachtoffer'* (d.d. 29-04-2020), via: https://eenvandaag.avrotros.nl/item/opvallende-stijging-aangiftes-van-online-fraude-tijdens-coronacrisis-vooral-kwetsbaren-en-ouderen/
- Baarda, B. et al. (2013). *Basisboek kwalitatief onderzoek.* Noordhoff Uitgevers.
- Babbie, E. (1998). *The practice of social research.* Wadsworth Publishing Company.
- Barbour, R. (2008). *Introducing Qualitative Research. A student Guide to the Craft of Doing Qualitative Research.* Sage Publication.
- Berding, J. & Witte, T. (2013). *Praktijkonderzoek op niveau. Inspelen op onderzoeksdilemma's bij sociale studies.* Coutinho.
- Beyens, K. & Tournel, H. (2009). Mijnwerkers of ontdekkingsreizigers? Het kwalitatieve interview. In: Decorte & Zaitch (eds.) *Kwalitatieve methoden en technieken in de criminologie,* 196-228.
- Boekhoorn, P. (2020). *De aanpak van cybercrime door regionale eenheden van de politie. Van intake van cybercrime naar opsporing en vervolging.* Sdu uitgevers.
- Broersma, M. (2020). *WhatsApp-oplichters uit Deventer maakten tienduizenden euro's buit en moeten nu jarenlang de cel in,* via: https://www.destentor.nl/deventer/jong-kwetsbaar-en-gebruikt-tientallen-verdachten-aangehouden-voor-whatsapp-fraude-in-deventer~aa529ac0/
- Buil-Gil, D., et al. (2020). Cybercriminaliteit and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies* 23.sup1 (2021): S47-S59. Via: https://doi.org/10.1080/14616696.2020.1804973
- CBS (2020). *Minder traditionele criminaliteit, meer cybercrime.* Via: Minder traditionele criminaliteit, meer cybercrime (cbs.nl).
- CBS (z.d.). *Cybercrime achterhalen in aangiften.* Via: https://www.cbs.nl/nl-nl/over-ons/innovatie/project/cybercriminaliteit-achterhalen-in-aangiften.
- Cohen, L. E.; Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review.* 44 (4): 588–608.
- Collier, B., Horgan, S., Jones, R., & Shepherd, L. A. (2020). *The implications of the covid-19 pandemic for cybercriminaliteit policing in Scotland: a rapid review of the evidence and future considerations.* Scottish Institute for Policing Research.
- De Lange, R., Schuman, H. & Montesano Montessiori, N.(2011). *Praktijkgericht onderzoek voor reflectieve professionals.* Garant.
- De Vries, H. & Hensen, M. (2018). *Podium voor goed politiewerk. Ontwikkelagenda GGP.* Nationale Politie.
- Deloitte (2017). *Cyber Value at Risk in The Netherlands 2017.* Deloitte.
- Deloitte (2020). *Cyber crime – the risks of working from home.* Via: https://www2.deloitte.com/ch/en/pages/risk/articles/covid-19-cyber-crime-working-from-home.html
- Financial Times (2020). *Why Covid-19 is a gift for cyber criminals* (d.d. 15-07-2020) Via: https://www.ft.com/content/935a9004-0aa5-47a2-897a-2fe173116cc9
- Fontanilla, M. V. (2020). Cybercriminaliteit pandemic. *Eubios Journal of Asian and International Bioethics*, 30(4), 161-165.
- Friese, S. (2014). *Qualitative data analysis with ATLAS.ti.* SAGE.
- Hadnagy, C.J. (2018). *Social Engineering: The Science of Human Hacking.* Wiley.

- Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercriminaliteit in America amid COVID-19: The initial results from a natural experiment. *American Journal of Criminal Justice,* 45(4), 546-562. https://doi.org/10.1007/s12103-020-09534-4
- Helsloot, I., Groenendaal, J. &Warners, E.C. (2012). *Politie in de netwerksamenleving. De opbrengst van de netwerkfunctie voor de kerntaken opsporing en handhaving openbare orde en de sturing hierop in de gebiedsgebonden politiezorg.* Politie en Wetenschap.
- Holt, T.J. & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, 35(1), 20-40.
- Horgan, S., Collier, B., Jones, R., & Shepherd, L. (2021). Re-territorialising the policing of cybercriminaliteit in the post-COVID-19 era: towards a new vision of local democratic cyber policing. *Journal of Criminal Psychology.* https://doi.org/10.1108/JCP-08-2020-0034
- Jansen, J. et al. (2020). *Level-Up! Kennis voor politiewerk in een digitale samenleving.* NHL Stenden / Politieacademie.
- Kayser, C. (2020). *Cybercrime Through Social Engineering: The New Global Crisis.* Library And Archives Canada.
- Klaassen, B. (2020). *Jong, kwetsbaar en gebruikt: tientallen verdachten aangehouden voor WhatsApp-fraude in Deventer,* via: https://www.destentor.nl/deventer/jong-kwetsbaar-en-gebruikt-tientallen-verdachten-aangehouden-voor-whatsapp-fraude-in-deventer~aa529ac0/
- Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security,* 102248. https://doi.org/10.1016/j.cose.2021.102248
- Leukfeldt, E.R. (2016). *Cybercriminal networks: Origin, growth and criminal capabilities.* Eleven International Publishers.
- Leukfeldt, E.R. (2018). *De 'human' factor in cybersecurity: Intreerede.* Den Haag: Haagse Hogeschool.
- Leukfeldt, E. R., Spithoven, R. & Misana-ter Huurne, E. F. J. (2020). De lokale aanpak van cybercrime. Risicocommunicatie als antwoord op een grenzeloos vraagstuk. In C. de Poot et al. (Eds.), *Politie en cybercriminaliteit* (pp. 203-222). Gompel&Scavina.
- Migchelbrink, F. (2013). *Handboek praktijkgericht onderzoek.* SWP.
- T. Meurs & Kreulen, B.J. (2017). *De uitdagingen voor gebiedsgebonden politiezorg,* Justitiële Verkenningen 2017-4, p. 64-80.
- Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing Cybercriminaliteit Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports,* 23(4), 1-9. https://doi.org/10.1007/s11920-021-01228-w
- Monterie, A. (2020). *Bijna 7 procent bedrijven last van corona-cybercrime.* Via: https://www.computable.nl/artikel/nieuws/security/6947773/250449/bijna-7-procent-bedrijven-last-van-corona-cybercrime.html
- Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercriminaliteit. *European Journal of Information Systems,* 29(3), 306-321. https://doi.org/10.1080/0960085X.2020.1771222
- Nationale Politie (2020). *Cybercriminelen misbruiken maatregelen rondom corona* (d.d. 17-03-2020). Via: https://www.politie.nl/nieuws/2020/maart/17/cybercriminelen-misbruiken-maatregelen-rondom-corona.html
- Politie Oost-Nederland (2019). *Veranderingen in criminaliteit. Een verkenning van de oorzaken in Oost-Nederland.* Politie Oost-Nederland.
- Politieacademie (2019). *Strategische onderzoeksagenda voor de Politie 2019 – 2022*. Politieacademie.
- RTV Oost (2021). *WhatsApp-fraude in Deventer: politie verricht 24 aanhoudingen,* via: https://www.rtvoost.nl/nieuws/330011/WhatsApp-fraude-in-Deventer-politie-verricht-24-aanhoudingen

- Saldaña, J. (2012). *The Coding Manual for Qualitative Researchers.* Second edition. SAGE Publications.
- Spithoven, R. (2020). *Verbonden risico's. Maatschappelijke veiligheid in de black box society.* Boom Criminologie.
- Steinmetz, K., Goe, R. & Pimentel, A. (2020). On social engineering. In: E.R. Leukfeldt & T.J. Holt (eds.) *The Human Factor of Cybercrime.* Routledge, pp.173-193.
- Struiksma, N., de Vey Mestdagh, C.N.J. en Winter, H.B. (2012). *De organisatie van de opsporing van cybercrime door de Nederlandse politie.* Politie en Wetenschap.
- Terpstra, J. & & Mein, A. (2010). De positie van de gemeente in de veiligheidszorg. Een inleiding. *Tijdschrift voor Veiligheid,* 9(3), 3-8.
- Terpstra, J. et al. (2016). *Basisteams in de Nationale Politie. Organisatie, taakuitvoering en gebiedsgebonden werk*. Politie en wetenschap.
- Terpstra, J. (2018). *Gebiedsgebonden politie: veranderingen en uitdagingen.* Via: https://www.websitevoordepolitie.nl/gebiedsgebonden-politie-veranderingen-en-uitdagingen/
- Terpstra, J., Fyfe, N. R., & Salet, R. (2019). The Abstract Police: A conceptual exploration of unintended changes of police organisations. *The Police Journal,* 92(4), 339-359.
- Torre, E. van der , Tops, P. & Van Valkenhoef, J. (2018). *Gebiedsgebonden politie: hervorming is broodnodig.* Politieacademie.
- Tran, C. (2020). Recommendations for ordinary users from mitigating phishing and cybercrime risks during COVID-19 pandemic. arXiv: 2006.11929 v1.
- Van 't Hoff-de Goede, S. & Leukfeldt, E.R. (2020). *WhatsApp-fraude in Nederland.* Via: https://www.dehaagsehogeschool.nl/docs/default-source/default-document-library/w2101-0071-infographic-what's-app-fraude-digi.pdf?sfvrsn=3ada4f88_0.
- Voskuil, K. (2020). 'Oplichters maken misbruik van coronavirus'. In: *Algemeen Dagblad,* 1 april 2020.
- Vu, A. V., Hughes, J., Pete, I., Collier, B., Chua, Y. T., Shumailov, I., & Hutchings, A. (2020). Turning Up the Dial: the Evolution of a Cybercriminaliteit Market Through Set-up, Stable, and COVID-19 Eras. In Proceedings of the ACM Internet Measurement Conference (pp. 551-566). https://doi.org/10.1145/3419394.3423636
- Wagen, W. van der, et al. (2019). *Cyberdaders: uniek profiel, unieke aanpak? Een onderzoek naar kenmerken van en passende interventies voor daders van cybercriminaliteit in enge zin.* WODC.
- Weiss, R.S. (1995). *Learning from strangers. The art and methods of qualitative interview studies.* Free Press
- World Economic Forum (2019). *The global risks report 2019 . World Economic Forum.* Retrieved 25 April, 2020 from https://www.weforum.org/reports/the-global-risks-report-2019
- Yar, M. (2005). The Novelty of 'Cybercrime'. An Assessment in Light of Routine Activity Theory. *European Journal of Criminology,* 2(4), 407-427.

Bijlage

Overzicht geïnterviewde functionarissen

Bijlage

Overzicht geïnterviewde functionarissen

Er zijn twee 'brainstorms' gehouden met hoofdzakelijk medewerkers van Basisteam IJsselland-Zuid (15/12/2020) en van Basisteam Vechtdal (21/1/2021); o.a. operationeel expert OCP, intake & service medewerkers, GGP- en noodhulpmedewerkers. Hieraan werd ook deelgenomen door rechercheurs van het cybercrimeteam Oost-Nederland en een teamchef van een basisteam.

In de periode september 2020 – maart 2021 zijn de volgende functionarissen geïnterviewd voor dit onderzoek:

District IJsselland:
- Operationeel Expert basisteam IJsselland-Zuid;
- Operationeel Expert van het Digitaal Flexteam;
- 4 basisteammedewerkers noodhulp/GGP, tevens medewerker van het Digitaal Flexteam;
- 1 basisteammedewerker Intake & Service, tevens medewerker van het Digitaal Flexteam;
- 1 basisteammedewerker VVC;
- 4 rechercheurs Districtsrecherche;
- 3 leidinggevenden Districtsrecherche;
- Districtsleiding.

Cybercrimeteam eenheid Oost-Nederland
- 2 rechercheurs;
- 1 projectleider.

Landelijke dienst:
- 1 medewerker Team Digitale Opsporing.

Om gedurende het onderzoek gerezen vragen te beantwoorden zijn in de periode juni-juli 2021 vijf aanvullende interviews gehouden met sleutelfiguren die zich binnen de politie, voornamelijk op landelijk niveau bezighouden met vraagstukken rond gedigitaliseerde criminaliteit. Het betreft onder meer functionarissen van het Landelijk Meldpunt Internetoplichting (LMIo) en het cybercrimeteam Oost-Nederland en een extern adviseur.

www.politie.nl

« waakzaam en dienstbaar »

P-21-0904