Scriptie

De aanpak van gedigitaliseerde criminaliteit binnen het basisteam

Een onderzoek naar het leveren van een bijdrage aan de aanpak van gedigitaliseerde criminaliteit binnen het basisteam Zeist-Bunnik-Leusden-Woudenberg

Naam: Patrick Kleijer

Studentnummer: 352558

Begeleider: Nikita Rombouts

Tweede beoordelaar: Wouter Stol

In opdracht van: David Meijerink en Priscilla de Vries

Politieacademie: BaCI1745 – Profileringsfase

Datum: 27 oktober 2020

Versie: 1.0

Voorwoord

Voor u ligt mijn bachelor thesis *'De aanpak van gedigitaliseerde criminaliteit binnen het basisteam'* die ik heb geschreven ter afronding van de compacte en zeer intensieve opleiding tot Politiekundige. Afronding, niet alleen van het schrijven van een thesis, maar ook de afronding van drie bewogen jaren. Drie bewogen jaren die zijn begonnen in November van het jaar 2017. Een periode waarin ik eindelijk de stap heb durven zetten om mijn droom van een baan binnen de politie te gaan realiseren. Ik kijk dan ook terug op een periode waarin ik veel geleerd over de organisatie, maar ook over mezelf. Ik ben trots op de ontwikkelingen die ik heb doorgemaakt en ik kijk uit naar mijn volgende stap in mijn politiecarrière. Ook kijk ik terug op een periode waarin ik veel nieuwe mensen heb mogen leren kennen. Mensen die ik nu mag beschouwen als vrienden, die ook hebben bijgedragen aan mijn ontwikkeling en me er soms doorheen sleepten wanneer dit nodig was.

Ik wil hier ook een aantal andere mensen bedanken. Mensen die hun steentje hebben bijgedragen aan de totstandkoming van deze thesis. Allereerst gaat mijn dank uit naar mijn scriptiebegeleider, Nikita Rombouts. Zij was op elk moment te bereiken voor feedback. Haar kritische blik heeft een belangrijke bijdrage geleverd voor de totstandkoming van dit eindproduct. Ook wil ik David Meijerink en Priscilla de Vries bedanken. Als opdrachtgevers hebben zij mij een kans geboden om een interessant onderwerp te onderzoeken. Ook wil ik de betrokken collega's bedanken voor het delen van hun visie en hun bereidheid tot meedenken omtrent het onderwerp van deze thesis. Collega's die mij ook voorafgaand aan het schrijven van deze thesis hebben meegenomen en mij veel hebben geleerd over de inhoud van het politiewerk. Ik hoop dan ook dat ik met deze thesis zowel de opdrachtgevers als de collega's handvatten heb kunnen bieden om de aanpak van gedigitaliseerde criminaliteit binnen het basisteam handen en voeten te geven.

Ik wens u veel leesplezier!

Patrick Kleijer

Ede, 27 oktober 2020

Inhoud

Hoofdstuk 1: Inleiding

1.1 Inleiding

Dit onderzoek richt zich op de aanpak van gedigitaliseerde criminaliteit binnen het basisteam Zeist-Bunnik-Leusden-Woudenberg (hierna: basisteam ZBLW). Het basisteam heeft namelijk stappen te zetten op het gebied van gedigitaliseerde criminaliteit.

In de huidige samenleving zijn woorden als 'internet', 'computer', 'smartphone' en 'e-mail' niet meer weg te denken. Razendsnelle digitale ontwikkelingen volgen elkaar op en in een mum van tijd zijn tal van handelingen, die vroeger handmatig en zonder digitaal middel werden uitgevoerd, inmiddels allemaal digitaal uit te voeren. Online bankieren, boodschappen, kleding of meubels bestellen. Allemaal uit te voeren zonder ook maar één stap buiten de deur te zetten. Criminelen maken volop gebruik van de mogelijkheden die digitalisering biedt.

Wat in de literatuur onder cybercriminaliteit wordt verstaan, is nog niet zo makkelijk in een eenduidige definitie te vatten. In de literatuur wordt gebruik gemaakt van uiteenlopende definities rondom (varianten van) cybercriminaliteit. In dit onderzoek wordt onder cybercriminaliteit verstaan: Strafbare feiten gepleegd met gebruikmaking van elektronische communicatienetwerken of informatiesystemen ofwel tegen dergelijke netwerken en systemen (Europese Commissie 2007, p.2.). Enerzijds zijn er dus delicten gericht op ICT (cybercrime), bijvoorbeeld hacken of het platleggen van websites of databases. Anderzijds zijn er delicten waarbij ICT van wezenlijk belang is voor het uitvoeren van het delict (gedigitaliseerde criminaliteit), bijvoorbeeld fraude of stalking via internet (Leukfeldt, et al., 2017).

Bij cybercrime in brede zin, ook wel gedigitaliseerde criminaliteit genoemd, gaat het om traditionele delicten die met computers worden gepleegd. Het kan hierbij gaan om vermogensdelicten, zoals oplichting via internet, om onlinebedreiging, maar ook om cyberspionage of het verspreiden van kinderporno. Bij cybercrime in enge zin, ook wel gewoon 'cybercrime' genoemd, moeten we denken aan criminaliteit waarbij de computer of software zelf het doelwit is van criminaliteit, zoals bij DDoS-aanvallen of hacken (Erp, et al., 2013).

Hoewel deze twee vormen van cybercriminaliteit veel van alle computer gerelateerde criminaliteit omvatten, heeft de inzet van hoogwaardige technologie ook tot meer diffuse vormen van criminaliteit geleid, waarbij computers of het internet wel een rol spelen, maar vermengd zijn met traditionele criminele (voorbereidings-) handelingen. Een voorbeeld hiervan is drugshandel via internet, waarbij productie en transport van drugs op traditionele manieren kunnen plaatsvinden, maar het bij elkaar brengen van vraag en aanbod en de transactie tussen deze partijen via internet plaatsvinden (Vijlbrief, 2012). De driedeling van

Parker beschrijft deze delicten als zogenaamde computer-relevante delicten. Hierbij zijn computers, computernetwerken of gegevens op de een of andere manier relevant als omgevingsfactoren en fungeren computers of gegevens als een niet-substantieel hulpmiddel (Koops, 2014).

Het Centraal Bureau voor Statistieken heeft in zijn Veiligheidsmonitor 2019 (2020) geconcludeerd dat er in 2019 13% van de Nederlanders slachtoffer is geworden van cybercriminaliteit. Dit is een lichte stijging ten opzichte van de eerder onderzochte resultaten in 2017 (11%) en 2012 (12%).

Cybercriminaliteit is de afgelopen jaren in toenemende mate aanwezig in het dagelijks leven van mensen. Ruim een kwart van de Nederlandse bedrijven tot 50 medewerkers is slachtoffer van cybercriminaliteit: 28,5 procent van het Nederlandse MKB en 27,9 procent van de ZZP'ers is in het jaar 2014 geconfronteerd met een of meer vormen van cybercriminaliteit. De meest voorkomende vormen waarmee ondernemers worden geconfronteerd zijn malware, e-fraude, phishing en hacken. Uit eerder onderzoek onder burgers en grotere bedrijven blijkt ook dat deze delicten het vaakst voorkomen. De meest voorkomende vormen van cybercriminaliteit raken dus niet alleen het MKB en ZZP'ers, maar kunnen worden getypeerd als een maatschappij breed verschijnsel (Veenstra, et al., 2015).

Hierdoor moeten ook politie en justitie een gerichte aanpak ontwikkelen om deze groei tegen te gaan. Politie en justitie hebben nu echter geen goede informatiepositie, omdat de aangiftebereidheid bij cybercriminaliteit erg laag is. Uit onderzoek naar zelf gerapporteerd slachtofferschap van cybercriminaliteit blijkt dat van alle respondenten die aangeven slachtoffer te zijn geworden, slechts 8% aangifte doet bij de politie (CBS, 2020). Dit percentage verschilt wel tussen verschillende cybercriminaliteitsdelicten: van koop- en verkoopfraude (19,5%) werd bijvoorbeeld aanzienlijk vaker aangifte gedaan dan van hacken (3%) (CBS, 2019).

Doordat de digitalisering niet alleen zorgt voor 'nieuwe' delicten, maar ook een nieuwe dynamiek geeft aan 'oude' delicten, heeft digitalisering consequenties voor het gehele spectrum van criminaliteit. Dit roept allerlei vragen op. Hebben we bijvoorbeeld te maken met 'oude' daders op een nieuw werk- terrein, of gaat het om een nieuw type dader met dito kenmerken en motieven? (Leukfeldt, et al., 2017).

Vaststaat dat de digitalisering een serieus criminaliteitsprobleem met zich mee heeft gebracht en dat politie en justitie (nog) niet goed weten hoe daarmee om te gaan. Misschien is het meest basale probleem nog wel dat mensen in de zogenaamde cyberspace niet zo eenvoudig zijn te identificeren en te lokaliseren: niet voor andere burgers, maar ook niet voor de overheid. (Erp, et al., 2013).

Het Ministerie van Veiligheid en Justitie heeft in samenwerking met de Nationale Politie in de Uitwerking Veiligheidsagenda 2019-2022 (2018) de aanpak van cybercriminaliteit als landelijke beleidsprioriteit benoemd. De Nationale Politie (2020) stelt dat cybercriminaliteit goed is voor ruim 50% van alle delicten. Het is dus naast gemeentes, bedrijven en burgers, ook voor de Nationale Politie van belang mee te gaan in de digitale ontwikkelingen om daders van deze delicten te kunnen aanpakken en cybercriminaliteit te kunnen voorkomen. Mede hierdoor is cybercriminaliteit, samen met ondermijning, ook in district Midden-Nederland benoemd tot prioriteit.

1.2 Aanleiding

De prioritering op landelijk en regionaal niveau bepaalt de wijze waarop de politie dient om te gaan met het bestrijden van cybercrime en gedigitaliseerde criminaliteit. Basisteams dienen de gestelde landelijke en regionale prioriteiten en speerpunten te vertalen naar concrete handelingen om de bestrijding van cybercrime en gedigitaliseerde criminaliteit te realiseren. Dit onderzoek richt zich specifiek op basisteam Zeist-Bunnik-Leusden-Woudenberg (hierna: basisteam ZBLW), onderdeel van district Midden-Nederland.

Sinds 2018 zien we in district Midden-Nederland een flinke stijging van het aantal zaken omtrent cybercrime en gedigitaliseerde criminaliteit. Voor een zo goed mogelijke interpretatie van de stijging, behoeven de cijfers enige vorm van toelichting: Er zijn binnen district Midden-Nederland cijfers bekend van twee ‘soorten’ criminaliteit, namelijk ‘cybercrime’ en ‘fraude met online handel’. Cybercrime wordt in het politiesysteem geregistreerd onder een specifieke feitcode (F90). Er worden geen specifieke cijfers weergegeven met betrekking tot gedigitaliseerde criminaliteit. Een uitzondering hierop is het delict ‘fraude met online handel’. Dit delict is echter slechts een klein deel van alle delicten die vallen onder gedigitaliseerde criminaliteit. Veel andere vormen worden in het politiesysteem geregistreerd onder de feitcode van het traditionele delict. Oplichting via marktplaats is bijvoorbeeld wel degelijk een gedigitaliseerd criminaliteitsdelict, maar valt binnen de politiesystemen onder de noemer ‘oplichting’ en wordt het dus ook als zodanig geregistreerd. Het aantal zaken van gedigitaliseerde criminaliteit zal binnen het district en binnen het basisteam ZBLW daarom hoger liggen dan alleen de cijfers van ‘fraude met online handel’ doen aangeven.

Wat zijn dan die cijfers? In tabel 1.1 zijn de geregistreerde cijfers te vinden van de geregistreerde delicten omtrent ‘cybercrime’ en ‘fraude met online handel’ binnen eenheid Midden-Nederland.

Tabel 1.1 Cijfers Eenheid Midden-Nederland

Delict	Geregistreerde misdrijven 2018	Geregistreerde misdrijven 2019	Geregistreerde misdrijven 2020	% verschil t.o.v. 2018	% verschil t.o.v. 2019
Cybercrime	221	436	1021	362%	134%
Fraude met online handel	3421	4249	5019	46%	18%

Waar er in 2018 binnen eenheid Midden-Nederland 221 zaken met betrekking tot cybercrime en 3421 zaken met betrekking tot fraude met online handel werden geregistreerd, waren dit er in 2019 al respectievelijk 436 en 4249. In 2020 zijn dit er op 1 augustus al 1021 (stijging van 134% ten opzichte van heel 2019) voor cybercrime en 5019 (18% stijging ten opzichte van 2019) voor fraude met online handel.

Tabel 1.2 geeft de specifieke cijfers weer van de geregistreerde delicten omtrent 'cybercrime' en 'fraude met online handel' binnen basisteam ZBLW.

Tabel 1.2 Cijfers **Basisteam ZBLW**

Delict	Geregistreerde misdrijven 2018	Geregistreerde misdrijven 2019	Geregistreerde misdrijven 2020	% verschil t.o.v. 2018	% verschil t.o.v. 2019
Cybercrime	10	14	95	850%	578%
Fraude met online handel	197	226	289	46%	27%

Specifiek voor basisteam ZBLW gold ten opzichte van 2018 in 2020 een stijging van 850% van het aantal zaken met betrekking tot cybercrime en een stijging van 46% van het aantal zaken met betrekking tot fraude met online handel.

Zoals de cijfers laten zien, stijgt het aantal zaken omtrent cybercrime en gedigitaliseerde criminaliteit binnen de eenheid Midden-Nederland. Het antwoord van de politie op de stijging van cybercrime en gedigitaliseerde criminaliteit blijft echter uit. Het ophelderingspercentage van de zaken met betrekking tot cybercrime en fraude met online handel ligt op districtsniveau in 2020 op 1,7% en in basisteam ZBLW ligt dit ophelderingspercentage zelfs op 0,0%. Hoewel deze cijfers niet de gehele gedigitaliseerde criminaliteit omvatten, geeft het wel degelijk aan dat er op dit gebied nog een flinke inhaalslag te maken valt en dat een onderzoek naar de aanpak van cybercrime en gedigitaliseerde criminaliteit binnen basisteam ZBLW geen ondienstige zaak is.

Hoewel er in de aanpak van cybercrime een (kleine) rol voor het basisteam is weggelegd, zoals preventie en signalering, wordt cybercrime voornamelijk opgespoord en aangepakt door specialistische (recherche)teams van de politie, in

samenwerking met externe partijen. Voorbeelden van dergelijke teams zijn het landelijke Team High Tech Crimes (THTC) en het Electronic Task Force (ECTF) en de regionale Cybercrimeteams (Nationale Politie, z.d.). De opsporing en de aanpak van cybercrime vergen namelijk specialistische digitale kennis en opsporingsmethoden die (nog) niet aanwezig zijn binnen elk basisteam. Echter valt niet elk cybercrime-delict buiten de verantwoordelijkheid van het basisteam. Het delict 'hacken' valt namelijk wel onder cybercrime (in enge zin) en vergt dus digitale expertise om te kunnen worden aangepakt, maar is volgens het CBS (2019) het meest voorkomende delict. In 2019 werd 5,5% van de Nederlandse bevolking slachtoffer van (een vorm van) hacken. Dit percentage ligt hoger dan bijvoorbeeld fietsendiefstal (2,9% in 2019). Dit houdt in dat deze vorm van cybercrime valt onder de noemer 'veel voorkomende criminaliteit' en dus wel degelijk op het bordje van de afdeling VVC komt. De vraag is echter of de collega's van de VVC voldoende kennis en/of expertise bezitten om deze vorm van cybercrime het hoofd te kunnen bieden.

De aanpak van gedigitaliseerde criminaliteit is niet per definitie uitsluitend weggelegd voor het basisteam. Ook hier zijn uitzonderingen te noemen van delicten die specialistische kennis vereisen in de opsporing of aanpak hiervan en vaak worden overgedragen aan de Dienst Regionale Recherche (DRR). Enkele voorbeelden hiervan zijn kinderporno en de handel van illegale goederen (drugs, wapens) via het darkweb.

Het basisteam speelt bij de aanpak van gedigitaliseerde criminaliteit echter wel een concretere en prominentere rol dan bij de aanpak van cybercrime. Bij gedigitaliseerde criminaliteit gaat het voornamelijk om traditionele delicten (waarbij ICT als middel wordt gebruikt) die door middel van bijvoorbeeld aangiftes door burgers bij het basisteam terecht komen.

Dit onderzoek richt zich dan ook specifiek op de aanpak van **gedigitaliseerde criminaliteit** binnen het **basisteam ZBLW**.

1.3 Probleemstelling

Vanuit eerdergenoemde landelijke en regionale prioriteit dient er binnen het basisteam ZBLW de focus gelegd te worden op een aanpak van gedigitaliseerde criminaliteit. Een doelgerichte aanpak blijft tot dusver nog uit en de focus op de aanpak van gedigitaliseerde criminaliteit is er nog niet. Vanuit de leiding van basisteam ZBLW is er daarom de behoefte om te onderzoeken hoe het basisteam een bijdrage kan leveren aan de aanpak van gedigitaliseerde criminaliteit.

Hoofdvraag:

Op welke wijze kan het basisteam ZBLW een bijdrage leveren aan de aanpak van gedigitaliseerde criminaliteit?

Theoretische deelvraag:

1. Wat wordt verstaan onder gedigitaliseerde criminaliteit?

Empirische deelvragen:

2. Langs welk kanaal krijgen basisteams te maken met gedigitaliseerde criminaliteit in het dagelijks politiewerk?
3. Wat behelst de huidige aanpak van gedigitaliseerde criminaliteit binnen basisteam ZBLW?
4. Wat zijn de ervaringen met de aanpak van gedigitaliseerde criminaliteit binnen andere basisteams?

1.4 Doelstelling

Het doel van dit onderzoek is inzicht verkrijgen in en een bijdrage leveren aan de aanpak van gedigitaliseerde criminaliteit binnen het dagelijkse politiewerk van basisteam ZBLW.

Operationalisering

Ter verduidelijking worden hier twee begrippen uit de doelstelling nader toegelicht, te weten:

Gedigitaliseerde criminaliteit

Zowel binnen als buiten de politie wordt er veel geschreven over cybercrime en gedigitaliseerde criminaliteit. Dit heeft ertoe geleid dat er veel definities van deze (uiteenlopende) vorm van criminaliteit bestaan die elkaar soms ook nog overlappen. Dit onderzoek richt zich specifiek op **gedigitaliseerde criminaliteit.** Om het overzichtelijk te houden en om de hoofdvraag juist te kunnen interpreteren wordt er in dit onderzoek gebruik gemaakt van de definitie van gedigitaliseerde criminaliteit zoals beschreven op de intranetpagina van de afdeling Cybercrime van de Nationale Politie:

Onder "gedigitaliseerde criminaliteit" wordt verstaan; *Alle delicten die worden gepleegd mét een ICT middel maar die niet zijn gericht óp een ICT middel*. (Politie, 2017).

Bij gedigitaliseerde criminaliteit is ICT dus een middel om (traditionele vormen van) criminaliteit te plegen, zoals marktplaatsfraude, bedreigingen via Twitter, identiteitsfraude via Facebook en voorhanden hebben/uitwisselen van digitale kinderporno (Politie, 2017).

Dagelijkse politiewerk

Onder het dagelijkse politiewerk wordt verstaan de basispolitiezorg. Hieronder vallen alle taken die gericht zijn op het houden van toezicht, preventie, opsporing,

hulpverlening en handhaving. In het basisteam ZBLW zijn zowel de afdeling Intake & Service, als de afdeling Veelvoorkomende criminaliteit (VVC) en de agenten op straat (incidentenafhandeling en wijkagenten) verantwoordelijk voor deze taken.

Hoofdstuk 2: Onderzoeksmethodologie

2.1 Type onderzoek

Om antwoord te krijgen op de hoofdvraag is gebruik gemaakt van kwalitatief onderzoek. Met behulp van literatuuronderzoek en interviews wordt beschreven wat nodig is voor het verkrijgen van inzicht voor en het leveren van een bijdrage aan de aanpak van gedigitaliseerde criminaliteit. Hierbij wordt niet alleen de theorie maar ook de huidige aanpak en visie van het basisteam ZBLW beschreven.

2.2 Dataverzamelingsmethoden

Literatuuronderzoek

Met behulp van literatuuronderzoek is ingegaan op wat cybercriminaliteit en met name gedigitaliseerde criminaliteit zoal omvat en welke definitie men daarvoor hanteert binnen de Nationale Politie. Er is gebruik gemaakt van wetenschappelijke literatuur en interne documenten van de Nationale Politie. Daarnaast zullen ook nieuwsberichten en internetartikelen als literatuur gebruikt worden om de maatschappelijke relevantie en actualiteit van het thema te onderschrijven.

Interviews

Met semigestructureerde interviews met collega's van het basisteam ZBLW is onderzocht wat de huidige aanpak van gedigitaliseerde criminaliteit in het dagelijkse politiewerk van het basisteam is. Binnen het basisteam zijn zowel de portefeuillehouders en experts op gebied van gedigitaliseerde criminaliteit alsmede de reguliere medewerker binnen de afdeling VVC, Intake & Service en Basispolitiezorg (blauw) meegenomen in de interviews om een zo compleet mogelijk beeld te kunnen schetsen van de huidige aanpak van gedigitaliseerde criminaliteit binnen het basisteam. Op deze wijze kan er een gedegen antwoord worden gegeven op deelvraag 3.

Ook hebben er interviews plaatsgevonden met experts op gebied van gedigitaliseerde criminaliteit van andere basisteams om te achterhalen welke ervaringen andere basisteams hebben met de aanpak van gedigitaliseerde criminaliteit. Op deze manier is er inzichtelijk gemaakt op welke wijze andere basisteams een bijdrage leveren aan de aanpak van gedigitaliseerde criminaliteit. De gekozen respondenten buiten basisteam ZBLW zijn geselecteerd op basis van de zogeheten 'sneeuwbalsteekproef-methode'. In dit onderzoek is er met behulp van het literatuuronderzoek contact gelegd met de eerste digitale wijkagent binnen de Nationale Politie, werkzaam bij basisteam Roosendaal. Dit was de eerste respondent buiten basisteam ZBLW. Er is gebruik gemaakt van de expertise en het netwerk van deze respondent om twee andere basisteams aan te wijzen waarin gewerkt wordt met een aanpak van de gedigitaliseerde criminaliteit. Hiervoor is

gekozen omdat uit literatuur- en veldonderzoek is gebleken dat er binnen de Nationale Politie duidelijkheid en overzicht ontbreekt over de specifieke aanpak van gedigitaliseerde criminaliteit. In dit onderzoek is dan ook uitgegaan van de conclusie dat het te willekeurig zou zijn geweest om een aselecte steekproef uit te voeren voor het praktijkonderzoek. De drie basisteams die na de gebruikte methode naar voren zijn gekomen en zijn betrokken bij het onderzoek zijn basisteams Roosendaal, Bergen op Zoom en Langstraat.

Triangulatie

Voor de beantwoording van deelvraag 2 en deelvraag 4 wordt gebruik gemaakt van triangulatie. Met behulp van zowel literatuuronderzoek als interviews wordt onderzocht langs welk kanaal basisteams in het dagelijks politiewerk te maken krijgen met gedigitaliseerde criminaliteit en wat de ervaringen van andere basisteams zijn met betrekking tot de aanpak van gedigitaliseerde criminaliteit.

Om een overzichtelijk beeld te creëren van de verschillende deelvragen en welke methoden worden gebruikt om antwoord op deze deelvragen te kunnen geven, volgt hieronder een methode matrix:

Deelvraag	Type vraag	Methode
1	Theoretisch	Literatuuronderzoek
2	Empirisch	Literatuuronderzoek en interviews
3	Empirisch	Interviews
4	Empirisch	Literatuuronderzoek en interviews

Met de beantwoording van alle vier de deelvragen wordt getracht voldoende toereikende informatie te hebben verschaft om antwoord te kunnen geven op de hoofdvraag.

2.3 Data-analyse

Literatuuronderzoek

De resultaten uit het literatuuronderzoek zal worden gebruikt om antwoord te geven op de theoretische deelvraag (1). Daarnaast zullen de uitkomsten van dit onderzoek verder worden geanalyseerd en worden vergeleken met en gerelateerd aan de resultaten die zijn verkregen uit de afgenomen interviews. Op deze manier draagt het literatuuronderzoek bij aan de beantwoording van de empirische deelvragen (2, 3 en 4).

Interviews

Na het afnemen van de interviews, dient deze data geanalyseerd te worden. De hoofd- en deelvragen zijn uitgewerkt in een aantal topics en deze topics hebben geleid tot concrete vragen die zijn gesteld tijdens het interview. De interviews zijn wegens de gevolgen en maatregelen rondom Covid-19 uitgevoerd middels een telefoongesprek. Elk interview heeft gemiddeld 35 tot 45 minuten in beslag genomen. De gesprekken zijn opgenomen met een spraakrecorder, waarna alle interviews per topic samenvattend zijn gecodeerd en gecategoriseerd. De topics komen overeen met de onderwerpen die bij deelvraag 2, 3 en 4 aan bod komen. Om uiteindelijk antwoord te kunnen geven op de hoofdvraag is de input van de interviews vergeleken met wat er uit het literatuuronderzoek is gekomen.

2.4 Betrouwbaarheid en validiteit

In dit onderzoek wordt gekeken naar hoe de landelijke en regionale prioritering en doelstellingen op het gebied van gedigitaliseerde criminaliteit in de praktijk worden vormgegeven binnen basisteam ZBLW. Ook wordt er onderzocht wat er praktisch gezien nodig is om een bijdrage te kunnen leveren aan de aanpak van gedigitaliseerde criminaliteit. Hiervoor zijn de meetinstrumenten gebruikt die bij hebben gedragen aan een zo juist en volledig mogelijke weergave van de realiteit en doelstelling van dit onderzoeksverslag.

Gezien de prioriteit die de politie, maar ook het Openbaar Ministerie en de politiek aan de aanpak van cybercriminaliteit (in het algemeen) geeft en gezien de actualiteit en relevantie van deze vorm van criminaliteit in deze tijd, wordt verwacht dat er voldoende relevantie literatuur over te vinden is. Omdat het fenomeen 'gedigitaliseerde criminaliteit' een actueel thema is, wordt verwacht dat er voldoende recente literatuur te vinden is, maar om te voorkomen dat er in het literatuuronderzoek verouderde informatie kan worden gebruikt zal er voor het beantwoorden van de deelvragen bronnen worden gebruikt die niet ouder zijn dan 7 jaar (2013).

Tevens wordt door het hanteren van een en dezelfde definitie van het begrip gedigitaliseerde criminaliteit, bijgedragen aan de betrouwbaarheid van dit onderzoek. Deze definitie uit het literatuuronderzoek voorkomt onjuiste interpretaties als het gaat om de uitwerking van 'gedigitaliseerde criminaliteit' versus bijvoorbeeld 'cybercrime'.

De interviews zijn semigestructureerd, de onderwerpen die bij ieder interview aan bod komen liggen vast, evenals de belangrijkste vragen. Ten behoeve van de validiteit zijn deze onderwerpen en vragen opgesteld op basis van de literatuur die is beschreven in het theoretisch kader van dit onderzoek. De onderwerpen die bij ieder interview terugkomen zullen worden bijgevoegd in een vragenlijst. Ook zal er bij het afnemen van de interviews zorgvuldig worden geselecteerd. Dit houdt in dat er binnen elke afdeling van het basisteam mensen met verschillende posities

ten opzichte van het onderwerp worden geïnterviewd. Zowel experts op het gebied van gedigitaliseerde criminaliteit alsook collega's die in mindere mate te maken krijgen met gedigitaliseerde criminaliteit worden meegenomen. Door gebruik te maken van deze verscheidenheid in functies van collega's, maar ook de verscheidenheid in leeftijden, wordt de betrouwbaarheid van het onderzoek en de resultaten geoptimaliseerd.

Hoofdstuk 3: Theoretisch kader

In het theoretisch kader worden de belangrijkste begrippen en theorieën van dit onderzoek besproken. Deze informatie is van belang om het onderzoek en de resultaten op de juiste manier te kunnen interpreteren. Ook worden de onderzoeksbevindingen van het literatuuronderzoek in dit hoofdstuk nader uitgewerkt. In paragraaf 3.1 wordt het begrip 'cybercriminaliteit' uitgebreid toegelicht waarna er in paragraaf 3.2 een korte toelichting wordt gegeven op het begrip 'cybercrime'. Paragraaf 3.3 beschrijft de definitie van 'gedigitaliseerde criminaliteit' en geeft tevens antwoord op de eerste (theoretische) deelvraag. In de daaropvolgende paragrafen wordt beschreven wat er in de literatuur te vinden is over de afdelingen binnen een basisteam die te maken krijgen met gedigitaliseerde criminaliteit, de huidige aanpak van gedigitaliseerde criminaliteit binnen het basisteam ZBLW en de ervaringen van andere basisteams in district Utrecht-Oost op het gebied van de aanpak van gedigitaliseerde criminaliteit. Hier wordt bij de conclusie van dit onderzoek dieper op ingegaan, omdat de resultaten vanuit het praktijkonderzoek met behulp van het theoretisch kader in context geplaatst kunnen worden om zo een gedegen antwoord te kunnen formuleren op betreffende deelvragen.

3.1 Wat is cybercriminaliteit?

Cybercriminaliteit is volgens McAfee (2018) een ''growth industry'', waar de opbrengsten hoog zijn en de pakkansen laag. De opkomst van cybercriminaliteit en de kans om hier slachtoffer van te worden zijn een zorg voor de samenleving, de rechtshandhaving en het beleid van het ministerie van Justitie en Veiligheid (J&V). Over de aard en de organisatie van deze criminaliteit is nog niet veel informatie beschikbaar, terwijl kennis hierover essentieel is om dit fenomeen aan te kunnen pakken. Wie zijn de daders van deze misdrijven en hoe gaan ze te werk? Hoe kan de politie deze criminaliteit opsporen en op welke manieren kan cybercriminaliteit worden tegengegaan? (Odinot, et al., 2018).

Een uitbreiding op de in de inleiding gedefinieerde omschrijvingen van cybercriminaliteit volgt uit het Cybercrime-verdrag en de driedeling van Parker (Koops, 2014). Deze onderscheiden namelijk niet twee maar drie typen cybercriminaliteit:

- **Computergerichte delicten (computer-focused crimes):** strafbare feiten gepleegd tegen computers, computernetwerken of computergegevens; hierbij fungeren computers of gegevens als doel;

- **Computer-gerelateerde delicten (computer-assisted crimes)** strafbare feiten gepleegd met gebruikmaking van computers, computernetwerken of computergegevens; hierbij fungeren computers of

gegevens als substantieel hulpmiddel, wat wil zeggen dat de deze een relevante rol speelt bij het plegen van het delict;

- **Computer-relevante delicten:** strafbare feiten waarbij computers, computernetwerken of gegevens op de een of andere manier relevant zijn, als omgevingsfactor; hierbij fungeren computers of gegevens als een niet-substantieel hulpmiddel, bijvoorbeeld voor het opslaan van kinderpornografie of het versturen van een email bij de voorbereiding van een bankoverval; deze categorie omvat vooral uitingsdelicten, maar ook alle klassieke delicten (zoals moord of verkrachting) waarbij mogelijk bewijsmateriaal opgeslagen ligt in computers en waarbij de computer dus voor de opsporing een relevante factor is.

Hoewel dit onderzoek zich richt op één van deze drie typen cybercriminaliteit, de zogenaamde computer-gerelateerde delicten, of te wel 'gedigitaliseerde criminaliteit', is een uiteenzetting van deze typen van wezenlijk belang om de strekking van dit onderzoek te duiden. Daarbij wordt het derde type, 'computer-relevante delicten' slechts beperkt uiteengezet door bovenstaande uitwerking en verder buiten beschouwing gelaten gedurende dit onderzoek. Voor de uiteenzetting van de eerste twee typen, 'computer-gerichte delicten' en computer-gerelateerde delicten', wordt eerst de wettelijke context geschetst van cybercriminaliteit op nationaal en internationaal niveau.

Wettelijke context

In de jaren tachtig drong het besef door dat computers ook een object of hulpmiddel van misdadigers waren. Sommige landen pasten hun wetgeving aan en internationaal gaf de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) richtlijnen voor welke computerhandelingen strafbaar zouden moeten worden (OECD, 1986). Ook de Raad van Europa boog zich over cybercriminaliteit, met aanbevelingen op materieel (1989) en procedureel (1995) gebied. Toen de aanbevelingen wel erg vrijblijvend bleken, werd besloten een bindend verdrag op te stellen. Dat leidde tot het Cybercrime-Verdrag van de Raad van Europa, dat in 2001 in Boedapest werd ondertekend en in 2004 in werking trad (Koops, 2012).

Dit verdrag is het belangrijkste internationale instrument op het gebied van cybercriminaliteit, dat (stand van zaken mei 2013) door 39 landen is geratificeerd, niet alleen de meeste RvE-lidstaten maar ook de VS, Australië, Japan en de Dominicaanse Republiek. Daarnaast volgen ook de nodige andere landen het verdrag als voorbeeld voor hun wetgeving zonder partij te worden (Koops, 2014). Per 1 augustus 2018 hebben in totaal 61 staten het verdrag geratificeerd (Oerlemans, 2019).

De landen aangesloten bij de Raad van Europa hebben in een Cybercrime-Verdrag afgesproken tot een gemeenschappelijk strafrechtelijk beleid te komen, gericht op

de bescherming van de samenleving tegen strafbare feiten verbonden met elektronische netwerken. Vooral het tot stand brengen van passende geharmoniseerde wetgeving en het versterken van de internationale samenwerking zijn speerpunten (NCSC, 2012).

Nederland liep internationaal voorop in het nadenken over en regelen van opsporingsbevoegdheden in de digitale wereld. De Nederlandse wetgeving heeft dan ook als inspiratiebron gediend voor het Cybercrime-Verdrag (Koops, 2012).

Het Cybercrime-Verdrag was een unieke poging om mondiaal de wetgeving op het gebied van cybercriminaliteit te benaderen. Hoewel Nederland, met name op het vlak van formeel strafrecht, een internationale voortrekkersrol heeft gespeeld, bood het verdrag ook voor Nederland nog diverse punten om de nationale wetgeving aan te passen. Bovendien was de Nederlandse wetgever uit zichzelf al druk doende met wijziging van de wetgeving rond cybercriminaliteit (Koops, 2003).

De Nederlandse wetgeving gebruikt van oudsher de term computercriminaliteit, wat kan worden omschreven als criminaliteit waarbij computers of computergegevens een substantiële rol spelen. In de jaren ’80 en ’90 lag de nadruk op computers zelf, terwijl inmiddels de nadruk ligt op computernetwerken (Koops, 2014).

De introductie van de Wet computercriminaliteit in 1993 markeert het begin van de cybercriminaliteit-wetgeving in Nederland. Vanaf dat moment werd voor het eerst wetgeving opgesteld die specifiek is gericht op cybercriminaliteit, al bestonden verschillende vormen van cybercriminaliteit al langer. Teneinde de positie van opsporingsdiensten te verstevigen heeft de regering in het verleden regelmatig nieuwe wetgeving ontwikkeld met nieuwe strafbaarstellingen en nieuwe opsporingsbevoegdheden op het terrein van cybercriminaliteit (Custers, 2018). De meest recente Nederlandse wetgeving is de Wet computercriminaliteit III, die in juni 2018 werd aangenomen door de Eerste Kamer (en eerder al door de Tweede Kamer).

De dynamiek van cybercriminaliteit-wetgeving laat zien dat een werkbare combinatie mogelijk is van internationale kaders en nationale invulling en aanvulling. De Nederlandse wet kent een breed vangnet om cybercriminaliteit te bestrijden. Vrijwel alle verschijningsvormen van cybercriminaliteit kunnen onder strafbepalingen worden gebracht, mede door de ruime formulering van basisdelicten als computervredebreuk (art. 138ab Sr) en gegevensaantasting (art. 350a Sr) (Koops, 2012).

3.2 Cybercrime (computer-focused crimes)

Het plegen van cybercriminaliteit lijkt met de jaren eenvoudiger te zijn geworden. Het vereist minder technische kennis, omdat kennis over modus operandi via fora

wordt gedeeld, en specifieke kennis eenvoudigweg kan worden gekocht. Dit leidt niet alleen tot een lift van traditionele misdrijven, maar heeft tevens tot gevolg dat traditionele georganiseerde misdaadgroepen ook betrokken raken bij cybercrime in enge zin (Odinot, et al., 2018), oftewel *cybercrime.*

Computergerichte criminaliteit, cybercrime in enge zin, computer-focused crimes (Furnell, 2002), oftewel *cybercrime*, omvat criminaliteit waarbij de computer of software zelf het doelwit is van die criminaliteit, zoals bij DDoS-aanvallen of hacken (Erp, et al., 2013).

Naast de verschillende definities in de literatuur wordt in het Wetboek van Strafrecht (Sr) definitie gegeven aan de strafbaarstelling van cybercrime. Hierin zijn namelijk wetsartikelen opgenomen die cybercrime strafbaar stellen en daardoor cybercrime in de wettelijke context kunnen definiëren. In het Wetboek van Strafrecht (Sr)zijn verschillende artikelen opgenomen die refereren aan cybercrime. Het gaat daarbij in het bijzonder om wetsartikelen die gericht zijn op strafbaarstelling van cybercriminaliteit. In artikel 138ab wordt bijvoorbeeld het opzettelijk en wederrechtelijk toegang verschaffen tot een geautomatiseerd werk of een deel daarvan strafbaar gesteld. Dit refereert aan computervredebreuk (Leukfeldt, et al., 2010).

3.3 Gedigitaliseerde criminaliteit (computer-assisted crimes)

Onder "gedigitaliseerde criminaliteit" wordt verstaan; *Alle delicten die worden gepleegd mét een ICT middel maar die **niet zijn gericht óp** een ICT middel*. Bij gedigitaliseerde criminaliteit is ICT een middel om traditionele vormen van criminaliteit te plegen, zoals marktplaatsfraude, bedreigingen via Twitter en identiteitsfraude via Facebook (Nationale Politie, 2017).

Bij gedigitaliseerde criminaliteit gaat het dus om misdrijven waarbij alleen het middel een ICT-component bevat en het misdrijf gericht is op de persoon, zoals online bedreiging via bijvoorbeeld e-mail of social media en oplichting zoals aan- of verkoopfraude (WODc, 2019). Andere voorbeelden zijn: stalkers die internet misbruiken om hun slachtoffer lastig te vallen of pedofielen die kinderporno grafische afbeeldingen in bezit hebben (Leukfeldt, et al., 2015). Omdat het bij gedigitaliseerde criminaliteit om traditionele delicten met een digitaal component gaat, zijn er tal van delicten die onder deze noemer vallen en zijn dit dus slechts enkele voorbeelden. In plaats van een fysieke omgeving wordt (voornamelijk) het internet als digitale omgeving gebruikt als koop-, verkoop- en verhandelplaats van illegale goederen en diensten en fungeert het als plaats om kennis en informatie uit te wisselen met betrekking tot criminele activiteiten. Ook zijn tegenwoordig tal van gebruiksvoorwerpen gekoppeld aan het internet waardoor apparaten op afstand kunnen worden gemanipuleerd. (RSIV, z.d.)

Zoals omschreven in het Cybercrime-Verdrag en de driedeling van Parker, gaat het hier dus om computer-gerelateerde delicten. Cybercrime in brede zin, computer-assisted crimes (Furnell, 2002), oftewel *gedigitaliseerde criminaliteit.* Zoals beschreven wordt deze definitie gehanteerd voor dit onderzoek naar cybercriminaliteit, specifiek de aanpak van gedigitaliseerde criminaliteit door het basisteam van de Nationale Politie, regio ZBLW.

3.4 Landelijke en regionale prioriteit

In 2019 gaf 13 procent van de 15-plussers aan slachtoffer te zijn geweest van een of meer cybercriminaliteitsdelicten. In 2012 was dit 12 procent, in 2017 11 procent. Bij cybercriminaliteit gaat het om digitale vormen van identiteitsfraude, koop- en verkoopfraude, hacken en cyberpesten (laster, stalking, chantage en bedreiging met geweld via internet)(CBS, 2020).

'Cybercriminaliteit heeft vele gezichten. De gevolgen kunnen zeer ingrijpend zijn met daarbij veel slachtoffers. Criminelen richten zich onder meer op het inbreken in computers voor nieuwe vormen van diefstal en afpersing van burgers en bedrijven, op het platleggen van websites en op bedrijfsspionage. Een zo veelomvattend fenomeen vraagt om een integrale aanpak van preventie, het voorkomen van dader- en slachtofferschap, opsporing en vervolging tot het terugdringen van recidive'. (Uitwerking Veiligheidsagenda 2019-2020 Ministerie van Justitie en Veiligheid, 2018). In de uitwerking van haar Veiligheidsagenda 2019-2022 heeft het Ministerie van Justitie en Veiligheid de bestrijding van cybercriminaliteit als een van haar landelijke beleidsdoelstellingen beschreven.

De missie van de Nationale Politie is al jaren dat ze Waakzaam en Dienstbaar staat voor de waarden van de rechtsstaat. Beschermen, begrenzen en bekrachtigen. Deze missie is onveranderd, maar heeft in de afgelopen jaren door de snelle digitalisering nadrukkelijk een extra dimensie gekregen: de taak van de Nationale Politie strekt zich al lang niet meer alleen uit tot het fysieke domein, maar de Nationale Politie heeft nu ook een rol in het digitale domein (Jaarplan Digitalisering en Cybercrime 2020).

Cybercriminaliteit is één van de landelijke prioriteiten bij de politie en het Openbaar Ministerie (hierna: OM). Om deze prioriteit concreet te maken zijn er onder andere afspraken gemaakt met betrekking tot bijvoorbeeld het aantal cybercriminaliteit-verdachten dat ingezonden moest worden naar het OM. Deze doelstelling is binnen de eenheid Midden-Nederland verdeeld tussen het cybercrime-team, de district-recherches en de *basisteams* (Cybercrime in de basisteams 2019).

In haar Strategie executie kaart (SE) 2018-2023 heeft basisteam ZBLW op het gebied van cybercriminaliteit een tweetal veranderdoelen beschreven. Zo zou basisteam ZBLW in 2019 een drietal cybercriminaliteitszaken aandragen bij het OM en moest het kennisniveau en de bewustwording op het gebied van

cybercriminaliteit van het basisteam in 2020 van een laag naar gemiddeld niveau (SE kaart District ZBLW 2018-2023).

3.5 Langs welk kanaal krijgen basisteams te maken met gedigitaliseerde criminaliteit in het dagelijks politiewerk?

Zoals reeds beschreven spitst dit onderzoek zich toe op een vorm van cybercriminaliteit, specifiek 'gedigitaliseerde criminaliteit'. Gedigitaliseerde criminaliteit uit zich in de 'klassieke' vormen van criminaliteit die nu (ook) via internet gepleegd worden. Niet alle delicten met een digitale component kunnen worden afgehandeld door digitale experts. Daarvoor zijn het er te veel. Zo krijgen steeds meer politiemedewerkers met dergelijke zaken te maken, ook de medewerkers van de Intake en Service (Leukfeldt, et al., 2015). De medewerkers van Intake en Service maken deel uit van de basisteams.

Om te begrijpen langs welk kanaal de basisteams te maken krijgen met gedigitaliseerde criminaliteit in het dagelijks politiewerk, is het van belang een kort overzicht te schetsen welke diensten/eenheden deel uitmaken van de basisteams van de Nationale Politie:

- **Intake en Service:** afhandelen aangifte, afhandelen informatieverzoek en het afhandelen van meldingen.

- **Incidentenafhandeling:** incidentenafhandeling of noodhulp is hulp bij incidenten die met spoed inzet van de politie nodig hebben. Hiervoor zijn 24 uur per dag en 7 dagen per week politiemensen beschikbaar. Bij deze incidenten is het noodzakelijk dat de politie direct handelt. Noodhulpeenheden behandelen deze incidenten. Zij worden aangestuurd door de meldkamer.

- **VVC (Veelvoorkomende Criminaliteit, hierna: VVC):** behandelen van veelvoorkomende criminaliteitszaken. Dit zijn voornamelijk zaken als diefstal, bedreiging, stalking, oplichting en (eenvoudige) mishandeling. Overige taken van de VVC zijn verdachten verhoren, getuigenverklaringen opnemen, bewijslast vergaren en dossieropbouw. Uiteindelijk worden de dossiers aangeboden aan het Openbaar Ministerie, die de zaak verder in behandeling neemt.

Wanneer in dit onderzoek een beschrijving zich specifiek richt op een dienst of eenheid van het basisteam, wordt de term 'basisteam' gehanteerd om dit te duiden. Het kan in dat geval dus gaan om ofwel Intake en service, de incidentafhandeling, VVC dan wel een combinatie daarvan. In de praktijk van dit onderzoek zal tevens dieper in gegaan worden op langs welk kanaal het basisteam in het dagelijks politiewerk in aanraking komt met gedigitaliseerde criminaliteit.

Waar specialistische teams als 'Team High Tech Crime' en cybercrimeteams binnen de Nationale Politie zich richten op de cybercrime, houdt het basisteam zich bezig met gedigitaliseerde criminaliteit. Gedigitaliseerde criminaliteit is veel voorkomende criminaliteit (VVC) met een digitaal component erin. Op de basisteams worden steeds vaker aangiftes gezien met een digitaal component (De (wijk)agent digitaal anno 2020, 2020).

3.6 De aanpak van gedigitaliseerde criminaliteit binnen de basisteams

In 2019 heeft er een onderzoek plaatsgevonden naar cybercrime in de basisteams (Cybercrime in de basisteams 2019). Van belang is het te weten dat er in dit onderzoek geen onderscheid wordt beschreven op welke vorm van cybercriminaliteit dit onderzoek zich destijds richtte en of er sprake is van een en dezelfde beschrijving van het soort zaken dat door de Nationale Politie geregistreerd wordt met betrekking tot cybercriminaliteit.

Uit het volgende blijkt echter dat ondanks het niet gemaakte onderscheid er een duidelijk gegeven naar voren komt met betrekking tot de aanpak van cybercrime of cybercriminaliteit in zijn algemeenheid binnen de basisteams anno 2019:

'Het overgrote deel van de zaken die worden doorgezet naar de basisteams wordt afgerond zonder dat er een verdachte is geïdentificeerd. De reden hiervoor wordt meestal niet vastgelegd, maar het ontbreken van BOB (Bijzondere opsporingsbevoegdheden)-aanvragen wijst erop dat er geen onderzoek heeft plaatsgevonden. Het lijkt hier veelal te gaan om zaken van Marktplaats- en betaalverzoek-fraude.' (Veraart, 2020).

Onderzoek dat zich alleen toespitst op de huidige aanpak van gedigitaliseerde criminaliteit van basisteam ZBLW heeft (nog) niet plaatsgevonden, waardoor een theoretisch aspect met een onderbouwing middels cijfers ontbreekt. Een huidige aanpak is daardoor (nog) niet te beoordelen op haar effectiviteit en in theoretische zin (nog) niet te beschrijven en weer te geven. Daar zal gedurende de praktijk van dit onderzoek informatie vergaard, verwerkt en uiteindelijk in hoofdstuk 4 beschreven worden.

Hoofdstuk 4. Resultaten

In dit hoofdstuk worden de resultaten van de interviews met de betrokken medewerkers van het basisteam ZBLW en medewerkers van drie andere basisteams gepresenteerd. Bij de interviews zijn vragen behandeld die uiteindelijk een antwoord formuleren op de drie empirische deelvragen. Hieronder worden de vragen en het resultaat van de empirische deelvragen uiteengezet waarna er in de conclusie specifiek wordt ingegaan op de hoofdvraag van dit onderzoek. Dit hoofdstuk wordt verdeeld in twee onderdelen:

1. Interviews binnen basisteam ZBLW
2. Interviews in andere basisteams, te weten:
    - Basisteam Langstraat
    - Basisteam Roosendaal
    - Basisteam Bergen op Zoom

4.1 Interviews binnen basisteam ZBLW

Term 'Gedigitaliseerde criminaliteit'

Uit de interviews blijkt dat drie van de tien respondenten goed wisten te benoemen wat de term 'gedigitaliseerde criminaliteit' inhoudt. Zij wisten een duidelijk onderscheid tussen de zogeheten cybercrime en de gedigitaliseerde criminaliteit te benoemen. De overige zeven respondenten hadden geen goed beeld van wat deze term inhoudt. Er werd geen onderscheid gemaakt tussen cybercrime en gedigitaliseerde criminaliteit.

4.1.1 Empirische deelvraag 1:

Langs welk kanaal krijgt het basisteam in de dagelijkse praktijk te maken met gedigitaliseerde criminaliteit?

Bij deze vraag wordt er onderscheid gemaakt tussen drie afdelingen binnen het basisteam. Deze drie afdelingen krijgen ieder op een andere wijze te maken met gedigitaliseerde criminaliteit. De resultaten zijn als volgt:

- Afdeling Intake & Service

Respondent 5 en 7 zijn beiden werkzaam op de afdeling Intake & Service. Beide respondenten geven aan dat zij voornamelijk in hun dagelijkse praktijk met gedigitaliseerde criminaliteit te maken krijgen tijdens het opnemen van een aangifte. Respondent 5 geeft aan dat zij per dag minstens twee aangiften per dag voorbij ziet komen die betrekking hebben op WhatsApp-fraude. Ook wordt er veel aangifte gedaan van online fraude waarbij een zogeheten account is gehackt om zo op iemands naam producten via het internet te bestellen.

Respondent 7 geeft aan dat er in de hedendaagse praktijk nog weinig aangiftes worden gedaan van fietsendiefstal en dat dergelijke aangiftes vervangen zijn voor zaken omtrent online fraude.

Beide respondenten benoemen dat zij ook met gedigitaliseerde criminaliteit in aanraking komen door vragen die zij van wijkbewoners krijgen aan de balie. Hier draait het voornamelijk om het geven van advies aan de wijkbewoners ter voorkoming van slachtofferschap van gedigitaliseerde criminaliteit.

- Afdeling VVC

Respondenten 1 en 6 zijn beiden werkzaam op de afdeling VVC. Respondent 1 geeft aan steeds meer te maken te krijgen met gedigitaliseerde criminaliteit in de dagelijkse praktijk. Zij helpt onder andere de afdeling Intake & Service met het opnemen van een kwalitatief goede aangifte waar digitale sporen bij zijn betrokken, ten behoeve van de opsporing.

> *"Je ziet duidelijk een verschuiving van klassieke delicten naar delicten met een digitaal component."* – Respondent 6

De aangiftes die worden opgenomen komen uiteindelijk bij de afdeling VVC in 'de bak' waarna de zaken door de Zaak coördinator wordt verdeeld onder de teamleden. Respondenten 1 en 6 bezitten beiden expertise op gebied van gedigitaliseerde criminaliteit, dus de zaken die hieronder vallen wordt altijd tussen deze twee respondenten verdeeld. Respondent 6 geeft aan dat zij ook regelmatig zelf een zaak waarbij een digitale component een rol speelt uit de bak vist om deze zaak vervolgens op eigen initiatief op te pakken.

- Incidentenafhandeling

Van de medewerkers die werkzaam zijn binnen de incidentenafhandeling geeft 66% (vier van de zes) van de respondenten aan nauwelijks tot niet in aanraking te komen met gedigitaliseerde criminaliteit in de dagelijkse praktijk. Respondent 1 benoemt dat *als* we er al mee te maken krijgen binnen het basisteam, dat dit voornamelijk bij de afdeling Intake & Service en bij de VVC is. De incidentenafhandeling krijgt er volgens respondent 1 alleen mee te maken als ze door mensen op straat worden aangesproken die hier een vraag over hebben.

Respondent 3 geeft aan dat hij wel eens in aanraking komt met gedigitaliseerde criminaliteit in de dagelijkse praktijk. Ook benoemt hij dat hij zelf, vanuit zijn digitale expertise, bewust bezig is met eventuele digitale sporen bij bijvoorbeeld een bedrijfsinbraak. Respondent 3 geeft aan dat hij denkt dat weinig andere collega's dit doen, omdat zij te weinig expertise hebben op het gebied van gedigitaliseerde criminaliteit.

"Sporen die wij in de incidentenafhandeling veiligstellen, zijn eigenlijk altijd fysieke sporen die door de Forensische Opsporing bekeken kunnen worden. Digitale sporen die mensen nalaten, wordt niet aangedacht." – Respondent 3

Respondent 4 geeft aan dat zij vaak pas achteraf met gedigitaliseerde criminaliteit te maken krijgen. Pas nadat er een aangifte is gedaan, kan de incidentenafhandeling door de VVC worden ingezet om bijvoorbeeld camerabeelden uit te kijken of een pseudokoop op te zetten wanneer een burger zijn gestolen fiets op marktplaats ziet staan. Ook geeft respondent 4 aan dat hij denkt dat de kennis op het basisteam beperkt is en dat de collega's niet weten wat er allemaal mogelijk is. Tijdens het interview werd door de afnemer een voorbeeld geschetst over een bedrijfsinbraak. Hierbij werd aangegeven dat je mogelijk via routergegevens kan achterhalen of er onbekende apparatuur in de buurt is geweest die een connectie heeft proberen te maken met het netwerk. Dit kan een indicatie, of 'digitaal spoor' zijn van een onbevoegd persoon die op een specifiek tijdstip op de locatie van de inbraak was. Respondent 4 zegt hierover: "Dat klinkt heel logisch, maar ik zou daar zelf niet aan denken".

Ook respondent 7 geeft aan dat er te weinig kennis en expertise binnen het basisteam is. Hij geeft als reden dat het slagingspercentage lager ligt dan klassieke delicten en dat het daarnaast meer capaciteit en tijd kost om dergelijke zaken te kunnen oppakken. Dit leidt er volgens hem toe dat zaken omtrent gedigitaliseerde criminaliteit gemakkelijker worden afgedaan.

"Verwacht een burger van ons dat wij voorkomen dat er DDOS aanvallen plaatsvinden, of vinden zij het belangrijker dat hun vader of moeder niet voor tienduizenden euro's wordt opgelicht?" – Respondent 9

Respondent 9 is Operationeel Expert Wijk en heeft cybercrime in zijn portefeuille. Hij geeft aan dat deze portefeuille veel meer gericht is op cybercrime dan op gedigitaliseerde criminaliteit en dat dit niet direct aansluit op de werkzaamheden van een basisteam. Respondent 9 geeft aan dat hij in de dagelijkse praktijk te weinig in aanraking komt met gedigitaliseerde criminaliteit.

4.1.2 Empirische deelvraag 2:

Wat behelst de huidige aanpak van gedigitaliseerde criminaliteit binnen basisteam ZBLW?

Van de 10 respondenten geeft 80% (respondenten 1, 2, 3, 5, 6, 7, 9 en 10) aan dat er geen specifieke aanpak of specifiek beleid is omtrent de aanpak van gedigitaliseerde criminaliteit. De overige 20% (respondenten 4 en 8) geeft aan hier geen weet van te hebben. Dit geldt voor zowel de afdeling Intake & Service, alsook voor de VVC en de incidentenafhandeling. Respondent 3 en 5 geven beiden

aan dat de aanpak van gedigitaliseerde criminaliteit niet anders is dan andere zaken waarbij een digitaal component geen rol speelt.

Respondent 2 benoemt dat er bovendien veel onduidelijkheid heerst omtrent het behandelen van zaken en sporen omtrent gedigitaliseerde criminaliteit, zoals een inbeslagneming van een smartphone.

> *"Welke lijntjes moeten er bewandeld worden? Vaak doen collega's het dan maar niet, omdat het te onduidelijk is."* – Respondent 2

Respondent 4 is werkzaam binnen de incidentenafhandeling en geeft aan dat een specifieke aanpak omtrent gedigitaliseerde criminaliteit ook niet nodig is voor zijn werk. Binnen de politie zijn er al tal van protocollen en werkwijzen. "Als ik van alles wat af moet weten, wordt dat wel heel veel".

Respondenten 1 en 6 zijn beiden werkzaam binnen de VVC. Zij gaven beiden aan dat er geen specifiek beleid is, maar dat er binnen de VVC wel bekend is dat zij beiden de meeste expertise hebben op gebied van gedigitaliseerde criminaliteit. Het is dan ook een ongeschreven regel dat zij alle zaken met een digitaal component op hun naam krijgen en in behandeling nemen.

Respondent 3 (Incidentenafhandeling) en respondent 6 (VVC) geven aan dat zij vanuit de teamleiding van basisteam ZBLW tijd en ruimte toegewezen hebben gekregen om zich bezig te houden met gedigitaliseerde criminaliteit. Zij geven aan dat zij zich in de komende tijd bezig gaan houden met het ontwikkelen van beleid rondom gedigitaliseerde criminaliteit en dit beleid en hun kennis en expertise willen gaan delen met en overdragen aan alle medewerkers van het basisteam. Zij geven dus aan dat er op dit moment nog geen beleid is, maar dat hier wel aan gewerkt wordt.

Wat heeft het basisteam ZBLW nodig om een betere bijdrage te kunnen leveren aan de aanpak van gedigitaliseerde criminaliteit?

Om de resultaten op deze vraag overzichtelijk te houden, wordt dit onderwerp in verdeeld onder de volgende topics:

1. Kennis en bewustwording
2. Specialist / vraagbaak
3. Tijd en middelen
4. Informatievoorziening

Hieronder worden de resultaten uit de interviews per topic uitgewerkt.

1. Kennis en bewustwording

70% van de respondenten (1, 2, 3, 6, 8, 9 en 10) heeft behoefte aan een bepaalde vorm van kennis en bewustwording. Dit kan volgens de respondenten bereikt worden op verschillende manieren. Respondent 1 geeft aan dat het van belang is dat de aanwezige kennis en expertise bij specifieke personen binnen het basisteam breder gedeeld moet worden. Respondent 2 geeft aan het gevoel te hebben dat er weinig mensen affiniteit hebben met gedigitaliseerde criminaliteit, maar dat dit wel een belangrijk onderwerp is binnen de hedendaagse politiepraktijk. Om medewerkers binnen het basisteam hier meer kennis in te laten opdoen, kun je bijvoorbeeld een verplichte profcheck in het leven roepen met gedigitaliseerde criminaliteit als onderwerp.

Respondenten 1, 2, 3 en 6 hebben al de nodige expertise op het gebied van gedigitaliseerde criminaliteit en geven aan dat hun behoefte vooral ligt bij het up-to-date houden van hun kennis door middel van het volgen van extra cursussen of opleidingen, zoals bijvoorbeeld een OSINT-opleiding. Respondent 3 benoemt hierbij dat dit ook van belang is om uiteindelijk routine te krijgen in het werken met zaken waarbij digitale componenten een rol spelen.

Respondenten 4, 5, 7 en 8 zijn medewerkers die minder affiniteit hebben met gedigitaliseerde criminaliteit. Zij geven aan dat zij het volgen van (al dan niet verplichte) opleidingen of cursussen als niet nuttig ervaren, omdat dit in hun ogen niet lang genoeg blijft hangen. *"De materie is te complex voor een korte cursus"* – Respondent 7. Respondent 5 zegt hierover het volgende: *"Een cursus is leuk en interessant om te doen, maar omdat de digitale wereld steeds vernieuwd, loop je na 2 weken alweer achter de feiten aan."*

> *"De trein is al weg, maar we moeten proberen om hem enigszins in zicht te houden"* – Respondent 10

Respondenten 1, 3, 9 en 10 benoemen dat "bewustwording" binnen het basisteam ook van belang is om een betere bijdrage te kunnen leveren aan de aanpak van gedigitaliseerde criminaliteit. Respondent 1 geeft aan dat de gedigitaliseerde criminaliteit binnen het basisteam nauwelijks leeft, terwijl een groot deel van de zaken die bij ons binnenkomt hieronder valt. Mensen zijn zich hier niet van bewust. Respondent 10 voegt hieraan toe dat deze onwetendheid de grootste angel is. *"Bewustwording is belangrijk en dit hopen we te gaan creëren met de twee collega's van de VVC en incidentenafhandeling die zich meer gaan richten op de gedigitaliseerde criminaliteit".*

> *"Mensen kunnen kiezen, of fietsendiefstal, of gedigitaliseerde criminaliteit. Dan kiezen ze natuurlijk de weg van de minste weerstand."* – Respondent 10

2. Specialist / vraagbaak

60% van de respondenten (3, 5, 6, 7, 8 en 10) geeft aan dat één of meerdere specialisten in het basisteam die ook kunnen fungeren als vraagbaak een bijdrage kan gaan leveren aan de aanpak van gedigitaliseerde criminaliteit. Respondent 5 zegt hierover: *"Er is heel erg behoefte aan iemand hier in het basisteam die zich heeft gespecialiseerd in criminaliteit. Een vraagbaak".* Respondent 3 geeft aan dat er binnen het basisteam behoefte is aan één of twee mensen die de gedigitaliseerde criminaliteitszaken vertalen zodat het voor iedereen op het basisteam behapbaar is. Een zaak voorbereiden zodat elke rechercheur of medewerker van de incidentenafhandeling de zaak kan oppakken. *"Eigenlijk alles voorbereiden om de zaak 'fysiek' te maken, zodat iedereen het snapt",* aldus respondent 3. Respondent 9 zegt hierover: *"Zorg ervoor dat er binnen het basisteam iemand helemaal is opgeleid en op vlieghoogte is om gedigitaliseerde criminaliteit te begrijpen en aan te pakken."*

3. Tijd en middelen

De helft van de respondenten (1, 3, 6, 8 en 10) geeft aan dat het basisteam een betere bijdrage kan leveren aan de aanpak van gedigitaliseerde criminaliteit wanneer er meer tijd en middelen worden vrijgemaakt, specifiek gericht op de gedigitaliseerde criminaliteit. Respondent 6 zegt hierover: *"De juiste middelen om gedigitaliseerde criminaliteit aan te pakken ontbreken, terwijl die middelen er voor zorgen dat het werk makkelijker en dus ook leuker wordt"*. Respondent 1 benoemt dat er momenteel een schreeuwend tekort aan medewerkers is op meerdere afdelingen, dus er is te weinig tijd om je het werken met gedigitaliseerde criminaliteit eigen te maken.

> *"Ik heb al te weinig tijd om mijn huidige werkzaamheden uit te voeren, dus er is al helemaal geen tijd om expertise op te doen op gebied van gedigitaliseerde criminaliteit".* – Respondent 8

Respondent 10 benoemt dat er nu al twee collega's van de VVC en van de incidentenafhandeling zijn aangesteld die meer tijd toegewezen krijgen voor digitale zaken. Er zijn volgens hem echter nog wel meer (fysieke) middelen nodig, zoals een goede computer die ook buiten het politienetwerk kan functioneren en de mogelijkheid om bestanden sneller te delen met interne en externe partners.

4. Informatievoorziening

Informatievoorziening in de vorm van protocollen, checklists of stappenplannen die bij kunnen dragen aan een betere aanpak van gedigitaliseerde criminaliteit. 3 van de 10 respondenten (4, 5 en 8) geven aan dat hier binnen het basisteam op alle drie de afdelingen behoefte aan is.

Respondent 4 zegt hierover*: "Er is behoefte aan een verzamelpunt van informatie en protocollen omtrent gedigitaliseerde criminaliteit, zoals een toegewezen pagina*

op Agora." Respondent 8 vult hierbij aan: *"Net als bij verkeer en hennep, zou je een pagina op Agora kunnen toewijzen waar collega's handleidingen, stappenplannen etc. kan vinden omtrent gedigitaliseerde criminaliteit."*

Respondent 5 geeft aan dat er binnen de Intake & Service behoefte is aan duidelijkere informatievoorziening; *"Wat ik heel fijn zou vinden is een soort stappenplan of checklist die ik bij een aangifte van gedigitaliseerde criminaliteit erbij kan houden, zodat de kwaliteit van de aangifte goed is."*

4.2 Interviews in andere basisteams

Term 'Gedigitaliseerde criminaliteit'

Alle respondenten (11, 12, 13, 14 en 15) wisten helder en duidelijk uit te leggen wat de term 'gedigitaliseerde criminaliteit' inhoudt. Ook het onderscheid tussen cybercrime en gedigitaliseerde criminaliteit werd door alle respondenten gemaakt. Respondent 12 zegt hierover: *"Ik weet zeker dat bij 9 van de 10 collega's en zelfs hogerop binnen de politie en bij betrokken externe partijen dit verschil niet helder is. Dit zorgt voor veel onduidelijkheid en leidt ertoe dat de termen door elkaar heen worden gebruikt".* Respondent 14 benoemt hierover het volgende: *"Als de term 'gedigitaliseerde criminaliteit' binnen het basisteam bekend is, ziet men in dat het eigenlijk helemaal niet zo'n enge en ingewikkelde term is. Het woord 'cybercrime' schrikt collega's af."*

Langs welk kanaal krijgt het basisteam in de dagelijkse praktijk te maken met gedigitaliseerde criminaliteit?

<u>Basisteam Langstraat</u>

Respondent 11, digitaal wijkagent, is voornamelijk bezig met de preventie op het gebied van gedigitaliseerde criminaliteit: "Ik ben vooral bezig met hoe we de burger kunnen informeren en zorgen dat ze bijvoorbeeld niet in de slimme trucs van gehaaide digitale criminelen trappen". Respondent 12, werkzaam in hetzelfde basisteam, benoemt: "Opsporen is vaak lastiger, dus voor mij is het voorkomen belangrijker." Respondent 11 is binnen zijn basisteam actief op social-media, whatsapp en geeft informatieavonden omtrent gedigitaliseerde criminaliteit. Ook benoemt respondent het volgende: "We hebben ook een Senior Tactische Opsporing, hij houdt zich voornamelijk bezig met de opsporing."

<u>Basisteam Roosendaal</u>

Respondent 13, digitaal wijkagent, geeft aan dat hij met gedigitaliseerde criminaliteit te maken krijgt via aangiftes van burgers: *"De aangiftes komen uiteindelijk terecht bij de VVC, waarna ik de moeilijkere zaken met een digitaal component toegewezen krijg."*

Basisteam Bergen op Zoom

Respondent 14 en 15 krijgen in hun basisteam op dezelfde wijze in hun dagelijkse praktijk te maken met gedigitaliseerde criminaliteit. Respondent 14 zegt hierover: *"Er wordt aangifte gedaan en deze aangifte komen in de werkvoorraad waarna de screeners de digitale zaken aan mij toewijzen".*

Hoe is de werkwijze omtrent de aanpak van gedigitaliseerde criminaliteit op dit moment geregeld binnen het basisteam?

In alle drie de basisteams is er geen sprake van een concrete werkwijze of beschreven beleid omtrent de aanpak van gedigitaliseerde criminaliteit. Wel zijn er binnen de basisteams ongeschreven regels hieromtrent.

Basisteam Langstraat

Respondent 11 (basisteam Langstraat) zegt hierover: *"Ik ben binnen mijn team de aangewezen persoon met de juiste expertise die de digitale zaken uitzet naar collega's en fungeert als vraagbaak. Iedereen is hier ook van op de hoogte".* Binnen basisteam Langstraat is er wel vanuit de teamleiding opgelegd dat de collega's digitaal bewuster moeten worden. Hierover zegt respondent 12 het volgende: "*Elke medewerker van het basisteam moet online surveilleren, waarbij ze eens in de zoveel tijd een half uur het internet moeten gaan bevragen."* Respondent 11 voegt hier het volgende aan toe: "*We hebben zelfs een digitale ruimte. Daar doen we OSINT sessies, waarbij we bijvoorbeeld aan de slag gaan met een vraag van een wijkagent met betrekking tot digitale sporen in open bronnen. Als een medewerker na een kwartier niks gevonden heeft, maar zijn buurman of -vrouw wel, gaan we samen kijken hoe diegene dat heeft gedaan. Hier leert iedereen veel van".* Ook benoemt hij dat zo'n digitale ruimte in het basisteam een goede aantrekkingskracht heeft. Collega's lopen langs en raken geïnteresseerd en geënthousiasmeerd.

Basisteam Roosendaal

Respondent 13 benoemt het volgende: "*De VVC mist bij ons in het basisteam heel erg de expertise op gebied van gedigitaliseerde criminaliteit. Hierdoor leunen ze erg op mij. Met alle respect, ik kan ook niet alle zaken doen".*

> *"De aanpak is veel te afhankelijk van collega's in het basisteam en die daar wel of niet bedreven in zijn."* – Respondent 13

Ook benoemt hij dat de zaken met een digitaal component vaak automatisch op hem worden afgeschoven, omdat binnen het basisteam bekend is dat hij de meeste expertise heeft op gebied van gedigitaliseerde criminaliteit.

Basisteam Bergen op Zoom

Ook binnen basisteam Bergen op Zoom is er sprake van een mondelinge afspraak en geen officieel of erkend beleid. Respondent 15 zegt hierover: *"Bij ons worden de zaken met betrekking tot gedigitaliseerde criminaliteit hetzelfde behandeld als alle andere zaken. Maar de screeners bij weten dat ik affiniteit heb met digitale zaken, dus krijg ik ze vaak toegewezen".*

4.2.1 Empirische deelvraag 3:

Wat zijn de ervaringen met de aanpak van gedigitaliseerde criminaliteit binnen andere basisteams?

Basisteam Langstraat

Op basisteam Langstraat leeft het onderwerp ´gedigitaliseerde criminaliteit´ bij de medewerkers op de werkvloer. Ook de teamleiding ziet in dat het een belangrijk onderwerp is, zegt respondent 11. Toch zegt respondent 11 hierover nog het volgende: *"Binnen de politie in het algemeen leeft het onderwerp nog niet voldoende. Je wordt niet afgerekend op het behalen van geen resultaat, terwijl je wel wordt afgerekend op het aantal onopgeloste zaken omtrent woninginbraak. Er moeten heldere doelen komen".* Ook ziet respondent 11 dat de gemeente en de politie veel investeren in bijvoorbeeld inbraken, zoals tekstkarren, buurtonderzoek en de gemeente die veel geld stopt in preventie van inbraken. *"Maar ondertussen worden er mensen voor meer dan tienduizenden euro's opgelicht op het internet, daar hoor je niks over."*

> *"Wij moeten gaan inzien dat het probleem groter is dan wij denken."* – Respondent 11

Respondent 12 zegt: *"Wij hebben over het algemeen meer digitale middelen dan een ander basisteam, maar toch hebben we meer middelen nodig om de aanpak te kunnen verstevigen en het werk makkelijker te maken".* Respondent 12 doelt hier op middelen als vrije internet laptops met een 4G netwerk en VPN. De standaard IRN computers van de politie voldoen niet om digitaal te kunnen rechercheren, volgens respondent 12.

Basisteam Roosendaal

Respondent 13 vindt dat er binnen het basisteam meer bewustwording moet komen op het gebied van gedigitaliseerde criminaliteit. Hij zegt: *"Ik denk dat het 'onbekende' gewoon heel eng is voor collega's, maar je moet het gewoon doen, dan wordt het ook veel makkelijker. Er moeten opleidingen komen die kennis verschaffen."*

Ook zegt respondent 13 dat er duidelijkheid moet komen over wie er in het basisteam verantwoordelijk is op gebied van gedigitaliseerde criminaliteit; *"Een persoon met affiniteit en expertise, die ook de juiste lijntjes binnen en buiten het basisteam uit kan zetten".* Als laatste benoemt respondent 13 dat hij vindt dat er een taakaccent komt te liggen bij de hoofdagenten op het basisteam. Net als taakaccenten verkeer en hennep; *"Zodat de focus ook meer naar de collega's op de werkvloer gaat, om zo meer slagkracht te creëren".*

"Collega's worden niet afgerekend op het aantal onafgeronde digitale criminaliteitszaken, maar bijvoorbeeld ook niet op hun digitale vaardigheden." Respondent 13

<u>Basisteam Bergen op Zoom</u>

Binnen basisteam Bergen op Zoom zijn de twee respondenten heel concreet. Respondent 14 zegt hierover: *"Om een betere bijdrage te kunnen leveren aan de aanpak van gedigitaliseerde criminaliteit hebben wij op de VVC ten minste 2 FTE nodig die zich volledig kunnen focussen op deze vorm van criminaliteit".*

"Er is te weinig expertise en wilskracht om deze tak van sport te beoefenen." – Respondent 14

Respondent 15 benoemt het volgende: *"Er moeten meer rechercheurs opgeleid worden in verschillende uitleessystemen zoals SummIT, TCS, ANPR, telefoons uitlezen."* Een belangrijk aspect om die betere bijdrage te kunnen leveren, is volgens respondent 15 gelegen in de rol die de persoon die zich met gedigitaliseerde criminaliteit bezig gaat houden krijgt toegewezen; *"Je moet deze personen laten 'freewheelen', geef ze artistieke vrijheid, omdat het nog onontgonnen gebied is voor de politie. Binnen bepaalde kaders lekker dingen laten uitzoeken."*

Ten slotte benoemt respondent 15 het volgende, over zijn ervaring van de aanpak van gedigitaliseerde criminaliteit binnen de Nationale Politie: *"We leven op dit moment in twee realiteiten. Je hebt de fysieke en de digitale realiteit. De politie heeft zijn bestel volledig ingericht binnen die fysieke realiteit. In de digitale realiteit zijn wij gewoon niet, of zeer ondervertegenwoordigd. Dit heeft ook zijn weerslag op criminelen. Bij klassieke delicten weten criminelen dat er altijd een pakkans is. Dat als je een delict pleegt, de politie in ieder geval onderzoek gaat doen. In de digitale realiteit zijn criminelen nog onschendbaar. De politie is daar niet de wachter van de wet".*

Hoofdstuk 5. Conclusie

Dit onderzoek richt zich op het verkrijgen van inzicht en het leveren van een bijdrage aan de aanpak van gedigitaliseerde criminaliteit binnen basisteam ZBLW. In dit hoofdstuk wordt, naar aanleiding van het theoretische- en praktijkonderzoek en de beantwoording van de deelvragen, antwoord gegeven op de hoofdvraag van dit onderzoek.

5.1 Algemene conclusie

Uit het literatuuronderzoek is duidelijk naar voren gekomen dat er zowel binnen als buiten de Nationale Politie veel verschillende termen worden gehanteerd omtrent cybercriminaliteit. Termen als cybercrime, cybercriminaliteit en gedigitaliseerde criminaliteit worden veelal door elkaar heen gebruikt. Dit resulteert in veel onduidelijkheid over de specifieke kenmerken van, in dit geval, gedigitaliseerde criminaliteit. Deze onduidelijkheid komt ook in het praktijkonderzoek naar voren. Er kon door veel medewerkers niet duidelijk worden aangegeven wat het onderscheid is tussen cybercrime en gedigitaliseerde criminaliteit.

In het theoretische gedeelte van dit onderzoek komt ook naar voren dat er binnen basisteam ZBLW weinig cijfers bekend zijn met betrekking tot gedigitaliseerde criminaliteit. Ook is er in de literatuur niets te vinden over een concrete aanpak of beschreven beleid met betrekking tot de aanpak van gedigitaliseerde criminaliteit. Dit komt ook duidelijk naar voren in het praktijkonderzoek. Medewerkers geven aan dat er geen specifieke aanpak of specifiek beleid is die beschrijft hoe het basisteam dient om te gaan met zaken omtrent gedigitaliseerde criminaliteit, of dat zij hier geen weet van hebben.

In het praktijkonderzoek komt ook naar voren dat 3 van de 5 respondenten van andere basisteams ‘digitaal wijkagent’ zijn. Deze functie is binnen de Nationale Politie nog niet erkend, maar er duiken overal steeds meer digitale wijkagenten op. De functie richt zich, naast het surveilleren in de digitale wijk, voor een groot deel op preventie van gedigitaliseerde criminaliteit. Dit gebeurt bijvoorbeeld door middel van informatieavonden, WhatsApp-vragenuurtjes en opgezette acties (in samenwerking met de gemeente) om de burger digitaal bewust te maken.

5.2 Beantwoording hoofdvraag

Op welke wijze kan het basisteam ZBLW een bijdrage leveren aan de aanpak van gedigitaliseerde criminaliteit?

Uit het onderzoek zijn een viertal onderwerpen naar voren gekomen die van belang zijn om als basisteam een bijdrage te kunnen leveren aan de aanpak van gedigitaliseerde criminaliteit:

1. **Kennis en bewustwording**

Het vergaren van kennis leidt ertoe dat het onderwerp 'gedigitaliseerde criminaliteit' binnen het basisteam breder gedragen wordt. Op dit moment weten 7 van de 10 respondenten binnen basisteam ZBLW geen duidelijke omschrijving te geven van de term 'gedigitaliseerde criminaliteit'. Het is gebleken dat er veel onduidelijkheid bestaat over deze specifieke vorm van criminaliteit, wat ervoor zorgt dat veel medewerkers het 'eng' vinden en zich er niet mee bezig willen houden. Cybercrime in enge zin is een ingewikkelde term en vereist vaak specialistische kennis die boven het niveau van een basisteam uit stijgt. Uit het literatuuronderzoek is gebleken dat gedigitaliseerde criminaliteit echter bij uitstek voor een basisteam is weggelegd. Ook het vergroten van bewustwording zal bijdragen aan een betere aanpak. Wat houdt gedigitaliseerde criminaliteit precies in? Hoe herkennen we het? Maar ook; Hoe groot is het probleem eigenlijk?

Er dient, ook door de teamleiding, geconstateerd te worden dat medewerkers binnen het basisteam niet meer weg kunnen komen met antwoorden als: *"Ik heb er geen affiniteit mee, dus ik doe er niets mee".* Medewerkers dienen zich er bewust van te worden dat gedigitaliseerde criminaliteit in het huidige politiewerk een dusdanige rol speelt, dat men er niet meer omheen kan.

2. **Specialist / vraagbaak**

De digitale wereld is voor het grootste gedeelte van de Nationale Politie nog onontgonnen gebied. Dit geldt ook voor basisteam ZBLW. In dit stadium is het nagenoeg onmogelijk om iedere medewerker op het basisteam op te leiden tot expert of specialist op gebied van gedigitaliseerde criminaliteit. Uit onderzoek binnen andere basisteams is gebleken dat het vaak begint met een aantal enthousiastelingen op de werkvloer die affiniteit en expertise hebben op digitaal gebied. Deze medewerkers zijn binnen hun eigen basisteam als zodanig bekend en daar wordt door andere medewerkers gretig gebruik van gemaakt. Ook uit het praktijkonderzoek binnen basisteam ZBLW blijkt dat er bij 6 van de 10 respondenten behoefte is aan één of twee specialisten binnen het basisteam die daarnaast fungeren als vraagbaak.

3. **Tijd en middelen**

Eén van de grootste struikelblokken die in dit onderzoek naar voren is gekomen, is het tekort aan tijd en middelen. 7 van de 10 respondenten binnen basisteam ZBLW en 4 van de 5 respondenten in de andere basisteams geven aan dat er te weinig tijd en middelen zijn om een gedegen aanpak van gedigitaliseerde criminaliteit te kunnen realiseren. Uit het onderzoek blijkt dat medewerkers van zowel basisteam ZBLW als de medewerkers van de andere basisteams al te weinig tijd hebben om hun huidige werkzaamheden uit te voeren. Er dient dus secuur te worden gekeken naar hoe medewerkers ingezet kunnen worden om

een bijdrage te kunnen leveren aan de aanpak van gedigitaliseerde criminaliteit. De teamleiding speelt hierin een belangrijke rol. Er dient vanuit de teamleiding draagvlak te zijn om hun medewerkers van tijd en middelen te voorzien om zich te kunnen ontwikkelen binnen de digitale wereld. Eén van de conclusies uit het praktijkonderzoek is immers ook: Meer tijd en middelen leidt tot meer expertise en uiteindelijk tot een efficiëntere aanpak van digitale zaken waarbij je tijd juist kunt gaan besparen. Het is een investering.

4. Informatievoorziening

Als laatste is uit het praktijkonderzoek gebleken dat 3 van de 10 respondenten binnen basisteam ZBLW behoefte hebben aan duidelijkere informatievoorziening. Binnen basisteam ZBLW bestaat er niet zozeer de behoefte aan opleidingen die voor iedere medewerker geldt, maar vooral aan specialisten en aan duidelijke stappenplannen, protocollen en algemene informatievoorziening op bijvoorbeeld een agora-pagina. Eén centrale plek, die voor iedere medewerker te vinden is, waar informatie omtrent gedigitaliseerde criminaliteit te vinden is.

Respondent 11 en 12 zien het belang in van heldere informatievoorziening naar buiten toe, in de vorm van preventiemaatregelen. Op deze wijze kan ook de bewustwording van de burger worden vergroot omtrent gedigitaliseerde criminaliteit waardoor zij minder snel slachtoffer zullen worden van slimme trucs van digitale criminelen. Een goede samenwerking met externe partijen, zoals de gemeente, is hierbij van belang.

Door op de bovenstaande vier punten te investeren zal basisteam ZBLW een bijdrage kunnen leveren aan de aanpak van gedigitaliseerde criminaliteit.

Hoofdstuk 6. Aanbevelingen

Er worden binnen dit onderzoek 4 aanbevelingen gedaan waarmee basisteam ZBLW binnen het dagelijkse politiewerk een bijdrage kan leveren aan de aanpak van gedigitaliseerde criminaliteit. Ook worden er 2 opties tot vervolgonderzoek beschreven. Deze aanbevelingen zijn gebaseerd op de resultaten van het theoretische- en praktijkonderzoek. De aanbevelingen zijn:

1. Verduidelijking term 'gedigitaliseerde criminaliteit'

Uit het onderzoek is gebleken dat er onduidelijkheid heerst onder het merendeel van basisteam ZBLW met betrekking tot de term 'gedigitaliseerde criminaliteit'. Gedigitaliseerde criminaliteit komt in eerste instantie via aangiften bij het basisteam terecht. Het wordt dan ook aanbevolen om meer specifieke aandacht te besteden aan het verduidelijken van de term 'gedigitaliseerde criminaliteit' binnen het basisteam.

2. Specialisten aanstellen

Uit het onderzoek komt naar voren dat er behoefte is aan specialisten die verantwoordelijk worden gemaakt voor de zaken rondom gedigitaliseerde criminaliteit binnen het basisteam. Aanbevolen wordt dat er in ieder geval twee specialisten worden aangewezen. Eén binnen de VVC en één binnen de incidentenafhandeling. Deze specialisten dienen dan zaken rondom gedigitaliseerde criminaliteit te vertalen naar (fysieke) handelingen zodat overige medewerkers de zaken kunnen overnemen en afhandelen. Ook dienen zij als vraagbaak te fungeren voor hun eigen afdeling.

3. Het basisteam van de juiste middelen voorzien

Om een bijdrage te kunnen leveren aan de aanpak van gedigitaliseerde criminaliteit is het van belang dat de medewerkers voorzien zijn van de juiste middelen om het werk te kunnen uitvoeren. De aanbeveling is om met de twee aangewezen personen binnen het basisteam in gesprek te gaan, om vast te stellen welke middelen benodigd zijn om dit werk te kunnen uitvoeren en hen hierin ook te voorzien. Betere middelen zorgen voor een efficiëntere en effectievere aanpak en dit leidt uiteindelijk tot meer opgeloste zaken. Het delen van de succesverhalen kan vervolgens weer leiden tot meer enthousiasme onder de overige medewerkers.

4. Centraal punt met informatievoorziening

De medewerkers binnen het basisteam hebben behoefte aan meer informatievoorziening. Een centrale plek waar informatie omtrent gedigitaliseerde criminaliteit te vinden is. Het is dan ook aan te bevelen om een taakaccenthouder binnen het basisteam aan te wijzen die verantwoordelijk wordt gemaakt om de interne Agora website van basisteam ZBLW een verzamelpunt van informatie omtrent gedigitaliseerde criminaliteit te creëren en deze up-to-date te houden met de nieuwste ontwikkelingen rondom deze vorm van criminaliteit.

5. Vervolgonderzoek: Inbedding van specialisten binnen het basisteam

De eerder genoemde aanbeveling met betrekking tot het aanstellen van twee specialisten behoeft eventueel een vervolgonderzoek waarin wordt onderzocht hoe deze 'functie' ingebed gaat worden binnen het basisteam. De onderzoeksvragen van dit vervolgonderzoek zouden kunnen zijn:

- Hoeveel tijd krijgen deze medewerkers toegewezen voor deze taak?
- Wat zijn de specifieke taken die aan hen worden toegewezen?
- Wat zijn de uiteindelijke doelstellingen die zij moeten behalen en binnen welk tijdsbestek?

6. Vervolgonderzoek: Digitale wijkagent

In het praktijkonderzoek hebben er gesprekken plaatsgevonden met 3 digitale wijkagenten. In de gesprekken kwam de meerwaarde van deze functie duidelijk naar boven. Waar de twee specialisten (zie aanbeveling 2) zich kunnen richten op de aanpak en het verspreiden van kennis omtrent gedigitaliseerde criminaliteit binnen het basisteam, kan de digitale wijkagent zich focussen op de externe betrokken partijen zoals de gemeente, lokale politiek en natuurlijk de burgers. De werkzaamheden zijn met name gericht op preventie. Een aanbeveling voor een mogelijk vervolgonderzoek zou dan ook zijn: Ga na of er binnen basisteam ZBLW formatieruimte gemaakt kan worden om een digitale wijkagent in te zetten en neem in het onderzoek ook eens een kijkje in de keuken van andere basisteams waar deze functie al is geïmplementeerd, om tot een gedegen invulling van de functie binnen basisteam ZBLW te komen.

Hoofdstuk 7. Discussie

7.1 Beantwoording hoofdvraag

Als onderzoeker heb ik beoogd om inzichtelijk te krijgen op welke manier basisteam ZBLW een bijdrage kan leveren aan de aanpak van gedigitaliseerde criminaliteit. Er is inzicht verkregen in de huidige stand van zaken omtrent gedigitaliseerde criminaliteit binnen basisteam ZBLW, het huidige kennisniveau van de medewerkers alsook de wensen van de medewerkers op de verschillende afdelingen om uiteindelijk een betere bijdrage te kunnen leveren aan de aanpak van gedigitaliseerde criminaliteit. Daarnaast is er ook inzicht verkregen in hoe dit binnen drie andere basisteams geregeld is ten opzichte van basisteam ZBLW. Terugkijkend op de resultaten van dit onderzoek kan worden gesteld dat de beantwoording van de hoofdvraag gelukt is. Enige terughoudendheid is hierbij wel geboden. De aanbevelingen dienen eerst te worden geïmplementeerd of verder worden onderzocht alvorens er daadwerkelijke resultaten zichtbaar zullen zijn.

7.2 Praktijkonderzoek

De keuze om kwalitatief onderzoek te doen is naar mijn idee een sterk punt. Op deze manier is er met ‘maar’ 10 respondenten in basisteam ZBLW een hoop bruikbare informatie verkregen omdat de interviews veel diepgang opleverden. Door tijdens het praktijkonderzoek mensen van verschillende afdelingen en verschillende niveaus van kennis over het onderwerp te interviewen, is er een verzadigingsniveau is bereikt met voldoende input om een generaliseerbaar beeld te creëren omtrent de huidige aanpak en de mogelijke verbeterpunten omtrent gedigitaliseerde criminaliteit binnen basisteam ZBLW.

Het aantal respondenten en de gekozen sneeuwbalsteekproef-methode voor de interviews in andere basisteams brengt wel beperkingen met zich mee. Zo geven de 5 geïnterviewde respondenten slechts een summier beeld van de aanpak van gedigitaliseerde criminaliteit in andere basisteams. Hierdoor zijn de verkregen resultaten niet generaliseerbaar. De keuze om in dit onderzoek te kiezen voor de sneeuwbalsteekproef-methode is gelegen in het feit dat er een landelijk overzicht ontbreekt over de aanpak van gedigitaliseerde criminaliteit binnen andere basisteams. Hoewel de verkregen informatie van de respondenten beknopt is gebleken, is er voor dit onderzoek waardevolle informatie naar boven gekomen. Het verzadigingsniveau is niet bereikt, maar vanwege de beperkte tijd en middelen en de bruikbare informatie die eruit is voortgevloeid is ervoor gekozen het in dit onderzoek hierbij te laten en een aanbeveling te doen voor een mogelijk vervolgonderzoek.

De wijze waarop de interviews zijn afgenomen brengt ook beperkingen met zich mee. Vanwege de maatregelen rondom Covid-19 is ervoor gekozen om de

interviews telefonisch af te nemen. Hierdoor kan er waardevolle informatie verloren zijn gegaan, doordat non-verbale communicatie en andere waarnemingen niet hebben kunnen plaatsvinden en dus niet zijn meegenomen in de resultaten van dit onderzoek. Deze vormen van communicatie hadden voor dit kwalitatieve onderzoek ook van waarde kunnen zijn.

Tijdens dit onderzoek is voornamelijk gekeken naar de medewerkers op de werkvloer. Wat hebben zij nou nodig om een bijdrage te kunnen leveren aan de aanpak van gedigitaliseerde criminaliteit? Hoewel de beantwoording van de hoofdvraag aansluit bij de wensen van de opdrachtgever, is het ook van belang dat de leiding de juiste vertaalslag weet te maken. De wensen vanuit de werkvloer en de aanbevelingen in dit onderzoek dienen te worden omgezet in concrete actiepunten. Zonder draagvlak en draagkracht vanuit de leiding zullen de aanbevelingen niet kunnen worden geïmplementeerd.

7.3 Presentatie

Naar aanleiding van de presentatie heb ik van de opdrachtgevers feedback mogen ontvangen over de resultaten, conclusie en aanbevelingen. Beide opdrachtgevers waren enthousiast en vonden de aanbevelingen concreet, haalbaar en toepasbaar. Naar aanleiding van de presentatie hebben er dan ook geen wijzigingen meer plaatsgevonden met betrekking tot de aanbevelingen. Wel is mij tijdens de presentatie nog duidelijker geworden dat de informatie en kennis van andere basisteams omtrent de aanpak van gedigitaliseerde criminaliteit erg waardevol kan zijn voor basisteam ZBLW. Dit inzicht is vertaald in een optie tot vervolgonderzoek (zie 7.4) die los staat van de aanbevelingen die terug zijn te vinden in hoofdstuk 6. Dit vervolgonderzoek is specifiek bedoeld om een grotere bijdrage te kunnen leveren aan dit huidige onderzoek.

7.4 Vervolgonderzoek

Met betrekking tot de interviews die zijn uitgevoerd buiten het basisteam, dient er een vervolgonderzoek plaats te vinden om de resultaten in dit onderzoek aan te sterken en generaliseerbaar te maken. De verkregen informatie is zeer waardevol gebleken voor dit onderzoek, maar om een gedegen beeld te creëren van hoe andere basisteams op landelijk niveau omgaan met de aanpak van gedigitaliseerde criminaliteit dient er een onderzoek plaats te vinden waarbij er meerdere basisteams en medewerkers worden betrokken.

7.5 Tot slot

Tijdens de uitvoering van dit onderzoek heeft het mij verbaasd hoe weinig bruikbare informatie er te vinden valt over de aanpak van gedigitaliseerde criminaliteit binnen basisteams. Cybercrime en gedigitaliseerde criminaliteit worden vaak samen in één ademteug gebruikt en dus ook vaak door elkaar

gehaald, terwijl er wel degelijk een groot verschil is tussen deze vormen van criminaliteit. Voorafgaand aan dit onderzoek was ik in de veronderstelling dat de aanpak van gedigitaliseerde criminaliteit beter georganiseerd was dan is gebleken. Het voelt, ook voor een aantal respondenten, alsof de politie achterloopt in de digitale wereld waardoor sommige kleine en grote digitale criminelen vrij spel hebben. Slechts een select groepje enthousiastelingen dragen zorg voor het realiseren van een aanpak tegen gedigitaliseerde criminaliteit op basisteamniveau. Gelukkig lijkt de tendens te zijn dat het aantal enthousiastelingen en hun invloed binnen de organisatie groeiende is en dat ook de Nationale Politie zich realiseert dat zij zich meer in de digitale wereld moet mengen.

Bronnenlijst

Boerman, F., Grapendaal, M., Nieuwenhuis, F., & Stoffers, E. (2012). *Nationaal Dreigingsbeeld 2017: Georganiseerde criminaliteit*. Geraadpleegd op 24 april 2020, via: https://www.politie.nl/binaries/content/assets/politie/algemeen/nationaal-dreigingsbeeld-2017/nationaal-dreigingsbeeld-2017.pdf

Centraal Bureau voor Statistieken. (2020). *Veiligheidsmonitor 2019.* Geraadpleegd op 7 april 2020, via: https://www.cbs.nl/nlnl/publicatie/2020/10/veiligheidsmonitor-2019

Centraal Bureau voor Statistieken. (2020). *Minder traditionele criminaliteit, meer cybercrime.* Geraadpleegd op 12 oktober 2020, via: https://www.cbs.nl/nl-nl/nieuws/2020/10/minder-traditionele-criminaliteit-meer-cybercrime

Centraal Bureau voor Statistieken. (2019). *Statline. Slachtofferschap criminaliteit.* Geraadpleegd op 12 oktober 2020, via: https://opendata.cbs.nl/#/CBS/nl/dataset/82464NED/table?ts=1602527486086

Centrum voor Criminaliteitspreventie en Veiligheid. (z.d.). *Definities Cybercrime.* Geraadpleegd op 24 april 2020, via: https://hetccv.nl/onderwerpen/cybercrime/definities/

Custers, B. (2018). Nieuwe online opsporingsbevoegdheden en het recht op privacy; een analyse van de Wet computercriminaliteit III. Justitiële Verkenningen, 44(5), 100-117.

Diez Requejo, J. (2020) *De (wijk)agent digitaal anno 2020.* Nationale Politie

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

Europese Commissie (2007), *Mededeling van de Commissie. Naar een algemeen beleid voor de bestrijding van cybercriminaliteit*, COM(2007) 267 definitief, 22.5.2007.

Erp van, J., Stol, D. W., & Wilsem van, J. (2013). *Criminaliteit en criminologie in een gedigitaliseerde wereld.* Tijdschrift voor Criminologie, 5(4), 328.

Koops, B. J. (2012). *De dynamiek van cybercrimewetgeving in Europa en Nederland.* Justitiële Verkenningen, 38(1), 9.

Koops, E. J. (2003). *Het Cyber-crimeverdrag, de Nederlandse strafwetgeving en de (computer)criminalisering van de maatschappij*. Computerrecht, 02, 115-123.

Koops, E. J. (2014). *Cybercriminaliteit*. In S. van der Hof, A. R. Lodder, & G. J. Zwenne (editors), Recht en computer, zesde druk (blz. 213-241). (Recht en praktijk: Informatie- en communicatietechnologie; Nr. 4). Kluwer.

Leukfeldt, E.R., Domenie, M.M.L., & Stol, W.Ph. (2010). *Verkenning cybercrime in Nederland 2009*. Den Haag: Boom Juridische uitgevers.

Leukfeldt, R., Kentgens, A., Prins, E., Stol., W. (2015). *Alledaags politiewerk in een gedigitaliseerde wereld.* Handreiking voor de intake van delicten met een digitale component, 1.

Leukfeldt, R., & Kranenbarg, M. W. (2017). *De menselijke factor in cybercrime.* Tijdschrift voor Criminologie, 59(3).

Ministerie van Veiligheid en Justitie. (2018). *Uitwerking Veiligheidsagenda 2019 –2022.* Geraadpleegd op 7 april 2020, via: https://www.regioburgemeesters.nl/thema/sturing-op-politie/landelijke-beleidsdoelstellingen/veiligheidsagenda-2019-2022/

Nationaal Cyber Security Centrum. (2012). *Handreiking Cybercrime.* Geraadpleegd op 20 juni 2020, via: https://www.ncsc.nl/documenten/publicaties/2019/juli/18/handreiking-cybercrime

Nationale Politie. (2020). *Midden-Nederland start digitaal district.* Geraadpleegd op 7 april 2020, via: https://intranet.politie.local/nieuws/0300/2020/februari/13/midden-nederland-start-digitaal-district.html

Odinot, G., de Poot, C., & Verhoeven, M. (2018). *De aard en aanpak van georganiseerde cybercrime: Bevindingen uit een internationale empirische studie*. Justitiele Verkenningen, 44(5).

Oerlemans, J. J. (2019). *Jurisdictie en grensoverschrijdende digitale opsporing.*

Organisation for Economic Co-operation and Development. (1986). *Computer-related crime: analysis of legal policy*. Organisation for Economic Co-operation and Development;[Washington, DC: OECD Publications and Information Centre.

Plas, T., van der. (2019). *Jaarplan Digitalisering en Cybercrime 2020.* Nationale Politie.

Regionaal Samenwerkingsverband Integrale Veiligheid. (z.d.) *Kennisbank Cyber.* Geraadpleegd op 20 juni 2020, via: https://rsiv.nl/kennisbank/cyber/

Sipma, T., Leijsen, van, E.M.C. (2019). *Slachtofferschap van online criminaliteit.* Wetenschappelijk Onderzoek- en Documentatiecentrum.

Veenstra, S., Zuurveen, R., Stol, W. (2015). *Cybercrime onder bedrijven. Een onderzoek naar slachtofferschap van cybercrime onder het Midden- en Kleinbedrijf en Zelfstandigen Zonder Personeel in Nederland.* Lectoraat Cybersafety, NHL Hogeschool & Politie Academie Faculteit Cultuur- en Rechtswetenschappen, Open Universiteit.

Veraart, E. (2020). *Cybercrime in de basisteams 2019.* Nationale Politie

Vijlbrief, M. (2012). *Synthetische drugs en precursoren. Criminaliteitsbeeldanalyse 2012.* Woerden: KLPD.

Wetenschappelijk Onderzoek- en Documentatiecentrum. (z.d.). *Aard en omvang cyber- en gedigitaliseerde criminaliteit.* Geraadpleegd op 24 april 2020, via: https://www.wodc.nl/onderzoeksdatabase/2921a-aard-en-omvang-cyber-en-gedigitaliseerde-criminaliteit.aspx