Wetenschappelijk Onderzoek- en Documentatiecentrum

Cahier 2021-23

Opsporen, vervolgen en tegenhouden van cybercriminaliteit

C.A.J. van den Eeden
J.J. van Berkel
C.C. Lankhaar
C.J. de Poot

Cahier
De reeks Cahier omvat de rapporten van onderzoek dat door en in opdracht van het WODC is verricht. Opname in de reeks betekent niet dat de inhoud van de rapporten het standpunt van de Minister van Justitie en Veiligheid weergeeft.

Inhoud

Dankwoord

Wij bedanken de leden van de begeleidingscommissie voor hun bijdragen aan het onderzoek en de feedback op eerdere versies van dit rapport. Daarnaast danken wij de respondenten voor de tijd die zij hebben vrijgemaakt om mee te werken aan dit onderzoek. Tot slot willen we Anniek Jonker bedanken voor haar hulp met de dataverzameling.

Samenvatting

Nederland heeft een snelle, stabiele en betrouwbare digitale infrastructuur, waar zowel nationaal als internationaal veelvuldig gebruik van wordt gemaakt. Die sleutelpositie geeft economische kansen, maar schept ook verplichtingen. Illegale activiteiten voltrekken zich op Nederlandse servers of worden (on)bewust gefaciliteerd door in Nederland gevestigde *hosters*.

Voor de opsporing van cybercriminaliteit beschikt de politie op landelijk niveau over het specialistische Team High Tech Crime (THTC) en zijn de afgelopen jaren gespecialiseerde cybercrimeteams op regionaal niveau versterkt. De cybercrimeteams werken samen met het THTC in een landelijke structuur en ondersteunen districtsrecherches en basisteams bij de kennisopbouw voor de uitvoering van reguliere onderzoeken naar cybercriminaliteit.

Omdat het opsporen en vervolgen van daders van cybercriminaliteit om meerdere redenen lastig kan zijn, wordt soms door de politie en het OM ook voor niet-strafrechtelijke oplossingen gekozen bij de aanpak van cybercriminaliteit. Voorbeelden van andersoortige oplossingen zijn verstoring van het criminele proces door het offline halen van servers. Ook inzetten op preventie door middel van waarschuwingscampagnes, zoals recent tegen Whatsapp-fraude, is hier een onderdeel van. Bij de aanpak van cybercriminaliteit wordt ook regelmatig publiek-private samenwerking gezocht en zijn diverse projecten gestart die gericht zijn op het tegengaan van verschillende cyberdelicten.

Het doel van dit onderzoek was om meer inzicht te krijgen in de aanpak van geavanceerde vormen van cybercriminaliteit door politie en OM. Daarnaast is gekeken in hoeverre het opsporingsonderzoek bijdroeg aan een betere informatiepositie jegens (in het *online* domein vaak anonieme) verdachten en hun modus operandi en hoe deze informatie kon worden gebruikt om acties te verrichten, die niet alleen gericht zijn op opsporing en vervolging van verdachten maar ook op het tegenhouden van illegale *online* activiteiten.

Methoden van onderzoek

Om de onderzoeksvragen te beantwoorden, zijn verschillende onderzoeksmethoden gebruikt. Door middel van literatuuronderzoek en deskresearch is achtergrondkennis verzameld om een beeld te kunnen schetsen van de aanpak van cybercriminaliteit. Daarnaast is een analyse gemaakt van politiedossiers van opsporingsonderzoeken naar *hightech* cybercriminaliteit. Wij hebben hiervoor acht dossiers van afgeronde opsporingsonderzoeken bestudeerd uit de periode 2014-2018. Ook is gekeken naar drie publiek-private samenwerkingsprojecten.
Bij de start van het onderzoek is een bijeenkomst belegd met een aantal experts van politie en OM. Aan hen is gevraagd om een lijst te maken van *hightech* opsporingsonderzoeken. Omdat dit onderzoek erop gericht was om meer zicht te krijgen op de mogelijkheden en dilemma's waar politie en OM mee te maken krijgen bij de aanpak van cybercriminaliteit is ook gevraagd naar opsporingsonderzoeken waar de knelpunten speelden die in eerder onderzoek zijn geïdentificeerd. Door middel van het dossieronderzoek werd nagegaan welke methoden van onderzoek

zijn ingezet tijdens het opsporingsonderzoek, hoe de onderzoeken zijn verlopen en welke resultaten ze hebben opgeleverd.

Tot slot zijn tweeënveertig interviews afgenomen met medewerkers van de politie, cyberofficieren van justitie en medewerkers van private partijen om een completer beeld te krijgen van de aanpak van cybercriminaliteit. Naast overkoepelende vragen boden interviews met zaaksofficieren en teamleiders die betrokken zijn geweest bij de geselecteerde zaken de mogelijkheid om meer inzicht te krijgen in de informatie en afwegingen die mogelijk niet in een dossier terecht zijn gekomen, maar wel een rol hebben gespeeld bij de gemaakte keuzes tijdens het opsporingsonderzoek. Ook gaven de interviews inzicht in de dilemma's en problemen waarmee de politie te maken krijgt.

Het grootste deel van de data is verzameld bij Team High Tech Crime, omdat dit team met name het type zaken onderzoekt dat binnen de scope van het huidige onderzoek valt.

Resultaten: opsporingsonderzoeken naar cybercriminaliteit

In tegenstelling tot de regionale cybercrimeteams werkt THTC vrijwel niet aangifte gestuurd. Hoewel het in theorie mogelijk is dat een THTC-onderzoek start op basis van een aangifte, laat de praktijk zien dat van *hightech* crime zelden aangifte wordt gedaan. Dat beeld is ook terug te zien in de dossiers die zijn bestudeerd voor dit onderzoek. Het enige onderzoek dat is gestart naar aanleiding van een aangifte is een zaak bij een regionale eenheid. Van de zeven bestudeerde THTC-onderzoeken zijn zes onderzoeken gestart naar aanleiding een tip van een private partij en/of buitenlandse politiedienst.

Omdat zich meer zaken aandienen dan opgepakt kunnen worden, moeten keuzes worden gemaakt over welke zaken opgepakt worden door de opsporingsdiensten. Of een zaak wordt opgepakt hangt zowel af van de beleidsprioriteiten die zijn gesteld als van de ernst van een zaak. Hoewel opsporingsonderzoeken als primair doel hebben om verdachten op te sporen en vervolgen, kan een onderzoek ook uit een meer strategisch oogpunt worden gestart, bijvoorbeeld vanuit een wens om meer kennis ten behoeve van het strafproces op te bouwen over een cybercrimineel fenomeen of een bepaalde criminele werkwijze. Die kennis kan dan worden benut bij het opsporen en tegenhouden van die vorm van criminaliteit.
Soms gaat het dan niet eens over cybercriminaliteit in de meest enge zin van het woord, zoals bijvoorbeeld een zaak over cryptocommunicatie. Daarbij was een reden om de zaak op te pakken het feit dat er in de georganiseerde criminaliteit veel gebruik werd gemaakt van cryptotelefoons en dat dit de reguliere opsporings-onderzoeken belemmerde. De techniek achter de telefoons was zo complex dat het onderzoek bij THTC terecht kwam. Hoewel in de interviews een aantal keer benoemd is dat het soms wat lastig uit te leggen is dat THTC ook dit soort zaken oppakt, is er wel een bredere overtuiging dat het juist belangrijk is om ook dit soort zaken te doen, omdat de impact hiervan wel degelijk groot is.

Doelen

Een opsporingsonderzoek wordt officieel alleen gestart als er opsporingsindicatie is, sporen waarmee mogelijke verdachten kunnen worden opgespoord en vervolgd,

omdat alleen dan opsporingsbevoegdheden mogen worden ingezet. Bij lang niet alle onderzoeken wordt echter bij een verdachte uitgekomen. Soms is dat al snel na aanvang van een onderzoek duidelijk en dan wordt nagedacht of er met de verkregen informatie ook andere doelen bereikt kunnen worden. Bijvoorbeeld zicht krijgen op een bepaald criminaliteitsfenomeen, om die kennis in volgende opsporingsonderzoeken te kunnen gebruiken of om tegenhoudmaatregelen in te zetten.

Met de vooraf opgestelde onderzoeksdoelen wordt in de praktijk flexibel omgegaan, ook omdat van tevoren nog niet bekend is welke informatie het onderzoek zal opleveren en dus welke doelen ermee kunnen worden gediend. Met het verkrijgen van extra informatie gedurende het onderzoek kunnen doelen soms worden gewijzigd. Zo kan bijvoorbeeld blijken dat het niet lukt om een verdachte te identificeren of vervolgen waardoor de nadruk komt te liggen op de inzet van tegenhoudmaatregelen. Ook komt het voor dat er gedurende een onderzoek juist meer mogelijk is dan men van tevoren dacht.

Opsporingsmiddelen en -methoden

De opsporingsactiviteiten in de bestudeerde dossiers bestonden, vooral in de startfase van een onderzoek, voornamelijk uit het vorderen en veiligstellen van servergegevens. Nader onderzoek aan servergegevens geeft inzicht in het soort data dat op een server staat opgeslagen en over het gebruik van een server. Soms werd deze vordering gedaan door een server fysiek veilig te stellen en andere keren door het maken van een forensische kopie of een *snapshot*. Daarna werden de digitale sporen nader onderzocht. Verder werd er in opsporingsonderzoeken veel gebruikgemaakt van internettaps om informatie te verzamelen en werd er onderzoek gedaan naar netwerkverkeer. De informatie die hiermee werd verkregen, kon worden gebruikt om de verdere richting van een opsporingsonderzoek te bepalen. Ook werden deze gegevens bestudeerd om na te gaan of de verdachte mogelijk ergens zijn of haar identiteit onthult. Hierbij moet worden opgemerkt dat de inzet van deze middelen niet bij elk onderzoek evenveel informatie opleverde.

Verder was in de dossiers die zijn onderzocht terug te zien dat wanneer er nog geen verdachte in beeld is, er eigenlijk uitsluitend digitale opsporingsmiddelen werden ingezet. Wanneer er Nederlandse verdachte(n) in beeld kwamen, werd veelal overgegaan tot een meer tactisch opsporingsonderzoek waarbij ook meer traditionele (‘offline’) opsporingsmiddelen en –methoden werden ingezet. Zo werden naast internettaps ook telefoontaps geplaatst die inzicht gaven in contacten die verdachten hadden met elkaar en anderen en in zaken die hen bezighielden. Dit werd vaak gecombineerd met financieel onderzoek om geldstromen in kaart te brengen om aan te tonen dat er sprake is van bijvoorbeeld witwassen.

Ook is in alle vijf de bestudeerde dossiers waarin Nederlandse verdachten in beeld kwamen gebruikgemaakt van bevoegdheden die vallen onder werken onder dekmantel. Deze bevoegdheden werden zowel online als offline ingezet. Dit is opvallend, gezien het geringe aantal ‘offline’ zaken waarin deze bijzondere opsporingsbevoegdheden normaliter worden ingezet. Dat kan te maken hebben met de ernst van de bestudeerde zaken, maar wellicht speelt ook mee dat bij de aanpak van dit soort nieuwe cybercriminele delicten, waarbij traditionele opsporingsstrategieën niet altijd toereikend zijn, ook nieuwe gedachtenvorming plaatsvindt over de inzet en zwaarte van al bestaande opsporingsbevoegdheden.

Mogelijkheden tot vervolging

In dit onderzoek werden in vijf van de acht bestudeerde dossiers verdachten geïdentificeerd. In vier zaken ging het om Nederlandse hoofdverdachten. Drie van deze zaken hebben inmiddels tot veroordelingen geleid; een *ransomewarez*aak, een *phishing*zaak, en de zaak die betrekking had op cryptocommunicatie. In de *ransomware*zaak werden taakstraffen en een voorwaardelijke gevangenisstraf opgelegd. In de *phishing*zaak gevangenisstraffen van vijf jaar. Dat is tevens de hoogst opgelegde straf voor dit specifieke delict tot nu toe. In de zaak die betrekking had op cryptocommunicatie is de hoofdverdachte door de rechtbank veroordeeld tot een gevangenisstraf van 4,5 jaar. In de vierde zaak, over DDoS-aanvallen, is vanwege de jonge leeftijd van de verdachte een alternatieve afdoening opgelegd en zijn *knock and talk* gesprek-ken gevoerd met de afnemers van de dienst. In de *darkweb*zaak met twee buitenlandse hoofdverdachten zijn de grootste Nederlandse aanbieders van de illegale producten strafrechtelijk vervolgd. Bij een deel van de overige aanbieders en afnemers heeft de politie *knock and talk* gesprekken ingezet.

Hoewel met name de THTC-onderzoeken niet altijd leiden tot vervolgbare verdachten, heeft de strafrechtelijke aanpak voor deze moeilijk vervolgbare delicten in de optiek van de geïnterviewden wel degelijk meerwaarde. Een criminele infrastructuur is voor autonome, zelfstandig opererende, groeperingen makkelijk te vervangen. Als interventies zich alleen op de verstoring van de infrastructuur zouden richten heeft dit kortdurend effect, omdat nieuwe infrastructuren ontstaan en activiteiten elders worden voortgezet. Het is daarom juist van belang om opsporingsonderzoeken te blijven verrichten die erop gericht zijn om verdachten te identificeren en vervolgen. Verder leveren de THTC-onderzoeken naar *facilitators* in een aantal gevallen geen hoofdverdachte op, maar wel informatie over andere vormen van criminaliteit die vervolgens in andere opsporingsonderzoeken kon worden gebruikt, of informatie die kon worden gebruikt bij de inzet van tegenhoudmaatregelen.

Tegenhoudmaatregelen

Uit dit onderzoek komt naar voren dat opsporing en tegenhouden van criminele processen hand in hand gaan, omdat dat in de optiek van de geïnterviewden de meest effectieve manier is om cybercriminaliteit aan te pakken. Hierbij werd ook verwezen naar de aanpak bij ondermijning, waar de aanpak heel specifiek is gericht op het criminele verdienmodel. Het samenspel tussen opsporen en tegenhouden is van belang omdat kennis uit de opsporingsonderzoeken gebruikt kan worden om inzicht te krijgen in die criminele processen en om de kennis hierover up-to-date te houden. Met alleen tegenhoudmaatregelen wordt slechts een klein deel van het proces zichtbaar, terwijl met een aanhouding of inbeslagname het hele proces gereconstrueerd kan worden en de sleutelfiguren kunnen worden geïdentificeerd. Opsporen zorgt dan niet alleen voor kennisopbouw, maar heeft ook door de afschrikkende werking een verstorend effect.

Juridisch gezien levert het uitvoeren van tegenhoudmaatregelen in de opsporingspraktijk soms discussies op. De politie heeft een bredere taak dan het OM. Dat roept de vraag op welk mandaat het OM heeft bij tegenhoudvraagstukken. Voor tegenhoudmaatregelen is inzicht nodig in het criminele proces dat vaak alleen verkregen kan worden met de inzet van BOB-middelen. Dat kan problematisch zijn wanneer bij de start van een onderzoek al snel duidelijk is dat er geen dader geïdentificeerd kan

gaan worden, terwijl de maatschappelijke impact van een cyberdelict wel erg groot is en op een andere manier interveniëren gewenst is. Voor de inzet van opsporingsbevoegdheden ten behoeve van verstoring bestaat tot op heden geen wettelijke grondslag. Uit de interviews blijkt dat in de praktijk nog niet tot problemen te leiden, maar soms komt men hiermee wel in een grijs gebied.

Dilemma's bij de aanpak van cybercriminaliteit

Tijdens de uitvoering van dit onderzoek werd duidelijk dat de wensen vanuit de opsporingspraktijk aan de ene kant en de beleidsmatige en juridische kaders aan de andere kant soms zorgen voor een spanningsveld in de aanpak van cybercriminaliteit. Hier wordt in de twee onderstaande paragrafen nader op ingegaan.

Informatiepositie

Ten eerste rondom de informatiepositie van de opsporing. Om slim op te sporen en onderbouwde keuzes te kunnen maken in het strafproces is het belangrijk om een goede informatiepositie op te bouwen ten behoeve van dat strafproces. De politie zou graag los van concrete onderzoeken samen met andere partijen activiteiten van (internationale) criminele groeperingen, *facilitators* en andere daders willen blijven volgen om daar een informatiepositie over op te bouwen. Om dit te bewerkstelligen streeft THTC naar een datagedreven manier van werken. Zo kan gekeken worden of er verbanden kunnen worden gelegd tussen data uit verschillende opsporingsonderzoeken om bijvoorbeeld na te gaan of er overeenkomsten zijn in modus operandi of gebruikte *malware*. Het OM en de politie mogen echter geen opsporingsbevoegdheden inzetten puur ten behoeve van het verbeteren van hun informatiepositie. Ook mogen gegevens uit verschillende opsporingsonderzoeken niet zonder meer met elkaar in verband worden gebracht. Als informatie wordt veiliggesteld is dat vanuit strafvorderlijke context. In het kader van de Wpg kan informatie eventueel wel, met toestemming, ook in ander onderzoek worden gebruikt. Deze uitgangspositie om in principe geen opsporingsbevoegdheden in te mogen zetten ten gunste van het verbeteren van de informatiepositie is soms lastig. Immers, als er goed zicht is op wat er speelt, is men ook beter in staat daar effectief en efficiënt op te reageren.

Om cybercriminele fenomenen goed te kunnen doorgronden, zijn vaak meerjarige onderzoeken nodig. Deze fenomeenonderzoeken kosten echter veel tijd en capaciteit en de resultaten van deze onderzoeken zijn vaak (vooral) gelegen in het tegenhouden en verstoren van cybercriminaliteit en minder in het identificeren en vervolgen van daders. De minder goed meetbare alternatieve interventies schuren soms met de beleidsmatige kwantitatieve resultaatverplichtingen. De keus tussen voldoen aan kwantitatieve doelen of het vergroten van de kennispositie is niet altijd zo zwart-wit, maar zorgt in de praktijk toch regelmatig voor een worsteling.

Informatie-uitwisseling

Ten tweede zijn in dit onderzoek problemen rondom informatiedeling nadrukkelijk naar voren gekomen. Deze problemen spelen allereerst een rol bij slachtoffernotifi catie. Er is op dit moment geen duidelijke partij die daar verantwoordelijk voor is. De hoeveelheid slachtoffers van bijvoorbeeld een *hack* is regelmatig zo groot dat de

opsporing het notificeren van deze slachtoffers er niet zomaar bij kan doen. Daarbij is het proces van notificeren complex. Vaak zijn abstracte datasets als lijsten met IP-adressen het uitgangspunt. Verder kan het delen van deze informatie juridisch lastig zijn. Wat in de praktijk logisch en voor de hand liggend lijkt om te doen, blijkt juridisch niet altijd haalbaar. Dit zorgt voor onduidelijkheid en inefficiëntie. In één van de bestudeerde onderzoeken betekende dit dat meerdere Nederlandse partijen later werden genotificeerd dan wenselijk was en dat het notificeren via een lastige omweg plaatsvond. Daardoor zijn deze Nederlandse partijen een onnodig lange tijd blootgesteld aan potentieel gevaar.

Daarnaast hebben de moeilijkheden ook betrekking op publiek-private samenwerking. Publiek-private samenwerking is een wezenlijk onderdeel van de integrale aanpak van cybercriminaliteit. Een samenwerking met private partijen biedt de mogelijkheid om andere expertise in de aanpak van cybercriminaliteit te brengen en extra informatie te vergaren voor zowel de politie als de private partij.
Toch kleven hier ook praktische bezwaren aan. Publieke en private partijen hebben andere, en mogelijk tegenstrijdige, belangen. Het is goed als partijen zich hier gedurende de gehele looptijd van de samenwerking bewust van te zijn. Ook kan de wet- en regelgeving omtrent het delen van informatie een samenwerking bemoeilijken. Zo heeft men naast de Wet Politiegegevens (Wpg) ook te maken met de Algemene Verordening Gegevensbescherming (AVG), Wet Beveiliging Netwerk- en Informatiesystemen (Wbni), de Wet Bescherming Persoonsgegevens (Wbp) en eventueel geheimhoudingsplichten. Hoewel het goed is om enige mate van terughoudendheid te hanteren bij het delen van informatie kan onduidelijkheid bij partijen over de wetgeving tot gevolg hebben dat er te terughoudend wordt omgegaan met het delen van informatie.

Internationale samenwerking

Bij de aanpak van cybercriminaliteit is men in veel gevallen afhankelijk van internationale samenwerking. Zelfs aan de kleinere zaken zit vaak een internationaal component. Internationale samenwerking is voor de opsporing dan ook belangrijk. Met verschillende Europese opsporingsdiensten, zoals in Engeland en Duitsland, wordt door THTC veelvuldig en goed samengewerkt. Datzelfde geldt voor de Amerikaanse FBI. Daarbij kan gedacht worden aan het verkrijgen van opsporingsinformatie, het gecoördineerd opsporen en aanhouden van verdachten en het gecoördineerd ontplooien van verstoringsactiviteiten.

Hoewel goede internationale samenwerking successen kan brengen, wordt de lange doorlooptijd van internationale rechtshulpverzoeken als één van de grootste knelpunten genoemd in dit onderzoek. Er is grote variatie in hoe lang een team moet wachten op de resultaten van zo'n verzoek. Uit dit onderzoek blijkt dat opsporingsfunctionarissen positief zijn over de rol van Europol, maar daarbij werd opgemerkt dat het succes sterk afhankelijk was van de capaciteit en prioriteiten in samenwerkende landen. Elk land heeft maar beperkte rechtshulpcapaciteit. Dat geldt ook voor Nederland. De realiteit is dan dat men soms pas reageert op het moment dat de informatie al lang weg is. Wat wel is verbeterd in de internationale samenwerking ten opzichte van een aantal jaar geleden, is dat in diverse landen steeds meer kennis aanwezig is en ook de contacten met veel landen steeds beter worden.

Tot slot

Uit dit onderzoek zijn een aantal punten naar voren gekomen die de vraag oproepen hoe de kaders die gelden voor de aanpak van traditionele criminaliteit zich verhouden tot de aanpak van (complexe) cybercriminaliteit. Het is daarom goed om kritisch te kijken of de huidige wet- en regelgeving toereikend is voor de omgang met informatie ten behoeve van de aanpak van cybercriminaliteit. Daarnaast vraagt het van partijen dat duidelijke kaders worden geschreven waarin informatie kan worden gedeeld. Zodat als er urgentie is en partijen informatie willen delen, die belangrijke informatie ook kan worden gedeeld.

1 Inleiding

Nederland beschikt over een goede ICT-infrastructuur waardoor het een aantrekkelijk land is voor cybercriminelen.[1] Illegale activiteiten voltrekken zich op Nederlandse servers of worden (on)bewust gefaciliteerd door in Nederland gevestigde *hosters*.[2],[3] De afgelopen jaren zijn er verschillende grote strafrechtelijke onderzoeken naar cybercriminaliteit verricht die veel aandacht kregen in de media, zoals de *ransomware* aanval op de universiteit Maastricht.[4]

Uit de afgelopen cybersecuritybeelden van het NCSC blijkt dat cybercriminaliteit een groeiend probleem is, dat potentieel veel maatschappelijke en financiële schade kan veroorzaken.[5] De omvang en ernst van de digitale dreiging in Nederland is nog steeds aanzienlijk en blijft zich ontwikkelen. Cyberaanvallen blijken lonend, laagdrempelig uit te voeren en weinig riskant voor de pleger. In het Cybersecuritybeeld Nederland (CSBN) 2020 staat beschreven dat de grootste cyberdreiging uitgaat van sabotage en spionage door statelijke actoren. Ook bestaat het risico van '(grootschalige) uitval van digitale diensten, processen of systemen' en het risico van 'cyberaanvallen door criminele actoren die het te doen is om economisch gewin' (CSBN, 2020 p. 7). In de begroting van Justitie en Veiligheid is structureel 95 miljoen euro gereserveerd om de doelstellingen in de Nederlandse Cyber Security Agenda (NCSA) uit te voeren.[6] Deze agenda bevat een breed palet aan doelstellingen en maatregelen om de cyberveiligheid in Nederland te vergroten en cybercriminaliteit aan te pakken.[7] De aanpak van cybercriminaliteit moet integraal gebeuren[8]. Hiermee wordt bedoeld dat het fenomeen in de breedte en door diverse partijen, onder andere in publiek-private samenwerking, moet worden aangepakt.

De integrale aanpak heeft al langer de aandacht van de politiek. In december 2016 heeft de Tweede Kamer de motie-Recourt aangenomen, waarin het toenmalige kabinet opgeroepen werd om 'in samenspraak met de private sector te komen tot een integraal plan van aanpak voor cybercriminaliteit, waarbij aandacht is voor preventie tot en met vervolging'.[9] In april 2018 informeerde Minister Grapperhaus van Justitie en Veiligheid de Tweede Kamer in reactie op de motie-Recourt over de integrale aanpak van cybercriminaliteit.[10] In deze kamerbrief worden vier sporen benoemd waaruit de aanpak moet bestaan: (i) er wordt geïnvesteerd in preventie,

---

1 TK brief Voortgang integrale aanpak van cybercrime, 29 juni 2020.

2 Een *hoster* is een bedrijf dat de mogelijkheid biedt om serverruimte af te nemen.

3 Veelvoorkomende vormen van cybercriminaliteit en technische begrippen worden nader toegelicht in bijlage 2 en bijlage 3.

4 Zie bijvoorbeeld: https://www.trouw.nl/nieuws/universiteit-maastricht-over-de-hack-we-konden-niet-anders-dan-betalen~bb2f0c13/?referrer=https%3A%2F%2Fwww.bing.com%2F en https://www.ad.nl/tech/politie-en-justitie-kraken-chatdienst-gebruikt-door-criminelen-miljoenen-berichten-live-meegelezen~a8ec7f96/?referrer=https%3A%2F%2Fwww.google.nl%2F

5 Cybersecuritybeeld Nederland 2018, NCSC; Cybersecuritybeeld Nederland 2019, NCSC; Cybersecuritybeeld Nederland 2020, NCSC

6 https://www.rijksoverheid.nl/actueel/nieuws/2018/09/18/justitie-en-veiligheid-pakt-nieuwe-vormen-van-criminaliteit-aan. Bezocht november 2020.

7 NCSC (2018). Nederlandse Cybersecurity Agenda.

8 TK brief integrale aanpak cybercriminaliteit, 20 april 2018.

9 *Kamerstukken II,* 2016/2017, 34 550 VI, nr. 53.

10 TK brief integrale aanpak cybercrime, 20 april 2018.

(ii) de opsporing wordt versterkt, criminele activiteiten worden verstoord en daders worden aangepakt, (iii) de ondersteuning van slachtofferschap wordt toegesneden op cybercriminaliteit, (iv) de wetenschappelijke kennis over cybercriminaliteit wordt vergroot. Het voorliggende onderzoek sluit aan bij het vierde spoor en maakt deel uit van een groter onderzoeksprogramma dat op verzoek van, en in samenwerking met, verschillende beleidsdirecties door het WODC is opgesteld en moet voorzien in kennis ten behoeve van de integrale aanpak van cybercriminaliteit.[11]

De landelijke beleidsdoelstellingen die zijn geformuleerd over de taakuitvoering van de politie staan in de Veiligheidsagenda.[12] Hierin is een sectie gewijd aan de aanpak van cybercriminaliteit, waarin kwantitatieve doelen worden gesteld aan het aantal en type cyberzaken dat de politie jaarlijks moet afronden. Naast de reguliere opsporingsonderzoeken en onderzoeken naar fenomenen krijgt ook de inzet van 'aanvullende en alternatieve interventies' door de politie nadrukkelijk de aandacht in de Veiligheidsagenda.[13] De afspraken in de veiligheidsagenda en de uitwerking daarvan worden verder toegelicht in hoofdstuk 3. Ook het Openbaar Ministerie (OM) heeft een strategie geformuleerd over een brede aanpak van cybercriminaliteit die aansluit bij de NCSA en de Veiligheidsagenda.[14]

Op 26 juni 2018 is het wetsvoorstel Computercriminaliteit III (CCIII) door de Eerste Kamer aangenomen.[15] Deze wet biedt de politie nieuwe onderzoeksinstrumenten in de opsporing, aangezien hiermee de mogelijkheden voor digitaal rechercheren worden verruimd. Zo geeft deze wet politie en justitie de bevoegdheid tot heimelijk en op afstand binnendringen van geautomatiseerde werken en de bevoegdheid tot het ontoegankelijk maken van gegevens. Daarnaast zijn er nog een aantal wijzigingen omtrent de strafbaarstelling van delicten. Zo is het wederrechtelijk overnemen en helen van gegevens en online handelsfraude strafbaar, en houdt de wet een verruiming in van de reeds eerder bestaande strafbaarstellingen van *grooming*.[16] In dit onderzoek zijn geen zaken meegenomen waarbij de bevoegdheden van de wet CCIII zijn ingezet, omdat de wet nog niet in werking was getreden toen de geselecteerde opsporingsonderzoeken liepen.

In dit hoofdstuk worden eerst de uitdagingen beschreven waar de politie mee te maken krijgt bij de aanpak van cybercriminaliteit. Daarna worden verschillende definities besproken die worden gehanteerd bij het beschrijven van cybercriminaliteit en het onderscheiden van verschillende delicttypen binnen de cybercriminaliteit. Daarna worden de doel- en vraagstelling van het onderzoek toegelicht, waarna de methoden van onderzoek worden beschreven. Tot slot volgt de opbouw van het rapport.

---

[11] Andere reeds afgeronde onderzoeken die deel uitmaken van dit onderzoeksprogramma richtten zich op de aard en omvang van cybercriminaliteit: Beerthuizen, Sipma & van der Laan (2020); Cyberdaders: Van der Wagen, Van 't Zand-Kurtovic & Matthijsse (2019). En op slachtofferschap van cybercriminaliteit: Sipma & Leijsen (2019).

[12] Veiligheidsagenda 2019-2022.

[13] TB brief Voortgang integrale aanpak van cybercrime, 29 juni 2020.

[14] Openbaar Ministerie: Aanpak van cybercrime 2019-2022. Missie, visie en strategie.

[15] Voluit 'Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)'. De ingangsdatum van deze nieuwe wet is 1 maart 2019.

[16] Custers (2018).

1.1 Opsporing, vervolging en het tegenhouden van cybercriminaliteit

De kerntaak van de politie en het OM is opsporing en vervolging van misdrijven. Bij cybercriminaliteit is het uitvoeren van die kerntaak om meerdere redenen lastig. Zo kent het Internet geen fysieke of geografische grenzen. Kenmerkend voor cybercriminaliteit is de schaal waarop het kan worden uitgevoerd. Dat komt enerzijds door de inzet van IT-middelen, wat het bereik vergroot, en anderzijds door de omvangrijke ondergrondse dienstverlening (zie ook Van de Sandt, 2019) Daarnaast moet het bewijs vaak grotendeels online worden gezocht en verzameld. Dat heeft invloed op het opsporingsproces en betekent ook dat internationale samenwerking van belang is bij het tegengaan van cybercriminaliteit. Servers kunnen in een ander land staan, waardoor het gecompliceerder is om bij informatie te komen dan bij opsporingsonderzoeken die zich binnen de nationale landsgrenzen afspelen. Verder kan informatie versleuteld zijn, is data vluchtig, kunnen daders zich gemakkelijk in de anonimiteit begeven en in het buitenland bevinden, en tot slot is ook niet altijd duidelijk is welke juridische bevoegdheden er zijn en wat de reikwijdte van bestaande bevoegdheden is, met name met betrekking tot het delen van informatie.

Voor de opsporing van cybercriminaliteit beschikt de politie op landelijk niveau over het specialistische Team High Tech Crime (THTC) en zijn, meer recent, met investeringen uit het Regeerakkoord gespecialiseerde cybercrimeteams op regionaal niveau versterkt. De cybercrimeteams werken samen met het THTC in een landelijke structuur en ondersteunen districtsrecherches en basisteams bij de kennisopbouw voor de uitvoering van reguliere onderzoeken naar cybercriminaliteit. Conform de afspraken in de Veiligheidsagenda is in 2019 door de politie en het OM gestart met een 'eenheidsoverstijgende fenomeenaanpak'. Kennis over cybercriminele fenomenen wordt geclusterd in regio's, waarbij elke politie-eenheid in Nederland een eigen aandachtsgebied heeft (zie Boekhoorn, 2020 voor een uitgebreide beschouwing).

Omdat het opsporen en vervolgen van cybercriminele daders om meerdere redenen lastig kan zijn, wordt door de politie en het OM ook voor niet-strafrechtelijke oplossingen gekozen bij de aanpak van cybercriminaliteit. Voorbeelden van andersoortige oplossingen zijn verstoring van het criminele proces door het offline halen van servers, of inzetten op preventie door middel van waarschuwingscampagnes, zoals recent tegen Whatsapp-fraude. Bij de aanpak van cybercriminaliteit wordt ook regelmatig publiek-private samenwerking gezocht en zijn diverse projecten gestart die gericht zijn op het tegengaan van verschillende cyberdelicten. In hoofdstuk 5 wordt nader ingegaan op deze publiek-private samenwerkingen.

Zoals eerder beschreven worden er veel middelen ingezet bij de aanpak van cybercriminaliteit. Toch is er maar weinig bekend over hoe de opsporing, vervolging en verstoring van cybercriminaliteit verloopt.[17],[18] Het huidige onderzoek moet inzicht bieden in de opsporing en vervolging van verschillende (ernstige) vormen van cybercriminaliteit door de politie. Hierbij wordt gekeken naar ernstige[19] zaken met

[17] NCSC (2018); Leukfeldt (2017).

[18] Er is wel eerder onderzoek verricht binnen de Europese Unie naar georganiseerde cybercriminaliteit, waarbij het WODC het Nederlandse deel voor haar rekening nam, zie Bulanova-Hristova, G., et al. (2016). Daarnaast is het thema van de meest recente monitor georganiseerde misdaad 'georganiseerde criminaliteit en ICT', zie Kruisbergen et al. (2018).

[19] De ernst van de zaak kan zowel bepaald worden door het type delict als door de (potentiële) impact.

een *hightech* component. Deze component kan ofwel aanwezig zijn door het leveren van een *hightech* (technisch geavanceerde) opsporingsinspanning door de politie, bijvoorbeeld door middel van een technisch complex onderzoek, ofwel doordat de daders zich bedienden van *hightech* modus operandi door bijvoorbeeld nieuwe criminele werkwijzen. Met deze selectie wordt gekeken welke eisen nieuwe, innovatieve vormen van cybercriminaliteit en/of zaken met een grote maatschappelijke impact stellen aan de aanpak van dit soort complexe zaken.

1.2 Definities

In de literatuur is geen eenduidigheid over het begrip cybercriminaliteit. Er wordt al vrij snel gesproken over cybercriminaliteit als ICT in enige mate een rol heeft bij het plegen van een delict (Van der Wagen, Oerlemans & Weulen Kranenbarg, 2020). In diverse Nederlandstalige (beleids)stukken, zoals de Veiligheidsagenda, wordt een tweedeling gehanteerd waarbij onderscheid wordt gemaakt tussen cybercriminaliteit in ruime zin en cybercriminaliteit in enge zin.[20] Bij cybercriminaliteit in enge zin is ICT zowel het middel als het doel. Voorbeelden die hierbij genoemd worden zijn *hacking, ransomware en DDoS*-aanvallen[21]. Onder cybercriminaliteit in ruime zin wordt iedere vorm van (traditionele) criminaliteit verstaan waarbij gebruik wordt gemaakt van ICT. Voorbeelden hiervan zijn online drugshandel of identiteitsfraude. Cybercriminaliteit in ruime zin wordt ook wel gedigitaliseerde criminaliteit genoemd en cybercriminaliteit in enge zin kortweg 'cybercrime'.

De gehanteerde tweedeling is in de praktijk echter niet altijd te handhaven. Het onderscheid tussen cybercriminaliteit in enge zin en cybercriminaliteit in ruime zin neemt af, mede door de toenemende verwevenheid van digitale criminaliteit en traditionele criminaliteit. Hierdoor is het met name voor de politieteams in de regio's soms lastig om beslissingen te nemen over zaken (Boekhoorn 2020). In meer recente rapportages en in internationale literatuur wordt veelal gebruikgemaakt van een classificatie op basis van de mate van techniek die nodig is om een delict te plegen (zie bijvoorbeeld NCSB, 2020; Van de Sandt, 2019; Yar, 2016). Deze driedeling, die ook gebruikt wordt binnen de politie, is gebaseerd op de typologie van Wall (2007). Hierbij wordt onderscheid gemaakt tussen *computer-focused,*[22] *computer-assisted* en *computer-enabled* crime.

- Computer-focused crime zijn misdrijven die niet kunnen bestaan zonder ICT. ICT is hierbij het doelwit en het middel van de aanvallen. Bijvoorbeeld DDoS-aanvallen, of hacking.
- Computer-assisted crime is criminaliteit die voorheen analoog, maar nu hoofdzakelijk digitaal wordt gepleegd. Bijvoorbeeld Marktplaatsfraude en CEO-fraude.
- Computer-enabled crime betreft alle vormen van traditionele criminaliteit die worden gepleegd met behulp van ICT, maar die niet gericht zijn tegen ICT. ICT kan wel een hulpmiddel zijn bij de modus operandi van het delict. Zo kan een

[20] Veiligheidsagenda 2019-2022; NCSC (2018); Holt, & Bossler (2014). Een andere veel gebruikte benaming is cyber-enabled crime voor cybercriminaliteit in ruime zin en cyber-dependent crimes voor cybercriminaliteit in enge zin.

[21] *Hacking* is het met kwaadaardige bedoelingen proberen in te breken in ICT-systemen. *Ransomware* is gijzelsoftware. Het is een type *malware* dat systemen of informatie daarop blokkeert en alleen tegen betaling van losgeld weer toegankelijk maakt. Bij een DDoS-aanval een bepaalde dienst (bijvoorbeeld een website) niet beschikbaar wordt gemaakt door deze te bestoken met een grote hoeveelheid dataverkeer.

[22] Ook wel *cyber-dependent* of *cyber-oriented crime* genoemd.

liquidatie niet digitaal worden uitgevoerd, maar versleutelde communicatie kan wel bijdrage aan de uitvoering ervan. Datzelfde geldt voor drugshandel via online marktplaatsen. In toenemende mate zijn zo alle vormen van criminaliteit in zekere zin computer-enabled door te toename van ICT-gebruik bij traditionele criminaliteit.

Naast de definities die gehanteerd worden in (criminologische) literatuur is er ook een juridisch onderscheid. Op basis van de in het Cybercrime-Verdrag gehanteerde categorieën zijn Koops en Oerlemans (2019) tot de volgende driedeling gekomen, die lijkt op de hierboven beschreven driedeling die door de politie wordt gehanteerd, maar op detailniveau licht afwijkt.

- Computergestuurde delicten: strafbare feiten tegen de vertrouwelijkheid, integriteit en beschikbaarheid van computergegevens en -systemen. Hierbij gaat het onder meer om het *hacken* van computersystemen of het uitvoeren van DDoS-aanvallen.
- Computergerelateerde delicten: strafbare feiten die gepleegd worden door gebruik te maken van computergegevens en -systemen. Hierbij spelen computergegevens of -systemen een substantiële rol, dat wil zeggen dat het delict anders niet had kunnen plaatsvinden. Daarbij gaat het bijvoorbeeld om *phishing* voor het ontfutselen van geld.
- Computerrelevante delicten: strafbare feiten waarbij computergegevens en -systemen relevant zijn als omgevingsfactor, maar geen substantiële rol spelen. Voorbeelden hiervan zijn het opslaan van kinderporno, maar het kan ook gaan om ander opgeslagen bewijsmateriaal dat relevant is bij delicten (zoals bij een moord).

In theorie is het onderscheid tussen verschillende vormen van cybercriminaliteit duidelijk. In de praktijk blijkt de afbakening lastiger omdat definities in elkaar overvloeien, overlap hebben, of net anders geïllustreerd worden. Dit geldt met name voor de termen *computer-enabled* en *computer-assisted* criminaliteit. De omschrijving van delicttypen die onder deze definities vallen wisselt soms tussen auteurs (zie bijvoorbeeld Wall, 2014 of Van de Sandt, 2019). Een voorbeeld van een delict dat soms anders geclassificeerd wordt, is drughandel via *online* marktplaatsen. Zoals ook beschreven door Kruisbergen et al. (2018) bepaalt de breedte van de definitie die men kiest welke delicten onder een bepaalde definitie vallen.

Samenvattend komt het erop neer dat er in de literatuur meestal gebruik wordt gemaakt van een twee-of driedeling wanneer er onderscheid wordt gemaakt tussen verschillende cyberdelicten. In dit onderzoek wordt geen specifieke indeling gekozen om het begrip cybercriminaliteit te operationaliseren. Dit onderzoek richt zich op alle drie van de bovenstaande vormen van cybercriminaliteit, zolang deze een *hightech* karakter hebben of de aanpak ervan een *hightech* karakter heeft. Het *hightech* karakter kenmerkt zich doordat het nieuwe, innovatieve of georganiseerde vormen van de genoemde vormen van cybercriminaliteit met een hoge (inter)nationale impact betreft. *Hightech* kan naast de vorm dus ook betrekking hebben op de aanpak van de verschillende cyberdelicten, bijvoorbeeld wanneer het gaat om een nieuwe, innovatieve manier van bestrijding.[23]

In dit rapport wordt in beginsel bij het beschrijven van zaken geen onderscheid gemaakt tussen de verschillende definities of classificaties en spreken we over cyberdelicten of cybercriminaliteit. Desalniettemin is het onderscheid tussen

[23] Interne documenten THTC.

cybercriminaliteit in enge zin en cybercriminaliteit in ruime zin wel relevant voor sommige vraagstukken die in de praktijk spelen. Zo speelt de definitie een rol in de kwantitatieve doelstellingen in de Veiligheidsagenda en de doelstellingen van het OM. Daarin wordt namelijk een beoogd aantal afgehandelde zaken gekoppeld aan verschillende vormen van cybercriminaliteit. Daarom zullen we in dit rapport terugkomen op het onderscheid tussen de definities van cybercriminaliteit waar dit relevant is voor de werkwijze van de politie en het OM.

1.3 Doel- en vraagstelling van het huidige onderzoek

Doel van dit onderzoek is nagaan welke keuzes worden gemaakt en welke opsporingsmiddelen worden ingezet bij de opsporing en vervolging van geavanceerde vormen van cybercriminaliteit. Daarnaast wordt als nevendoel ook gekeken in hoeverre door het opsporingsonderzoek een betere informatiepositie wordt opgebouwd jegens (in het online domein vaak anonieme) verdachten en door hen gehanteerde werkwijzen en hoe deze informatiepositie kan worden gebruikt om acties te verrichten die niet alleen gericht zijn op opsporing en vervolging van verdachten maar ook op het tegenhouden van illegale *online* activiteiten. De focus van het onderzoek ligt op het beschrijven van de opsporing en vervolging en de verstoring van cybercriminaliteit vanuit het perspectief van de politie en het Openbaar Ministerie.
Daarnaast wordt gepoogd na te gaan in hoeverre de (door opsporing en publiek-private samenwerking) toegenomen informatiepositie bijdraagt aan (a) mogelijkheden voor uiteindelijke aanhouding, (b) gerichtere tegenhoudmaatregelen (bijvoorbeeld met gepersonaliseerde waarschuwingen of het offline halen van servers). Doel van dergelijke maatregelen is het ontwrichten van het criminele proces. Ook kan op die manier preventief worden opgetreden tegen cybercriminaliteit. Verder wordt nagegaan in hoeverre van deze mogelijkheden gebruik wordt gemaakt en wat de motivatie is om wel of geen gebruik te maken van de geboden mogelijkheden.

Tot slot moet het onderzoek inzichtelijk maken welke mogelijkheden en beperkingen zich voordoen bij deze opsporingsonderzoeken. In een eerder onderzoek naar de aanpak van georganiseerde vormen van cybercriminaliteit in Nederland werden diverse knelpunten geïdentificeerd.[24] Knelpunten betroffen onder andere de internationale samenwerking bij opsporingsonderzoeken naar cybercriminaliteit en de informatiepositie van de politie op internet. Het voorliggende onderzoek moet inzichtelijk maken of voor de eerder beschreven knelpunten inmiddels oplossingen zijn gevonden, of deze mogelijke oplossingen nieuwe dilemma's met zich mee brengen en of er in de huidige situatie knelpunten bij zijn gekomen die eerder nog niet werden benoemd.

De centrale vraagstelling van het onderzoek luidt als volgt:
Hoe verloopt de opsporing, vervolging en verstoring van verschillende vormen van geavanceerde cybercriminaliteit en welke mogelijkheden en beperkingen doen zich voor bij deze onderzoeken?[25]

---

[24] Zie Odinotet al. (2017).

[25] In de oorspronkelijke vraag aan het WODC werd er onderscheid gemaakt tussen opsporing, vervolging en verstoring van cybercriminaliteit. Omdat opsporing en verstoring echter met elkaar verweven zijn bij de bestrijding van cybercriminaliteit worden deze begrippen in dit rapport samengevoegd en wordt waar mogelijk gesproken over 'de aanpak van cybercriminaliteit'.

1.4 Methoden van onderzoek

De benodigde gegevens voor dit onderzoek zijn verzameld door middel van (1) literatuuronderzoek (2), dossieronderzoek en (3) interviews. Door verschillende methoden te gebruiken om de onderzoeksvragen te beantwoorden wordt gepoogd een beeld te schetsen van de opsporing, vervolging en tegenhoudmaatregelen van ernstige vormen van cybercriminaliteit.

Met literatuuronderzoek en deskresearch is achtergrondkennis verzameld om een beeld te kunnen schetsen van de aanpak van cybercriminaliteit. De verzamelde literatuur bestond uit een combinatie van wetenschappelijke artikelen, grijze literatuur, kamerstukken en interne documenten. Omdat stukken over de aanpak van cybercriminaliteit voornamelijk grijze literatuur betreffen is naast wetenschappelijke zoekmachines ook gebruikgemaakt van Google en de sneeuwbalmethode om literatuur te zoeken. Verder is aansluitend aan de interviews aan respondenten gevraagd of zij over (interne) documenten beschikten die mogelijk relevant konden zijn voor dit onderzoek.

Daarnaast is dossieronderzoek verricht. Bij de start van het onderzoek is een bijeenkomst belegd met een aantal experts van politie en OM. Aan hen is gevraagd om een lijst te maken van *hightech* opsporingsonderzoeken die recent waren afgerond. Omdat dit onderzoek erop gericht is om meer zicht te krijgen op de mogelijkheden en dilemma's waar politie en OM mee te maken krijgen bij de aanpak van cybercriminaliteit is ook gevraagd naar opsporingsonderzoeken waar de knelpunten die in eerder onderzoek zijn geïdentificeerd een rol speelden. Aan de hand van de lijst met zaken die tijdens de expertmeeting zijn aangedragen, zijn gezamenlijk acht dossiers geselecteerd van nog niet eerder onderzochte zaken uit de periode 2014-2018.[26] Door middel van het dossieronderzoek werd nagegaan welke methoden van onderzoek zijn ingezet tijdens het opsporingsonderzoek, hoe de onderzoeken zijn verlopen en welke resultaten ze hebben opgeleverd. Om het dossieronderzoek te structureren is een aangepaste versie gebruikt van de topiclijst die eerder is ingezet voor de vijfde monitor georganiseerde criminaliteit (Kruisbergen et al., 2018). De thema's in de aangepaste versie van deze topiclijst waren meer specifiek gericht op de aanpak van cyberdelicten en de inzet van opsporingsmiddelen dan op het fenomeen in zijn algemeenheid en de onderlinge relaties binnen criminele samenwerkingsverbanden. Daarnaast zijn nog drie publiek-private samenwerkingsprojecten bestudeerd waarbij sprake was van samenwerking bij de aanpak van specifieke vormen van cybercriminaliteit. Om meer zicht op deze projecten te krijgen zijn interviews gehouden met directe betrokkenen en interne documenten bestudeerd.

In totaal zijn tweeënveertig semigestructureerde interviews afgenomen met medewerkers van de politie, cyberofficieren van justitie en medewerkers van private partijen om een completer beeld te krijgen van de aanpak van cybercriminaliteit. Naast overkoepelende vragen boden interviews met zaaksofficieren en teamleiders die betrokken zijn geweest bij de geselecteerde zaken de mogelijkheid om meer inzicht te krijgen in de informatie en afwegingen die mogelijk niet in een dossier terecht zijn gekomen, maar wel een rol hebben gespeeld bij de keuzes in de opsporing. Ook gaven de interviews inzicht in de dilemma's en problemen waarmee de politie te maken krijgt en nieuwe cybercriminele ontwikkelingen die zij zien. De

[26] In de periode van 2009-2013 zijn elf dossiers onderzocht voor het rapport 'organised cybercrime in the Netherlands'. Om overlap te voorkomen zijn in het huidige onderzoek alleen dossiers geselecteerd van na dit tijdvak.

interviews duurden gemiddeld een uur en vonden grotendeels plaats tussen januari 2020 en juli 2020, deels op de werklocatie van de geïnterviewde en deels telefonisch of via Webex.[27] De interviews zijn opgenomen en getranscribeerd. Na de uitwerking zijn de opnames van de interviews verwijderd. Met behulp van het programma Maxqda zijn de interviews gecodeerd en geanalyseerd. In eerste instantie is gebruikgemaakt van een open codering, waarna de data axiaal gecodeerd zijn (zie Boeije & Bleijenbergh, 2019). Hierbij zijn clusters gemaakt van codes, waarbij hoofdcodes en subcodes zijn onderscheiden.

Het grootste deel van de data is verzameld bij Team High Tech Crime. Dit team onderzoekt cyberzaken met een *hightech* component die vaak ook innovatief of technisch complex zijn. Zij onderzoeken dan ook met name het type zaak dat binnen de scope van het huidige onderzoek valt.[28] Zoals eerder is beschreven is een deel van het geld dat is vrijgemaakt voor de aanpak van cybercriminaliteit bedoeld om te investeren in de regionale cybercrimeteams. Kennis die bij THTC is opgedaan wordt overgedragen aan de regionale eenheden zodat zij ook zelfstandig grotere en complexere cyberonderzoeken kunnen oppakken. Daarom is ook een opsporingsonderzoek geïncludeerd dat door een cybercrimeteam van een regionale eenheid is gedaan en binnen de reikwijdte van het huidige onderzoek past.

1.4.1 Beperkingen

Zoals elk onderzoek kent ook dit onderzoek een aantal methodologische beperkingen. Ten eerste zijn maar acht opsporingsonderzoeken geïncludeerd. Dat komt omdat het aantal opsporingsonderzoeken dat binnen de scope van dit onderzoek viel beperkt was. Aangezien we voor dit onderzoek zicht wilden krijgen op besluitvormingsprocessen en dilemma's die spelen rondom de opsporing, vervolging en tegenhoudmaatregelen die zijn ingezet, zochten we opsporingsonderzoeken die groot genoeg waren om meerdere beslismomenten te bestuderen, en waar bij voorkeur ook verdachten in beeld kwamen om zicht te krijgen op mogelijkheden tot vervolging. Om die reden zijn de dossiers niet aselect geselecteerd, maar in overleg met operationeel experts. Deze selectie heeft daarom impact op de externe validiteit van de resultaten. Hoewel wij ons best hebben gedaan zo veel mogelijk betrokkenen bij cyberonderzoeken te spreken is met name het aantal specialisten op het gebied van *hightech* crime beperkt. Sommige rechercheurs en officieren die wij spraken waren betrokken bij meerdere opsporingsonderzoeken. Tot slot hebben de COVID-19 maatregelen invloed gehad op de dataverzameling van het onderzoek. Zo hebben we van één opsporingsonderzoek het dossier niet in kunnen zien en hebben we de informatie over dit onderzoek verzameld door middel van interviews. Ook heeft een deel van de interviews telefonisch of per videobellen plaatsgevonden in plaats van in persoon.

1.5 Opbouw van het rapport

In hoofdstuk 2 wordt het juridisch kader beschreven dat van toepassing is bij de aanpak van cybercriminaliteit. Hoofdstuk 3 gaat in op de uitwerking van de integrale aanpak van cybercriminaliteit door de politie en het OM. Hierbij worden zowel de

[27] Webex is een programma waarmee online videogesprekken kunnen worden gevoerd.

[28] Bij de aanpak van cybercriminaliteit zijn de opsporing en verstoring of tegenhouden geïntegreerde processen. Om die reden zullen beide processen bij de dataverzameling evenredig aan bod komen.

beleidsmatige kaders geschetst, als de situatie zoals hij in de praktijk wordt vormgegeven. In hoofdstuk 4 wordt nader ingegaan op de onderzoeksbevindingen. De opsporingspraktijk wordt in meer detail beschreven en er wordt nader ingegaan op de dossiers die voor dit onderzoek zijn bestudeerd. Hoofdstuk 5 schenkt aandacht aan publiek-private samenwerking bij de aanpak van cybercriminaliteit, zowel aan de theorie als aan de uitwerking in de praktijk. In hoofdstuk 6 wordt een aantal dillema's geschetst waar men in de opsporingspraktijk tegenaan loopt. Het rapport wordt afgesloten met de slotbeschouwing in hoofdstuk 7.

2 Juridisch kader

In dit hoofdstuk wordt stilgestaan bij het juridisch kader bij de aanpak van cybercriminaliteit. Gedurende de jaren zijn zowel het Wetboek van Strafrecht als het Wetboek van Stafvordering meerdere keren aangepast en uitgebreid om in te spelen op nieuwe ontwikkelingen op het gebied van cybercriminaliteit. Eerst wordt kort beschreven wat de belangrijkste wetsontwikkelingen zijn geweest rondom de strafbaarstelling en aanpak van cybercriminaliteit. Vervolgens wordt in paragraaf 2.3 ingegaan op delicten gerelateerd aan cybercriminaliteit (materiaal strafrecht) en in paragraaf 2.4 op de opsporingsbevoegdheden voor de aanpak van cybercriminaliteit (formeel strafrecht). Ten slotte wordt in paragraaf 2.5 kort stilgestaan bij de juridische grondslag voor het nemen van verstoringsmaatregelen.

2.1 Wetsontwikkelingen cybercriminaliteit

In 1993 werd de Wet computercriminaliteit (CCI) aangenomen in Nederland.[29] Vanwege het toenemende gebruik van ICT rees de vraag in hoeverre het materiele strafrecht nog voldoende bescherming bood tegen de mogelijke dreigingen die gepaard gingen met het gebruik van ICT. Daarnaast rees de vraag of het Wetboek van Strafvordering nog toereikend was om aan waarheidsvinding te kunnen doen op het gebied van ICT. [30] De Commissie-Franken werd gevraagd mogelijke tekortkomingen in het Wetboek van Strafrecht en Wetboek van Strafvordering te signaleren. Op basis van het rapport Informatietechnologie en Strafrecht van de Commissie-Franken werden in de Wet CCI verschillende strafbaarstellingen en opsporingsbevoegdheden op het gebied van cybercriminaliteit geïntroduceerd.[31] Daarbij ging het onder meer om de strafbaarstelling van het opzettelijk en wederrechtelijk (zonder toestemming van rechthebbende) binnendringen van een geautomatiseerd werk (*hacken)*. Door nieuwe technologische ontwikkelingen was er behoefte aan nieuwe aangepaste wetgeving in de vorm van de Wet computercriminaliteit II. In 1999 werd daarvan een eerste concept besproken in de Tweede Kamer. Tegelijkertijd werd er in internationale context gewerkt aan het zogenoemde Cybercrime Verdrag (of verdrag van Boedapest)[32]. Vanwege het toenemende gebruik van internet en het daarmee gepaard gaande internationale karakter van cybercriminaliteit was er behoefte aan harmonisering van wetgeving op dit gebied (Koops, 2012, p. 11).

In 2006 trad de Wet computercriminaliteit II in werking, waarin tevens de bepalingen van het Cybercrime Verdrag werden geïmplementeerd (Van der Flier, 2006, p. 914-915; Koops, 2012, p. 12). De Wet computercriminaliteit II leidde tot de verhoging van enkele strafmaten en introduceerde enkele nieuwe strafbepalingen, waaronder de strafbaarstelling van *DDoS*-aanvallen[33] (Van der Flier, 2006, p. 915; Koops, 2012, p. 12). Ook paste het op onderdelen het procedurele strafrecht aan

[29] Staatsblad 1993, 33.

[30] *Kamerstukken II* 1989/90, 21 551, nr. 3, p.1.

[31] *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 2.

[32] Voluit het 'Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken'.

[33] 'Dit zijn aanvallen op een systeem of service met als doel een systeem, service of netwerk zo te belasten dat deze uitgeschakeld wordt of niet meer beschikbaar is. Bijvoorbeeld het platleggen van een website' (Leukfeldt et al., 2015, p. 18).

(Van der Flier, 2006, p. 918; Koops, 2012, p.12).[34] Ook later stonden de technologische ontwikkelingen niet stil en was er behoefte aan aangepaste wetgeving. Thema's zoals het verwijderen van illegale inhoud van het internet, heling van gegevens en het *hacken* als opsporingsbevoegdheid werden in een eerste consultatieronde in 2013 besproken (Koops, 2014). Op 1 januari 2019 is de Wet computercriminaliteit III (CCIII) in werking getreden. De wet introduceerde onder meer de 'hackbevoegdheid' voor de politie, de bevoegdheid om gegevens ontoegankelijk te maken en de strafbaarstelling van het overnemen en helen van gegevens (Langius & Mol Lous, 2018).

In de volgende paragrafen zal nader worden ingegaan op de hierboven aangestipte wetgeving. Belangrijk om op te merken is dat de besproken casuïstiek in dit onderzoek zich afspeelde voor de introductie van de Wet CCIII. Omdat die wet een aantal belangrijke bevoegdheden introduceert bespreken we de wet CCIII wel beknopt, maar deze bevoegdheden zullen dus verder beperkt aan bod komen in dit rapport.[35] Zoals Koops (2012, p. 12) aangeeft ligt het zwaartepunt van de Nederlandse cybercriminaliteit wetgeving bij de Wet computercriminaliteit en zijn opvolgers, maar ook enkele andere wetten zijn relevant. Daarbij gaat het onder meer om thema's die sterk samenhangen met cybercriminaliteit, zoals seksueel misbruik van kinderen, of die relevant zijn in de opsporing, zoals het vorderen van gegevens (Koops, 2012, p. 12). Enkele van deze thema's zullen daarom ook worden besproken in dit hoofdstuk.

2.2 Definities

Voor het juridisch kader zijn een aantal definities belangrijk om nader toe te lichten. De gebruikte definitie van computercriminaliteit is relevant omdat het de reikwijdte van de bespreking van de cyberdelicten bepaalt. Daarnaast wordt kort stil gestaan bij de begrippen 'gegevens' en 'geautomatiseerd werk'. Deze begrippen zijn belangrijk, omdat ze veel gebruikt worden in wetsartikelen en daarmee de reikwijdte van de wetsartikelen bepalen.

2.2.1 Computercriminaliteit

Zoals eerder in het voorgaande hoofdstuk al werd beschreven is er in de literatuur veel discussie over de reikwijdte en definitie van het begrip cybercriminaliteit. Voor het bespreken van het juridisch kader wordt in dit hoofdstuk gebruikgemaakt van de driedeling die wordt gehanteerd door Koops en Oerlemans (2019). Deze indeling Is eerder beschreven in de inleiding van hoofdstuk 1. De focus in het huidige onderzoek ligt op complexe cyberonderzoeken, welke veelal computergestuurde en computergerelateerde delicten betreffen. Dit hoofdstuk richt zich dan ook primair op deze twee typen delicten. Computerrelevante delicten worden kort aangestipt.[36]

Het is belangrijk om op te merken dat in de praktijk bij de aanpak van cybercriminaliteit ook gebruik wordt gemaakt van 'klassieke' delictsvormen in de tenlastelegging (hierbij gaat het bijvoorbeeld om diefstal of fraude). Koops en Oerlemans

[34] Voor een uitgebreide bespreking zie: Van der Flier (2006).

[35] Voor meer informatie zie de nog te verschijnen evaluatie van de wet CCIII, tevens uitgevoerd door het WODC: Evaluatie Wet Computercriminaliteit III: de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk.

[36] Voor een meer uitgebreide bespreking zie: Koops en Oerlemans (2019).

(2019, p. 30) geven als voorbeeld het gebruik van *banking malware*, waarbij verdachten ook kunnen worden veroordeeld voor traditionele delicten zoals diefstal met valse sleutel en oplichting. Dit kan tevens implicaties hebben voor de zwaarte van de strafmaat. Ook vanuit het opsporingsperspectief kan het gunstig zijn om in de tenlastelegging een traditioneel delict te hanteren, omdat daardoor mogelijk andere (meer vergaande) opsporingsbevoegdheden kunnen worden ingezet. Om deze reden worden in dit hoofdstuk ook 'klassieke' delicten en opsporingsbevoegdheden genoemd die in de opsporingspraktijk relevant kunnen zijn bij de aanpak van cybercriminaliteit.

2.2.2 Geautomatiseerd werk

De term 'geautomatiseerd werk' wordt in de wet vaak gebruikt om computers aan te duiden. In artikel 80sexies van het Wetboek van Strafrecht (Sr) wordt het omschreven als: 'een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken'. De definitie is ruim zodat ook 'slimme' apparaten zoals slimme lampen, energiemeters en speakers eronder kunnen vallen (ook wel aangeduid als het *Internet of Things*).[37]

Koops en Oerlemans (2019, p. 33) merken op dat het gebruik van de term 'computergegevens' verwarrend kan zijn in deze definitie, omdat er niet is gedefinieerd wat 'computers' of 'computergegevens' zijn. In dit kader kan daarom ter verduidelijking ook gesproken worden van (digitale) gegevens (Koops & Oerlemans, 2019, p. 33).

2.2.3 Gegevens

Gegevens worden in artikel 80quinquies Sr omschreven als 'iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken'. De term gegevens is relevant omdat de wetgever bewust heeft gekozen computergegevens niet te kwalificeren als goederen (Koops & Oerlemans, 2019, p. 29). Zoals Koops en Oerlemans (2019, p. 66) aangeven kunnen gegevens alleen maar deel uitmaken van goederendelicten 'wanneer sprake is van een twee-eenheid van de materiële drager en de daarmee verbonden inhoud of waarde; zo kan het aantasten van een bepaalde gegevensvastlegging zaakbeschadiging opleveren'. Dit betekent dat wanneer een USB-stick wordt gestolen, er sprake is van diefstal van de fysieke USB-stick, maar geen sprake is van diefstal van gegevens. Dit is dan ook één van de redenen dat in de Wet CCIII een nieuwe strafbepaling is opgenomen die het helen van gegevens strafbaar maakt.[38]

Er bestaan uitzonderingen in de jurisprudentie waarbij gegevens toch als goederen worden gekwalificeerd. Hierbij gaat het om gegevens die 'voldoen aan de eigenschappen van uniciteit en directe geldelijke waardeerbaarheid' (Koops & Oerlemans, 2019, p. 67), zoals bijvoorbeeld giraal geld of *bitcoins*. In de jurisprudentie komt naar voren dat beltegoed[39] en onder bepaalde omstandigheden ook virtuele voorwerpen in online computerspellen als goed kunnen worden aangeduid.[40]

---

[37] Zie voor meer informatie Van Berkel et al., (2017).

[38] Artikel 139g, 273, 98 e.v. Wetboek van Strafrecht.

[39] HR 31 januari 2012, ECLI:NL:HR:2012:BQ6575.

[40] HR 31 januari 2012, ECLI:NL:HR:2012:BQ9251.

2.3 Materiaal strafrecht

In deze paragraaf worden de belangrijkste cyberdelicten besproken. Eerst wordt ingegaan op de computergestuurde delicten, vervolgens wordt ingegaan op de computergerelateerde delicten en ten slotte wordt kort stilgestaan bij een aantal computerrelevante delicten.

Onderstaande tabel geeft een overzicht van de besproken delicten in dit hoofdstuk. Vanwege de overlap in online en offline delicten is dit overzicht niet uitputtend.

Tabel 2.1 Overzicht van de in dit hoofdstuk besproken delicten

Delict groep	Delict	Relevante wetsartikelen
Computergestuurde delicten	Computervredebreuk	138ab Sr
	Opzettelijk wederrechtelijk overnemen niet-openbare gegevens	138c Sr
	Aftappen en overnemen van gegevens (o.a. *malware*)	139a Sr, 139b Sr, 139c Sr, 139f Sr, 441b Sr, 139d Sr, 139e Sr
	Verstoring van computergegevens (o.a. *defacement* en *ransomware*)	350a Sr, 350b Sr, 284 Sr, 317 Sr, 326 Sr
	Verstoring van computersystemen	161sexies Sr, 161septies Sr, 351Sr, 139d Sr, 350d Sr
	DDos-aanvallen	138b Sr, 350a Sr, 161sexies Sr, 161septies Sr
Computergerelateerde delicten	Diefstal	310 Sr
	Verduistering	321 Sr
	Helen van gegevens	139g Sr, 271 lid 1 sub 2 Sr, 98-98c Sr
	Witwassen	420bis Sr e.v
	Phishing	326d Sr, 225 Sr, 326 Sr
	Valsheid in geschrifte	225 Sr
	Oplichting	326 Sr
	Identiteitsfraude	231a Sr, 231b Sr
Computerrelevante delicten	Kinderporno	240b Sr
	Sextortion	246 Sr, 318 Sr
	Wraakporno	261 Sr, 262 Sr, 268 Sr, 266 Sr, 271 Sr
	Grooming	284e Sr
	Smaad of laster	261 Sr, 262 Sr, 268 Sr
	Belediging	266 Sr, 271 Sr
	Bedreiging	285 Sr
	Discriminatie	137c-137g Sr, 429quater Sr
	Auteursrechtschendingen	31 Aw, 34 Aw

Computervredebreuk
Computervredebreuk, of hacken, is het opzettelijk en zonder toestemming toegang verkrijgen tot een geautomatiseerd werk. Het is strafbaar gesteld in artikel 138ab Sr. Bij computervredebreuk moet sprake zijn van het opzettelijk en wederechtelijk binnendringen van een geautomatiseerd werk (of deel daarvan). Hiervan is in ieder geval sprake indien er toegang tot wordt verkregen (a) door het doorbreken van een beveiliging, (b) door een technische ingreep, (c) met behulp van valse signalen of een valse sleutel of (d) door het aannemen van een valse hoedanigheid.

Omdat het niet altijd duidelijk is of er sprake is van computervredebreuk (of er is onvoldoende bewijs) is er in de Wet CCIII een nieuwe strafbepaling opgenomen. Artikel 138c Sr stelt het opzettelijk en wederrechtelijk overnemen van niet-openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk, voor zichzelf of voor een ander strafbaar. Koops en Oerlemans (2019, p. 41) noemen als voorbeeld het overnemen van privéfoto's uit een gedeelde map op een lokaal wifi-netwerk. Indien iemand toegang heeft tot dit netwerk (bijvoorbeeld als gast) dan zal het lastig zijn iemand te vervolgen voor computervredebreuk, maar kan iemand met de komst van 138c wel vervolgd worden voor het opzettelijk en wederrechtelijk overnemen van deze gegevens.

Aftappen en overnemen van gegevens
Het aftappen en opnemen van gegevens is strafbaar gesteld in artikel 139c Sr. Daarbij gaat het om het 'opzettelijk en wederrechtelijk met een technisch hulp-middel gegevens aftappen of opnemen die niet voor iemand bestemd zijn en worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk'.[41] Dit heeft bijvoorbeeld betrekking op het vastleggen van gegevens met behulp van *malware*. Andere relevante artikelen zijn artikel 139a Sr en 139b Sr die het heimelijk afluisteren van personen met een technisch hulpmiddel in een besloten sfeer strafbaar stellen. Ook het heimelijk maken van beeldopnames met een technisch hulpmiddel is strafbaar gesteld in artikel 139f Sr en 441b Sr, indien dit niet op een duidelijke wijze kenbaar is gemaakt.

Voor het aftappen en overnemen van gegevens zijn ook voorbereidende of daarmee samenhangende handelingen strafbaar gesteld. Op basis van artikel 139d Sr is het strafbaar om een technisch hulpmiddel op een bepaalde plek te plaatsen met het oogmerk om gegevens af te luisteren, af te tappen of op te nemen. Een voorbeeld hiervan zijn verdachten die op basis van dit artikel zijn veroordeeld vanwege het voorhanden hebben van software (*banking malware*) die specifiek ontworpen was om te plaatsen op computers van ING-klanten (Koops & Oerlemans, 2019, p. 46). Ook het bezitten van een voorwerp waarop 'naar hij weet of redelijkerwijs moet vermoeden, gegevens zijn vastgelegd [die] door wederrechtelijk afluisteren, aftappen of opnemen van een gesprek' is strafbaar gesteld in artikel 139e Sr. Hierbij kan het bijvoorbeeld gaan om een usb-stick met daarop gestolen gegevens.

Verstoring van computergegevens
In artikel 350a Sr wordt het opzettelijk en wederrechtelijk veranderen, wissen, onbruikbaar of ontoegankelijk maken van gegevens of het toevoegen van gegevens strafbaar gesteld. Indien iemand door nalatig handelen gegevens verandert, wist, onbruikbaar of ontoegankelijk maakt kan iemand ook strafbaar zijn op basis van artikel 350b Sr. In dat geval moet er sprake zijn van 'ernstige schade' door nalatig handelen. De strafbaarstelling uit deze artikelen kunnen onder meer betrekking

[41] Artikel 139c Sr, lid 1.

hebben op *defacement*[42] en het verspreiden van *ransomware*[43]. Onder bepaalde omstandigheden kunnen voor *ransomware* ook klassieke delicten zoals dwang (artikel 284 Sr), afpersing (artikel 317 Sr) of oplichting (artikel 326 Sr) ten laste worden gelegd (Koops & Oerlemans, 2019, p. 52).

Verstoring van computersystemen
Op basis van artikel 161sexies Sr is strafbaar 'hij die opzettelijk enig geautomatiseerd werk of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt'. Hiervan is sprake als er een 'zeker gevolg' optreedt waardoor de 'algemene' veiligheid van personen of goederen in gevaar wordt gebracht. Dit betekent dat het artikel alleen betrekking heeft op geautomatiseerde werken die een algemeen nut dienen. Het kan hier bijvoorbeeld gaan om het verstoren van computersystemen in de zorg, waardoor bepaalde zorg niet meer kan worden geleverd. Artikel 161septies Sr stelt dat ook als er geen direct gevolg optreedt het verstoren van systemen van 'spoorweg of elektriciteitswerken, geautomatiseerde werken of werken voor telecommunicatie' op basis van artikel 351 strafbaar is. Voor beide delicten geldt dat het ook strafbaar is als een verstoring wordt veroorzaakt door 'grove of aanmerkelijke onvoorzichtigheid, onachtzaamheid of nalatigheid' (Koops & Oerlemans, 2019, p. 62). Ook als het verstoren van computersystemen geen systemen van algemeen nut betreft kan het strafbaar zijn op basis van artikel 350c Sr. Daarin wordt het opzettelijk vernielen, beschadigen of onbruikbaar maken van geautomatiseerde werken of werken voor telecommunicatie strafbaar gesteld.

Op basis van artikel 138b Sr is het strafbaar om opzettelijk en wederrechtelijk de toegang of het gebruik van een geautomatiseerd werk te belemmeren door daaraan gegevens aan te bieden of toe te zenden. Daarbij gaat het om het uitvoeren van DDoS-aanvallen. Een strafverzwarende omstandigheid is als voor de DDoS-aanval een *botnet*[44] wordt gebruikt (artikel 138b lid 2). Voor DDoS-aanvallen geldt dat ook andere delicten kunnen worden opgelegd, zoals de hier boven genoemde computersabotage, het wederrechtelijk toevoegen van gegevens (artikel 350a Sr), of computervredebreuk (artikel 138ab Sr) (Koops & Oerlemans, 2019, p. 59). Een afgeleide daarvan is het uitvoeren van *email bombing,* waarbij de e-mailbox van het slachtoffer verstopt raakt zodat deze persoon of instantie geen e-mails meer kan ontvangen (Leukfeldt et al., 2015, p. 18).

Ten slotte worden verschillende vormen van voorbereidingshandelingen strafbaar gesteld in artikel 139d lid 2 en 3 Sr en artikel 350d Sr. Daarbij gaat het om het misbruik van technische hulpmiddelen. Er is sprake van misbruik als een technisch hulpmiddel (software) hoofdzakelijk ontworpen is om een misdrijf te plegen en de verdachte deze 'vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft' (artikel 350d lid a Sr). Ook het voorhanden hebben van inloggegevens kan strafbaar zijn indien iemand daarmee

---

[42] '*Defacing* is het zonder toestemming veranderen, vervangen of vernielen van een website. Het wordt ook wel gezien als elektronische graffiti, oftewel het bekladden van de startpagina van een site door hackers' (Leukfeldt et al., 2015, p. 25).

[43] Vorm van *malware* (kwaadaardige software) waarbij de computer wordt 'gegijzeld', hierbij worden bestanden versleuteld en pas vrijgegeven na het betalen van een bepaald bedrag.

[44] 'Groep geïnfecteerde computers die onder commando van een crimineel zijn gebracht' (Leukfeldt et al., 2015, p. 18).

bijvoorbeeld van plan is computervredebreuk te plegen of deze te verkopen (artikel 350d lid b Sr).

2.3.1 Computergerelateerde delicten

Klassieke vermogensdelicten
Zoals eerder opgemerkt worden gegevens in beginsel niet als goederen geclassificeerd. In paragraaf 2.2.3 is echter ook al kort aangestipt dat er uitzonderingssituaties zijn waarbij gegevens bepaalde eigenschappen bezitten zoals uniciteit en directe geldelijke waardeerbaarheid, waardoor zij toch als goederen kunnen worden behandeld. In dat geval kan het zijn dat delicten zoals diefstal (artikel 310 Sr) en verduistering (artikel 321 Sr) van toepassing zijn. Koops en Oerlemans (2019, p. 71) geven aan dat delicten als diefstal en verduistering kunnen worden gehanteerd als gegevens bovenstaande eigenschappen bevatten en een vermogensbelang wordt geschaad. Wanneer echter vooral andere belangen zijn geschaad (bijvoorbeeld de integriteit van de gegevens) dan ligt het eerder voor de hand om de specifieke cyberbepalingen te hanteren.

Vanwege het verschil tussen goederen en gegevens is in de Wet CCIII artikel 139g Sr geïntroduceerd, welke het helen van gegevens strafbaar stelt. Daarbij gaat het om (a) het voorhanden hebben van niet-openbare gegevens, waarvan de verdachte (redelijkerwijs) wist ten tijde van het voorhanden krijgen dat deze door een misdrijf zijn verkregen en (b) het ter beschikking stellen van niet-openbare gegevens, waarvan bekend was dat deze door een misdrijf verkregen zijn. Hierbij kan het bijvoorbeeld gaan om het verhandelen van uitgelekte inloggegevens. Eerder was het helen van bedrijfsgegevens en staatsgeheimen al strafbaar gesteld.[45]

Voor veel van de besproken delicten in dit hoofdstuk geldt dat als het delict uit geldbejag wordt gepleegd er mogelijk ook sprake is van witwassen.[46] Dit kan bijvoorbeeld van toepassing zijn bij de heling van computergegevens (Leukfeldt et al., 2015, p. 61). Er zijn verschillende vormen van witwassen met verschillende strafmaten. Zonder al te diep in te gaan op de verschillende vormen en strafmaten, gaat het bij witwassen in beginsel om het verhullen van de herkomst, vindplaats of verplaatsing van een voorwerp waarvan bekend is dat het afkomstig is uit een misdrijf.[47] Een voorwerp kan ook virtuele valuta betreffen, zoals *bitcoin* (Koops & Oerlemans, 2019, p. 75). Het gegeven dat virtuele valuta als voorwerp kunnen worden aangewezen speelt ook een belangrijke rol bij de aanpak van online marktplaatsen op het *darkweb*. Door de kenmerken van deze marktplaatsen kunnen zij ook als platform worden gebruikt voor witwassen en daarmee strafbaar worden gesteld. Op basis van de jurisprudentie[48] zijn er enkele kenmerken te noemen die erop kunnen duiden dat online marktplaatsen voor witwassen worden gebruikt: (i) een onredelijke hoge commissie voor het omzetten van *bitcoins* in euro's, (ii) het bieden van absolute anonimiteit en (iii) het gebruik van *bitcoin mixers* die de herkomst van *bitcoins* verhullen (Koops & Oerlemans, 2019, p. 77).

[45] Artikel 271 lid 1 sub 2 Sr en artikelen 98-98c Sr.

[46] Artikel 420bis Sr e.v.

[47] Zie bijvoorbeeld artikel 420bis Sr.

[48] Zie voor een overzicht Koops en Oerlemans (2019, p. 77).

Valsheid in geschrifte en oplichting
Bij valsheid in geschrifte en oplichting is in de context van computercriminaliteit met name *phishing*[49] een belangrijk delict. Op basis van artikel 225 is het strafbaar om een valselijk opgemaakt of vervalst geschrift als bewijs te gebruiken met als oogmerk deze als echt of onvervalst door anderen te doen gebruiken. Leukfeldt et al., (2015, p. 43) geven als voorbeeld dat hier sprake van kan zijn als er gebruik wordt gemaakt van valse documenten in een *phishing*-email. Indien *phishing* wordt gebruikt om een persoon ertoe te doen bewegen om bepaalde handelingen te verrichten, bijvoorbeeld het verstrekken van vertrouwelijke gegevens, kan er sprake zijn van oplichting. Dit is strafbaar gesteld in artikel 326 Sr. Hiervan is alleen sprake als de verdachte heeft gehandeld met het oogmerk zichzelf of een ander wederrechtelijk te bevoordelen. Online handelsfraude is met de komst van de Wet CCIII in artikel 326d Sr specifiek strafbaar gesteld. Daarbij gaat het om handelingen die er toe leiden personen of bedrijven te bewegen tot het doen van betalingen, zonder de beloofde dienst of goederen te leveren (of maar gedeeltelijk te leveren).

Hiermee samenhangend is identiteitsfraude strafbaar gesteld in artikel 231a en 231b Sr. Hierbij gaat het om het valselijk gebruikmaken van biometrische persoonsgegevens van een ander om de eigen identiteit te verhullen. Daarbij kan het bijvoorbeeld gaan om online bestellingen die worden gedaan door misbruik te maken van iemand anders' identiteit, waardoor de persoon waartoe de identiteit behoort onvrijwillig voor de kosten opdraait.

2.3.2 Computerrelevante delicten

Zoals in het begin van dit hoofdstuk is opgemerkt, wordt vanwege de focus op complexe cyberdelicten minder uitgebreid stilgestaan bij de computerrelevante delicten. In deze paragraaf worden kort de belangrijkste computerrelevante delicten genoemd.[50] Verschillende zedenmisdrijven zijn relevant in de context van computercriminaliteit. Hierbij gaat het onder meer om kinderporno (artikel 240b Sr), *sextortion* (strafbaar op basis van online aanranding (artikel 246 Sr) en afdreiging (artikel 318 Sr)) en wraakporno (zie o.a. smaad en belediging). Met de komst van de Wet CCIII is ook de strafbaarstelling van *grooming* in artikel 284e Sr uitgebreid. Eerder was het al strafbaar om personen onder de 16 er toe te bewegen ontuchtige handelingen te plegen of kinderporno te vervaardigen. Met de komst van de Wet CCIII is het nu ook strafbaar als iemand 'meent te communiceren met een persoon beneden de 16 jaar, maar die persoon in werkelijkheid ouder is' (Koops & Oerlemans, 2019, p. 96-97). Dit kan bijvoorbeeld het geval zijn als een opsporingsambtenaar zich voordoet als een minderjarig persoon (in deze context wordt ook wel gesproken over de inzet van een 'lokpuber'). Deze aanpassing van artikel 284^{e} Sr biedt daarmee een oplossing voor de bewijsproblemen die zich eerder bij de inzet van 'lokpubers' voordeden. Daarnaast zijn verschillende uitingsdelicten relevant in het kader van computerrelevante delicten. Hierbij gaat het onder meer om smaad of laster (artikel 261, 262 en 268 Sr), belediging (artikel 266 en 271 Sr), bedreiging (285 Sr), discriminatie (artikel 137c-137g en 429quater Sr) en auteursrechtschendingen (artikel 31 en 34 Aw).

[49] '*Phishing* is een poging om via digitale middelen (bijvoorbeeld e-mail of sms) persoonlijke informatie van mensen te ontfutselen, vaak door zich voor te doen als een vertrouwde instantie' (Leukfeldt et al., 2015, p. 42).

[50] Voor een uitgebreidere bespreking zie onder meer: Koops en Oerlemans (2019) en Leukfeldt et al., (2015).

2.4 Formeel strafrecht

In hoofdstuk 4 wordt besproken op welke wijze opsporingsbevoegdheden in de praktijk worden ingezet bij de opsporing van cyberdelicten. In deze paragraaf wordt daarom van de belangrijkste opsporingsbevoegdheden slechts kort de juridische grondslag besproken.[51]

2.4.1 Doorzoeking en inbeslagname

De politie is bevoegd om bij een heterdaad of verdenking van een misdrijf een plaats te doorzoeken. De wet maakt daarin onderscheid in verschillende typen plaatsen, waarvoor verschillende voorwaarden gelden. Daarbij wordt onder andere onderscheid gemaakt tussen vervoersmiddelen (artikel 96b Sv), plaatsen met uitzondering van woning zonder toestemming en kantoor geheimhouder (artikel 96c Sv), woning zonder toestemming bewoner (artikel 97 Sv) en overige plaatsen (110 Sv). Het belangrijkste verschil tussen deze plaatsen is wie de autoriteit heeft de plaats te doorzoeken en wie hiervoor toestemming kan verlenen ((hoofd)officier van justitie of rechter-commissaris). Bij een doorzoeking is de politie bevoegd om computers te doorzoeken. Omdat gegevens in de wet niet als goederen worden gekwalificeerd is het echter niet mogelijk om beslag te leggen op gegevens, maar wel op gegevensdragers (bijvoorbeeld computers of smartphones). Wanneer bij een doorzoeking het doel is om alleen op gegevens beslag te leggen kan gebruik worden gemaakt van artikel 125i Sv, welke de bevoegdheid geeft 'tot het doorzoeken van een plaats ter vastlegging van gegevens die op deze plaats op een gegevensdrager zijn opgeslagen of vastgelegd'. De voorwaarden voor een doorzoeking zijn gelijkgesteld aan de reguliere doorzoeking (artikel 96b Sv e.v.). Tabel 2.2 geeft de genoemde artikelen op basis waarvan een doorzoeking plaatsvindt schematisch weer.

Tabel 2.2 Overzicht bevoegdheden doorzoeking en inbeslagname

Type doorzoeking en inbeslagname	Artikel	Autoriteit
Vervoersmiddelen	96b Sv	Opsporingsambtenaar
Alle plaatsen, met uitzondering van woning zonder toestemming bewoner en kantoor geheimhouders	96c Sv	Officier van justitie
Woning zonder toestemming bewoner	97 Sv	Officier van justitie met machtiging rechter-commissaris (bij spoed)
Alle plaatsen	110 Sv	Rechter commissaris
Vastleggen van gegevens	125i Sv	Zelfde voorwaarden als bovenstaande, afhankelijk van plaats.

Hoewel er juridische gronden zijn om gegevensdragers te onderzoeken en gegevens op te slaan, is er in de literatuur en jurisprudentie discussie over de reikwijdte van deze bevoegdheid (Koops & Oerlemans, 2019; Lassche, 2019). Zonder deze discussie hier uitgebreid opnieuw te voeren, is met name het complete beeld dat gegevensdragers (zoals smartphones) kunnen geven van iemands persoonlijke leven genoemd als een potentieel probleem wat betreft de proportionaliteit van het in te zetten middel. In hoeverre het doorzoeken van een gegevensdrager juridisch houdbaar is hangt onder meer af van de gekozen bevoegdheid, wie de autoriteit heeft om de doorzoeking uit te voeren en welke partij toestemming geeft (Koops & Oerlemans, 2019, p. 131; Lassche, 2019, p. 23-24). Een ander aandachtspunt is in

[51] Voor een uitgebreidere juridische bespreking zie onder meer Koops en Oerlemans (2019) en Lassche (2019).

hoeverre kennis mag worden genomen van berichten op een gegevensdrager nadat deze in beslag is genomen (Koops & Oerlemans, 2019, p. 133; Lassche, 2019, p. 25). Daarbij gaat het bijvoorbeeld om een in beslag genomen telefoon waarop nog nieuwe (tekst)berichten binnenkomen. Tot op heden is hier geen duidelijk kader voor beschikbaar. De verwachting is dat het nieuwe wetboek van stafvordering hier duidelijkheid in zal scheppen.[52]

Tijdens het doorzoeken van plaatsen kunnen aangetroffen apparaten zoals computers en smartphones worden doorzocht. Het kan zijn dat deze apparaten verbonden zijn met andere apparaten via een netwerk. In dit geval kan op basis van artikel 125j Sv een netwerkzoeking plaatsvinden. Bij het doen van een netwerkzoeking gelden een aantal voorwaarden en beperkingen:

- De netwerkzoeking reikt niet verder dan de 'in dat werk opgeslagen gegevens die redelijkerwijs nodig zijn om de waarheid aan de dag te brengen' (125j lid 1 Sv).
- De netwerkzoeking kan alleen plaatsvinden vanaf de plaats van doorzoeking, het kan dus niet op een later tijdstip plaatsvinden (bijvoorbeeld vanaf het politiebureau).
- Er geldt een 'dubbele-bandcriterium': er moet zowel een feitelijke band bestaan tussen de persoon en de locatie waar de doorzoeking plaatsvindt, als een juridische band tussen de persoon en de locatie (de persoon moet gerechtigd zijn zich toegang te verschaffen tot de andere locatie, het kan dus niet gaan om 'gehackte' computers) (Koops & Oerlemans, 2019, p. 134; Lassche, 2019, p. 27).
- De netwerkzoeking mag slechts plaatsvinden binnen Nederland. Indien bij de start duidelijk is dat een computer zich in het buitenland bevindt zal eerst een rechtshulpverzoek moeten worden ingediend. Indien achteraf duidelijk wordt dat een computer zich in het buitenland bevindt zal een buitenlandse staat alsnog moeten worden ingelicht (Koops & Oerlemans, 2019, p. 135). Ook hiervoor geldt dat de verwachting is dat het nieuwe wetboek van strafvordering hier wijzigingen in zal brengen om het voor de opsporingspraktijk te vereenvoudigen (Commissie-Koops, 2018, p. 117).

Tijdens een netwerkzoeking of een doorzoeking waarbij het doel is beslag te leggen op gegevens, kan op basis van artikel 125k Sv een persoon worden bevolen toegang te verschaffen tot het betreffende apparaat. Dit bevel geldt voor personen waarvan 'redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van beveiliging van een geautomatiseerd werk' (125k lid 1 Sv), het bevel kan niet worden gegeven aan verdachten (125k lid 3 Sv).[53]

Als er tijdens een doorzoeking gegevens worden aangetroffen die betrekking hebben op het strafbare feit kunnen deze op basis van artikel 125o Sv ontoegankelijk worden gemaakt. Dit is alleen mogelijk voor zover dit nodig is voor het beëindigen van het strafbare feit of ter voorkoming van nieuwe strafbare feiten (125o lid 1 Sv). Een voorbeeld hiervan is een verdachte die in het bezit is van kinderporno en dit heeft opgeslagen op een server. In dit geval kunnen deze gegevens ontoegankelijk wor-

[52] De Commissie modernisering opsporingsonderzoek in het digitale tijdperk ('Commissie-Koops') heeft in 2018 een rapport uitgebracht met aanbevelingen voor aanpassingen in het Wetboek van Strafvordering. Zij spreken in dit kader van pure en voorzienbare bijvangst. Van pure bijvangst is sprake als er is van 'er een kort, natuurlijk, tijdsverloop is tussen de inbeslagname en het verbreken van de verbinding' (na inbeslagname worden verbindingen afgesloten), in die situatie zouden de huidige bevoegdheden voldoende waarborgen bieden. Als hier geen sprake van is dan schieten de huidige bevoegdheden te kort (Commissie-Koops, 2018, p. 92-93).

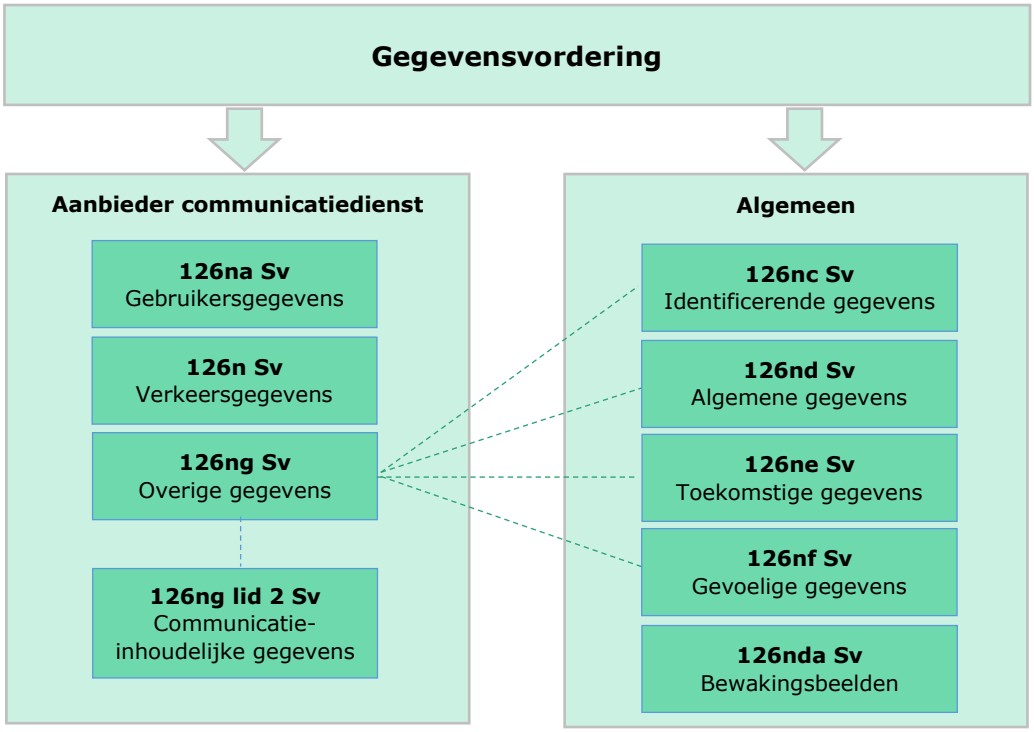
[53] Een mogelijke uitzondering geldt voor biometrische beveiliging, hiermee kunnen verdachten doormiddel van hun vingerafdruk of irisscan gedwongen worden toegang te verlenen (Koops & Oerlemans, 2019, p. 138).

den gemaakt voor derden (Lassche, 2019, p. 29). Met de komst van de Wet CCIII is op basis van artikel 125p Sv ook de *'notice-and-takedown'* (NTD) bevoegdheid geïntroduceerd. Met behulp van deze bevoegdheid kunnen communicatiedienstaanbieders verplicht worden strafbaar materiaal te verwijderen. Al sinds 2008 bestaat er een gedragscode waarin aanbieders op verzoek strafbaar materiaal vrijwillig kunnen verwijderen. De bevoegdheid wordt daarom pas ingezet als er geen gehoor wordt gegeven aan de vrijwillige gedragscode of een aanbieder hier niet bij is aangesloten (Koops & Oerlemans, 2019, p. 141-142).

2.4.2 Vorderen van gegevens

Als opgeslagen gegevens van een derde van belang zijn voor een opsporingsonderzoek kunnen deze worden gevorderd door middel van verschillende bevoegdheden. Daarvoor bestaan twee wettelijk regimes: één voor vorderingen specifiek gericht aan communicatiediensten (zoals ISP's) en één algemeen regime voor alle (overige) partijen (Koops & Oerlemans, 2019, p. 147). Figuur 2.1 geeft dit schematisch weer.

Figuur 2.1 Wettelijke regimes gegevensvorderingen[a]



a Aangepast figuur naar Lassche (2019, p. 30).

In geval van verdenking van een misdrijf kunnen gebruikers- en verkeersgegevens worden gevorderd bij communicatiediensten, indien het van belang is voor het opsporingsonderzoek. Deze vordering kan zowel betrekking hebben op historische als toekomstige gegevens. Bij gebruikersgegevens gaat het om de naam, adres, postcode, woonplaats, nummer en soort dienst die de gebruiker van een communicatiedienst afneemt (126na lid 1 Sv). Bij verkeersgegevens gaat het om de tijd, duur, gebruikte apparatuur, afgenomen diensten en de locatiegegevens (Koops & Oerlemans, 2019, p. 152). Daarnaast kunnen op basis van 126n Sv naast

verkeersgegevens ook gebruikersgegevens worden gevorderd (Artikel 2 Besluit vorderen gegevens telecommunicatie). Lassche (2019, p. 32-34) noemt hierna enkele voorbeelden van opsporingsmiddelen die op basis van deze bevoegdheden kunnen worden ingezet. Indien een telefoonnummer onbekend is, kan dit worden achterhaald door aan de hand van de tijd en plaats dat verdachten een telefoon hebben gebruikt (hetgeen bijvoorbeeld bekend is op grond van observaties) de gebruikte verkeersgegevens in dat gebied te vorderen. Wanneer het nummer bekend is, maar onduidelijk is waar de telefoon zich bevindt en er geen communicatie plaatsvindt, kan ervoor worden gekozen om een *stealth-sms* te sturen, dat is een sms-bericht dat niet zichtbaar is voor de gebruiker van de telefoon, maar wel een signaal genereert voor de aanbieder van de communicatiedienst. Deze locatiegegevens kunnen vervolgens gevorderd worden.

Gegevens die niet vallen onder de hierboven genoemde gebruikers- of verkeersgegevens kunnen worden gevorderd op basis van 126ng Sv. Deze bevoegdheid is gekoppeld aan de algemene bepalingen 126nc, 126nd, 126ne en 126nf Sv. Deze algemene bepalingen hebben betrekking op diensten of personen zoals sportverenigingen, verhuurbedrijven of financiële dienstverleners (Lassche, 2019, p. 34). Tabel 2.3 geeft een kort overzicht van de verschillende bevoegdheden en mogelijke gegevens die kunnen worden gevorderd. Een uitzondering hierop vormen communicatie-inhoudelijke gegevens. Dit zijn bijvoorbeeld e-mails of sms-berichten die opgeslagen zijn bij communicatieaanbieders. Deze kunnen worden gevorderd op basis van artikel 126ng lid 2 Sv. Voor toekomstige gegevens geldt dat deze op basis van artikel 126ne Sv voor een periode van vier weken kunnen worden gevorderd, hierbij kan het bijvoorbeeld gaan om toekomstige pintransacties. Om te voorkomen dat mogelijke gegevens verloren gaan kan er op basis van artikel 126ni Sv ook een bevriezingsbevel worden gegeven. De beheerder van de gegevens zorgt dan dat hij de gegevens gedurende een periode van ten hoogste negentig dagen ter beschikking kan stellen.

Tabel 2.3 Overzicht bevoegdheden vorderen gegevens

Bevoegdheid	Artikel	Type gegevens
Gebruikersgegevens	126na Sv	Naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst.
Verkeersgegevens	126n Sv	Tijd, duur, gebruikte apparatuur, afgenomen diensten en locatiegegevens.
Overige gegevens	126ng Sv	Zie 126nc, 126nd, 126ne en 126nf Sv.
Communicatie-inhoudelijke gegevens	126ng lid 2 Sv	Opgeslagen email of sms-berichten.
Identificeerbare gegevens	126nc Sv	Naam, adres, woonplaats, postadres, geboortedatum, geslacht, administratieve kenmerken, rechtsvorm en vestigingsplaats (indien van toepassing).
Algemene gegevens	126nd Sv	Bijvoorbeeld betalingsgegevens.
Gevoelige gegevens	126na Sv	Godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging.
Bewakingsbeelden	126nda Sv	Beelden gemaakt voor de beveiliging van goederen, gebouwen of personen.

2.4.3 Publiek toegankelijke online gegevens

Het vergaren van publiek toegankelijke *online* gegevens kan op basis van de algemene taakstelling van de politie in artikel 3 Politiewet (Pw) of op basis van het Wetboek van Strafvordering, zoals artikel 126g, de stelselmatige observatie (Koops & Oerlemans, 2019, p. 188; Lassche, 2019, p. 9). Wanneer het vergaren van informatie een 'niet meer dan beperkte inbreuk' op iemand zijn privacy oplevert kan op basis van artikel 3 Pw *online* informatie worden ingewonnen. Het moet daarbij gaan om publiek toegankelijke *online* gegevens. Daaronder vallen ook sociale media en online fora, ook als daarvoor eerst een account voor moet worden aangemaakt (Koops & Oerlemans, 2019, p. 188; Lassche, 2019, p. 9). Wanneer de inbreuk meer dan gering is, moet er gebruik worden gemaakt van de stelselmatige observatie. Bij een stelselmatige observatie is er sprake van het verkrijgen van een min of meer compleet beeld van bepaalde aspecten van het privéleven van een persoon. Er is geen eenduidig criterium wanneer er sprake is van meer dan een geringe inbreuk. Wel is duidelijk dat in ieder geval de volgende factoren moeten worden meegewogen: de duur, plaats, intensiteit, frequentie en de gebruikte methode van de observatie (Koops & Oerlemans, 2019, p. 191; Lassche, 2019, p. 10).

2.4.4 Aftappen en observatie

Op basis van artikel 126m Sv kan communicatie die plaatsvindt via diensten van een communicatieaanbieder worden opgenomen (afgetapt). In beginsel wordt de aanbieder gevorderd de tap uit te voeren, tenzij dit niet in het belang is van het onderzoek (bijvoorbeeld als de verdachte werkzaam is bij de aanbieder). Openbare aanbieders zijn op basis van artikel 13.2 Telecommunicatiewet verplicht om mee te werken aan een bevel. Voor gesloten aanbieders geldt deze verplichting niet (hier gaat het bijvoorbeeld om interne netwerken van bedrijven). In die situaties is het mogelijk dat de opsporingsambtenaren met eigen apparatuur de tap uitvoeren (Koops & Oerlemans, 2019, p. 162). Op basis van de bevoegdheid kunnen aanbieders verplicht worden de door hun aangebrachte versleuteling ongedaan te maken (Koops & Oerlemans, 2019, p. 162). Indien een te tappen communicatiemiddel zich in het buitenland bevindt moet vooraf een rechtshulpverzoek worden ingediend (126ma lid 1 Sv). Indien tijdens het tappen pas blijkt dat de verdachte zich in het buitenland bevindt, moet het land in kennis worden gesteld en moet alsnog toestemming worden verworven. Aanbieders van diensten zoals Facebook, Instagram en Whatsapp vallen niet onder de huidige Telecommunicatiewet, hierdoor hebben zij geen verplichting om het aftappen van berichten mogelijk te maken (Koops & Oerlemans, 2019, p. 166).

In plaats van een communicatiemiddel af te tappen kan een verdachte ook direct worden afgeluisterd. Op basis van artikel 126l Sv kan met behulp van een technisch hulpmiddel vertrouwelijke communicatie worden opgenomen van een verdachte die betrokken is bij misdrijven die een 'ernstige inbreuk op de rechtsorde' opleveren. Onder vertrouwelijke communicatie valt onder meer: een in beslotenheid gevoerd gesprek of een niet-openbaar emailbericht (Koops & Oerlemans, 2019, p. 168). Er moet sprake zijn van communicatie met een ander, dit betekent dat 'zelfcommunicatie' hier niet onder valt. Hierbij kan gedacht worden aan ingetypte wachtwoorden of geschreven tekst in een dagboek.

Het gebruik van een *keylogger* zou in deze context kunnen worden gebruikt indien de 'redelijke verwachting' bestaat dat daarmee de communicatie met anderen wordt vastgelegd (Koops & Oerlemans, 2019, p. 168). Op basis van artikel 126l lid 2 Sv kan voor de uitvoering van de tap ook een besloten plaats worden betreden om de benodigde apparatuur te plaatsen.

Voor het observeren van verdachten kan, zoals eerder beschreven in het zoeken naar publiek toegankelijke online gegevens, gebruik worden gemaakt van artikel 3 Pw en het wetboek van strafvordering. In geval van een verdenking van een misdrijf kan op basis van artikel 126g Sv een opsporingsambtenaar stelselmatig een persoon volgen of gedrag waarnemen. Hier kan een technisch hulpmiddel voor worden ingezet, voor zover daarmee geen vertrouwelijke informatie wordt opgenomen (artikel 126g lid 3 Sv). Het kan daarbij bijvoorbeeld gaan om GPS-bakens die onder auto's worden geplaatst ter locatiebepaling. Technische hulpmiddelen mogen niet op personen of binnen woningen worden geplaatst. Wel is het mogelijk om met technische hulpmiddelen een woning van buitenaf te observeren, 'voor zover het gaat om waarnemingen die zonder technische manoeuvres kunnen plaatsvinden: hetgeen normaal gesproken van buiten af zichtbaar is, mag worden waargenomen' (Koops & Oerlemans, 2019, p. 172).[54]

2.4.5 Binnendringen en onderzoeken in geautomatiseerde werken

Met de introductie van de Wet CCIII is in artikel 126nba Sv de bevoegdheid geschapen voor geautoriseerde opsporingsambtenaren om binnen te dringen in een geautomatiseerd werk en onderzoek te doen. Deze bevoegdheid wordt ook wel aangeduid als het '*hacken*' of 'terughacken' door de politie.[55] Het onderzoek kan gericht zijn op de volgende zaken (artikel 126nba lid 1 Sv):

a de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;
b uitvoering geven aan een 126l of 126m Sv bevel (opnemen van vertrouwelijke communicatie of uitvoering tap);
c uitvoering geven aan een 126g Sv bevel (observatie);
d de vastlegging van gegevens die in het geautomatiseerde werk zijn opgeslagen;
e de ontoegankelijkmaking van gegevens.

Er mag slechts binnen worden gedrongen in een geautomatiseerd werk dat gebruikt wordt door de verdachte (Lassche, 2019, p. 41). Er kan dus niet binnen worden gedrongen in een computer van een vriend(in) van de verdachte als de verdachte daar niet zelf ook gebruik van maakt. Een gedeelde computer kan wel worden binnen gedrongen. In de Memorie van Toelichting van de Wet CCIII worden enkele voorbeelden genoemd van manieren waarop de politie een geautomatiseerd werk kan binnendringen:[56]

- binnendringen met behulp van inloggegevens die door middel van *social engineering* of het gebruik van kunstmatige intelligentie zijn verkregen;
- verdachten verleiden te reageren op een emailbericht, *malware* te plaatsen, waarna een *bug* of *keylogger* kan worden geplaatst;

---

[54] Zie ook *Kamerstukken II* 199697, 25 403, nr. 3, p. 70-71.

[55] Veel respondenten betrokken bij de uitvoering van de bevoegdheid geven aan dat deze term niet de lading dekt, omdat het hacken betrekking heeft op het onrechtmatig binnendringen van een werk en dat is niet het geval voor de politie.

[56] *Kamerstukken II* 201516, 34 372, nr. 3, p. 34.

- het misbruiken van kwetsbaarheden in een computer, zoals fouten of lekken in de software.

2.4.6 Werken onder dekmantel

Bij werken onder dekmantel maakt een opsporingsambtenaar contact met een individu met als doel bewijs te verzamelen over diegene of een ander individu ten behoeve van een opsporingsonderzoek (Kruisbergen & de Jong, 2010, p. 13; Koops & Oerlemans, 2019, p. 194). Het Wetboek van Strafvordering maakt onderscheid in drie typen van werken onder dekmantel, te weten: (i) infiltratie (artikel 126h Sv), (ii) pseudokoop of -dienstverlening (artikel 126i Sv) en (iii) stelmatige inwinning van informatie (artikel 126j Sv). Voor deze bevoegdheden geldt dat deze zowel in offline als online wereld kunnen worden ingezet.

Bij infiltratie kan op basis van artikel 126h lid 1 Sv een opsporingsambtenaar bevoegd zijn om deel te nemen of mee te werken aan 'een groep van personen waar binnen naar redelijkerwijs kan worden vermoed misdrijven worden beraamd of gepleegd'. Om zijn dekmantel te bewaren kan een opsporingsambtenaar genoodzaakt zijn in dit kader (geautoriseerde) strafrechtelijke handelingen te verrichten (Kruisbergen & de Jong, 2010, p. 47; Koops & Oerlemans, 2019, p. 201). De opsporingsambtenaar mag een individu er niet toe bewegen andere strafbare feiten te plegen dan dit individu reeds van plan was (artikel 126h lid 2 Sv).

Op basis van artikel 126i Sv heeft een opsporingsambtenaar de bevoegdheid om pseudoaankopen te doen of diensten te verlenen aan een verdachte. Daarbij kan het zowel gaan om goederen als gegevens die worden afgenomen. Ook voor deze bevoegdheid geldt dat de opsporingsambtenaar een individu er niet toe mag bewegen om strafrechtelijke feiten te verrichten die afwijken van de reeds verrichtte (of toekomstige) strafrechtelijke feiten. Concreet betekent dit dat de opsporingsambtenaar geen pseudoverkoop kan verrichten (Kruisbergen & de Jong, 2010, p. 46).[57]

Ten slotte kan een opsporingsambtenaar op basis van 126j Sv zonder dat kenbaar is dat hij optreedt als opsporingsambtenaar stelselmatig informatie inwinnen van een verdachte. In de context van computercriminaliteit kan het bijvoorbeeld gaan om chatgesprekken met een verdachte, berichten plaatsen op online fora of vrienden te worden met de verdachte op sociale media (Koops & Oerlemans, 2019, p. 197).

2.4.7 Internationale samenwerking

Cybercriminaliteit heeft een sterk internationaal karakter, omdat het voor een groot deel online plaatsvindt en daarom niet beperkt wordt door landsgrenzen. Dit bemoeilijkt de opsporing omdat opsporingsbevoegdheden veelal wel gebonden zijn aan landsgrenzen. Het uitgangspunt is dat de Nederlandse rechtsmacht reikt tot het eigen grondgebied. Als een strafbaar feit niet onder de Nederlandse rechtsmacht valt, kan er ook geen opsporing en vervolging plaatsvinden (Lassche, 2019, p. 45). Het algemene uitgangspunt daarbij is dat de Nederlandse strafwet van toepassing is op 'ieder die zich in Nederland aan enig strafbaar feit schuldig maakt' (artikel 2 Sr). Daarbij gaat het om de plaats waar het strafbare feit plaatsvindt (of de gevolgen plaatsvinden) (Lassche, 2019, p. 45). Een buitenlandse hacker die een Nederlands bedrijf hackt valt om deze reden dus onder de Nederlandse rechtsmacht.

[57] Het kan wel zijn dat een opsporingsambtenaar bij het infiltreren een pseudo-verkoop verricht, maar in dat geval is het doel niet vervolgen van de verdachte voor het kopen van goederen of gegevens.

Artikel 539a Sv geeft aan op welke gronden opsporingsbevoegdheden buiten de landsgrenzen kunnen worden ingezet. Op basis van dit artikel kunnen opsporingsbevoegdheden in het buitenland worden ingezet, 'voor zover het volkenrecht en het interregionale recht dit toelaten' (artikel 539a lid 3 Sv). Dit betekent dat de opsporingsbevoegdheden kunnen worden ingezet op basis van een verdrag of op basis van een internationaal rechtshulpverzoek. Het eerdergenoemde Cybercrimeverdrag biedt een aantal mogelijkheden om opsporingshandelingen buiten de eigen landsgrenzen te verrichten. Allereerst verplicht het verdrag aangesloten landen opsporingsbevoegdheden te implementeren ten aanzien van het vorderen en veiligstellen van gegevens (Oerlemans, 2019, p. 217).[58] Doordat de opsporingsbevoegdheden worden geharmoniseerd zijn landen ervan verzekerd dat zij de gewenste gegevens kunnen vorderen in andere deelnemende landen. Het verdrag bevat daarnaast verschillende bepalingen over wederzijdse rechtshulp. Zo zijn landen verplicht om 'een zo ruim mogelijke bijstand ten behoeve van onderzoeken of procedures betreffende strafbare feiten' te verlenen (artikel 25 lid 1 CCV). Op basis van artikel 35 stellen deelnemende landen een contactpunt op waarbij 24/7 verzoeken kunnen worden ingediend. In het Cybercrimeverdrag is geen termijn opgenomen waarbinnen landen moeten reageren op een verzoek, wel verplicht de EU-richtlijn 'Aanvallen op informatiesystemen' landen ertoe binnen 8 uur te reageren op een rechtshulpverzoek (Oerlemans, 2019, p. 217).[59] De rechtshulp kan onder meer bestaan uit een spoedbewaring van opgeslagen gegevens (artikel 29 CCV), spoedverstrekking van vastgelegde verkeersgegevens (artikel 30 CCV), toegang tot opgeslagen computergegevens (artikel 31 CCV), verstrekking realtime verkeersgegevens (artikel 33 CCV) en het onderscheppen van de inhoud van berichtenverkeer (artikel 34 CCV). Zonder rechtshulpverzoek kunnen opsporingsambtenaren op basis van artikel 32 CCV buiten de landsgrenzen zich (i) 'toegang verschaffen tot opgeslagen publiek toegankelijke (open bron) computergegevens' en (ii) 'via een computersysteem dat zich op haar grondgebied bevindt, zich toegang verschaffen tot of de beschikking krijgen over opgeslagen computergegevens die zich bevinden in een andere staat'.

2.5 Verstoringsmaatregelen

Verstoringsmaatregelen zijn maatregelen die kunnen worden getroffen om een strafbaar feit te beëindigen, te verhinderen of te belemmeren (Commissie-Koops, 2018, p. 23; Paulus, 2020, p. 14). In dit onderzoek noemen we dergelijke maatregelen tegenhoudmaatregelen omdat ze meer activiteiten omvatten dan alleen het verstoren van criminaliteit. Er kan bijvoorbeeld ook worden gedacht aan preventie of schadebeperking. Tegenhoudmaatregelen kunnen worden getroffen wanneer een verdachte niet kan worden vervolgd (bijvoorbeeld omdat deze niet kan worden geïdentificeerd of zich in het buitenland bevindt), terwijl het wel wenselijk is dat een strafbaar feit wordt gestopt (bijvoorbeeld het offline halen van een server). Voor het treffen van tegenhoudmaatregelen kan de inzet van opsporingsbevoegdheden noodzakelijk zijn (zoals bij het offline halen van een server). In deze situaties betekent het dat voor de inzet van deze bevoegdheden sprake moet zijn van een opsporingsonderzoek. Juridisch gezien zou dit problematisch kunnen zijn als het wenselijk is een opsporingsbevoegdheid in te zetten als tegenhoudmaatregel, zonder dat het doel is een verdachte op te sporen en te vervolgen. Dit knelpunt wordt ook beschreven door de Commissie-Koops, die de vraag stelt of de inzet van

[58] Artikel 14-21 Cybercrimeverdrag.

[59] Artikel 13 en 14 Richtlijn 2013/40/EU aanvallen op informatiesystemen.

opsporingsbevoegdheden nog wel geoorloofd is als in de toekomst opsporing en vervolging van daders niet meer het primaire doel is bij de aanpak van cybercriminaliteit (2018, p. 23).

Bij de inzet van opsporingsbevoegdheden geldt traditioneel dat er toezicht vooraf (toestemming voor de inzet) en toezicht achteraf plaatsvindt (controle bij de rechtszitting) (Commissie-Koops, 2018, p. 24). Deze controle achteraf ontbreekt echter wanneer het doel van de ingezette middelen alleen verstoren is.

3 De integrale aanpak van cybercriminaliteit door politie en OM

In dit hoofdstuk wordt de uitwerking van de integrale aanpak van cybercriminaliteit door de politie en het OM beschreven. De nieuwe structuur waarin de politie werkt wordt toegelicht en de kwantitatieve doelstellingen bij de aanpak van cybercriminaliteit worden beschreven voor zowel politie als OM. Daarna volgt een paragraaf over tegenhoudmaatregelen. Tot slot wordt ingegaan op publiek-private samenwerking in de opsporing. In dit hoofdstuk worden zowel de beleidsmatige kaders geschetst, als de kennis die dit onderzoek heeft opgeleverd over de toepassing in de praktijk.

3.1 Uitwerking beleidsdoelstellingen bij politie en OM

In 2008 is bij de politie het Programma Aanpak Cybercrime (PAC) van start gegaan en werd binnen het Openbaar Ministerie het Intensiveringsprogramma Cybercrime opgericht. Het PAC heeft bij de politie mede op basis van de Veiligheidsagenda 2015-2018 binnen de portefeuille Cybercrime en Digitalisering een vervolg gekregen in de vorm van het Programma Intensivering Aanpak Cybercriminaliteit (PIAC).[60] Daar waar het PAC meer gericht was op agendasetting, is het PIAC gericht op de concrete uitvoering van de doelstelling om cybercriminaliteit effectiever aan te pakken (Van der Laan, Beerthuizen & Weijters, 2016). Naast opsporing en vervolging besteden politie en OM aandacht aan tegenhoudmaatregelen, bijvoorbeeld met behulp van publiek-private samenwerking (PPS). In de volgende paragrafen worden de werkwijzen van politie en OM beschreven.

3.1.1 Politie

In het Regeerakkoord en de Miljoenennota is 145 fte beschikbaar gesteld voor de aanpak van cybercriminaliteit door de politie. Ongeveer twee derde van deze middelen is bedoeld voor de versterking van de cybercrimeteams in de regionale politie-eenheden. De rest is gereserveerd voor de versterking van de Landelijke Eenheid, waar ook THTC onder valt.[61] Door de politie is een plan opgesteld met een voorstel voor de inzet van deze extra personele capaciteit. Dit voorstel is opgesteld door de Portefeuillehouder Digitalisering en Cybercrime, leden van het Project Intensivering Aanpak Cybercrime (PIAC) en THTC en sluit aan bij het door de minister beschreven viersporenbeleid voor de integrale aanpak van cybercriminaliteit.[62] Voorgesteld wordt de operationele thema's op het gebied van cybercriminaliteit te verdelen over THTC en de cybercrimeteams in de regionale politie-eenheden, waarbij elk team een eigen aandachtsgebied (geprioriteerd fenomeen) toegewezen krijgt waarover het een kennispositie kan opbouwen (zie ook Boekhoorn, 2020). Dit voorstel is overgenomen en inmiddels geëffectueerd. De volgende cybercrimi nele fenomenen zijn momenteel verdeeld onder de diverse teams: *Ransomware*, *Phishing*, DDoS, Account-overnames, BEC-fraude/CEO-fraude,[63] *Tech Support*

[60] Veiligheidsagenda 2015-2018.

[61] Politie, intern document.

[62] Politie, intern document; TK brief integrale aanpak cybercriminaliteit, juni 2018.

[63] Oplichtingsmethode waarbij criminelen zich voordoen als CEO (of andere hoge functie) van een bedrijf om werknemers ertoe te bewegen om betalingen te doen. Ook wel CEO-fraude genoemd.

Scam/Helpdeskfraude, *Sextortion*,[64] RAT's,[65] *bulletproof hosting*,[66] vriend-in-nood/WhatsApp-fraude en Betaalverzoekfraude.

Daarnaast worden in dit plan vier kernpunten genoemd die leidend moeten zijn bij de aanpak van cybercriminaliteit. Ten eerste moet een kwantiteit- en kwaliteitsslag worden gemaakt, door het aannemen van extra, gespecialiseerd personeel in alle bestaande cybercrimeteams. Ten tweede wordt ingezet op betere sturing. Omdat cybercriminaliteit zich niet laat begrenzen door districten of regio's wordt een vorm van 'functionele' sturing geïntroduceerd. Hierbij zijn de cybercrimeteams in de eenheden gezamenlijk verantwoordelijk voor het zicht op en de aanpak van fenomenen en is een sturende en coördinerende rol weggelegd voor het oppakken van zaken voor het Landelijk Operationeel Cybercrime Overleg (LOCO). Bij dit operationele overleg zijn teamleiders van de regionale cybercrimeteams, cyberofficieren van het Openbaar Ministerie en leden van DLIO betrokken. Het derde punt betreft de versterking van alle niveaus van cybercriminaliteit. Door informatie, kennis en expertise uit te wisselen tussen alle niveaus van de opsporing, van basisteams tot THTC, zou iedereen van elkaars kennis moeten kunnen profiteren. Tot slot wordt het belang van een uniforme aanpak genoemd. Voor alle teams wordt een gestandaardiseerd werkproces geïntroduceerd, naar het model waar THTC al langer mee werkt. Dit werkproces wordt verderop in deze paragraaf in meer detail beschreven.

In de Veiligheidsagenda 2019-2022 zijn niet alleen ambities beschreven over de kwalitatieve aanpak van cybercriminaliteit, maar ook kwantitatieve doelstellingen geformuleerd over het aantal uit te voeren onderzoeken door de politie en het OM (zie tabel 3.1). De onderzoeken zijn verdeeld in drie typen (zie tabel 3.1). Ten eerste zijn er de reguliere onderzoeken, die worden uitgevoerd in de eenheden. Deze onderzoeken moeten veelal worden uitgevoerd door districten, basisteams of cybercrimeteams en zijn gericht op de aanpak van cybercriminaliteit in enge zin of *computer-focused* crime. Ten tweede zijn er fenomeenonderzoeken, die gericht zijn op de 'brede bestrijding van eenheidsoverstijgende cybercriminele fenomenen en dadergroepen'. Dit zijn complexe onderzoeken die buiten de taakstelling van Team High Tech Crime vallen en moeten worden uitgevoerd door de gespecialiseerde regionale cybercrime teams. Naast cybercriminaliteit in enge zin vallen ook onderzoeken naar *computer-enabled* criminaliteit, waarbij bijvoorbeeld sprake is van innovatief gebruik van technologie of een sterke nadruk ligt op digitale opsporingsmethoden in deze categorie. Deze onderzoeken zijn er, naast het identificeren van daders, ook op gericht om een betere informatiepositie op te bouwen over bepaalde cybercriminele fenomenen. De informatie die wordt verzameld over een fenomeen wordt door de politie beschreven in een zogeheten '*book of crime'* waarin de stappen van de delictsvorm zo volledig en nauwkeurig mogelijk in kaart worden gebracht om zodoende tot een passende aanpak te komen. Het is de bedoeling dat elke eenheid een *book of crime* maakt over zijn eigen geprioriteerde fenomeen. Dit document kan dan gedeeld worden binnen de politie, bijvoorbeeld met de andere cybercrimeteams. De coördinatie en verdeling van deze onderzoeken vindt plaats in het LOCO. Het derde type zaken zijn de onderzoeken van het Team High Tech

[64] Manier van afpersen waarbij gedreigd wordt met het openbaren van seksueel getint materiaal.

[65] RAT staat voor *Remote Access Tool*. Dat is software waarmee vanaf één basiscomputer kan worden ingelogd op alle geregistreerde computers die bij een netwerk horen en waarmee ze op afstand kunnen worden beheerd, bijvoorbeeld door systeembeheerders van een ICT-afdeling. Een RAT kan ook gebruikt worden voor criminele doeleinden.

[66] Een bedrijf dat de mogelijkheid biedt volledig anoniem gebruik te maken van serverruimte en er daarmee van verdacht wordt bewust criminaliteit te faciliteren.

Crime. Op de samenstelling en doelstelling van THTC en de cybercrimeteams in de eenheden wordt later in dit hoofdstuk nader ingegaan.

Tabel 3.1 Overzicht kwantitatieve doelen Veiligheidsagenda 2019-2022

	2019		2020		2021	2022
	Doel	Afgerond	Doel	Afgerond	Doel	Doel
Regulier	310	381	310	468	310	Ntb
Waarvan 25% alternatieve of aanvullende interventies	77	36	77	38	77	Ntb
Fenomeen	41	21	41	39	41	Ntb
Waarvan 50% alternatieve of aanvullende interventies	20	0	20	0	20	Ntb
THTC	20	19	20	12	20	Ntb
Totaal	**371**	**421**	**371**	**519**	**371**	**Ntb**

Bron: https://www.rijksfinancien.nl/memorie-van-toelichting/2022/OWB/VI/onderdeel/1033739

Zoals te zien is in tabel 3.1 is in de veiligheidsagenda ook beschreven welk percentage van de onderzoekscapaciteit mag worden besteed aan alternatieve of aanvullende interventies. Met alternatieve of aanvullende interventies worden afdoeningen bedoeld die in plaats van het strafrecht of in aanvulling daarop worden toegepast. Specifiek voor cybercriminaliteit gaat het dan met name om maatregelen als preventie, verstoring, schadebeperking of notificatie van slachtoffers. Voor de onderzoeken van Team High Tech Crime wordt in de veiligheidsagenda geen onderscheid gemaakt tussen opsporingsonderzoeken en aanvullende interventies.

In een Kamerbrief van eind juni 2020 over de voortgang van de integrale aanpak van cybercriminaliteit staat beschreven dat in 2019 in totaal 21 fenomeenonderzoeken zijn afgerond. Verder zijn er 381 reguliere onderzoeken afgerond en heeft THTC 19 van de 20 geambieerde zaken afgerond.[67] In 2020 zijn 468 reguliere onderzoeken afgerond. Bij 8% van de reguliere onderzoeken was sprake van alternatieve of aanvullende interventies. Daarnaast zijn 39 fenomeenonderzoeken afgerond en 12 zijn *hightechcrime* onderzoeken uitgevoerd door THTC.[68]

Team High Tech Crime

Team High Tech Crime is het specialistische politieteam van de Landelijke Eenheid dat cybercriminaliteit met een *hightech* component onderzoekt. Het team geeft aan dat zij de volgende typen zaken onderzoekt: 'cybercrime die gekenmerkt wordt door een combinatie van de volgende factoren: geavanceerde methoden voor het plegen van het misdrijf en het afschermen van de activiteiten en de identiteit van de criminelen, hoge mate van schaalbaarheid, grote maatschappelijke impact (b.v. ontwrichting), hoge mate van gerichtheid van de aanvallen, sterke internationale component, hoge organisatiegraad'.[69] Het team is in 2006 opgericht en bestaat uit zowel digitaal experts als tactisch en financieel rechercheurs. Daarnaast werken in het team onder andere ook analisten, dossiervormers en coördinatoren. Voor de oprichting van dit team was de politie ook al bezig met de aanpak van criminaliteit in 'cyberspace'. Zo was er in 1999 sprake van een Landelijke Unit Digitaal Rechercheren en zijn nadien diverse andere initiatieven gevolgd. Hierbij was telkens sprake van een zoektocht naar de beste manier om de in toenemende mate digitaliserende criminaliteit aan te pakken (Stol & Strikwerda, 2017).

[67] TK brief voortgang integrale aanpak cybercrime, 29 juni 2020.

[68] Jaarverantwoording 2020, Nationale Politie.

[69] Politie, intern document.

In 2012 is THTC uitgebreid en ten tijde van de uitvoering van dit onderzoek werkten er ongeveer 120 mensen. THTC bestaat uit één vooronderzoeksteam en drie operationele teams. Het vooronderzoeksteam voorziet de onderzoeksteams van input voor opsporingsonderzoeken en de invulling van 'brede bestrijding'. Tot en met 2019 richtte THTC zich met name op cybercriminaliteit die gericht was op de financiële sector, de vitale infrastructuur, economische spionage, grote datalekken en cybercriminele afpersingen. Vanaf 2020 zijn de onderzoeken meer actorgericht en ligt de aandacht op de aanpak van key facilitators, *bulletproof hosters*[70] en autonome groeperingen.

Naast dit soort grote opsporingsonderzoeken verleent THTC ook assistentie aan andere politieteams – zowel binnen, als buiten het cybercrimedomein – en handelt het rechtshulpverzoeken af.
De kennis die THTC opdoet kan vervolgens worden overgedragen aan de regionale eenheden. Zo kan bijvoorbeeld een innovatieve bestrijdingsvorm van cybercriminaliteit in eerste instantie worden uitgevoerd door THTC, om de opgedane expertise vervolgens beschikbaar te maken voor de cybercrimeteams. Vervolgens kunnen de regionale cybercrimeteams de opgedane kennis ook onderling uitwisselen. Een voorbeeld hiervan is de aanpak van criminele cryptocommunicatie. In hoofdstuk 4 wordt nader ingegaan op de werkwijze van THTC tijdens opsporingsonderzoeken.

Cybercriminaliteit is in hoge mate schaalbaar. Daarmee wordt bedoeld dat het eenvoudig in grootte toe kan nemen. Door het Internet is er een enorm bereik en daarmee een toegenomen en laagdrempelige afzetmarkt van illegale goederen en diensten, bijvoorbeeld via online marktplaatsen (Odinot, De Poot & Verhoeven, 2018; Van de Sandt, 2019). Hierbij worden diensten aangeboden en afgenomen voor zowel het plegen, als het afschermen van cybercriminaliteit. Het identificeren en bestrijden van de belangrijkste verleners van dit soort diensten is één van de prioriteiten van THTC. Door in te zetten op de aanpak van zogenoemde *facilitators* is de verwachting dat met één onderzoek meer effect kan worden gesorteerd dan met het opsporen en vervolgen van een enkele afnemer van zo'n dienst. Daarnaast richten zij zich in de opsporingsonderzoeken op *bulletproof hosters*.

THTC werkt met een raamwerk dat ook wel CSAE wordt genoemd. De afkorting CSAE staat voor *collect*, *store*, *analyse* en *engage* (Van de Sandt et al., 2021). Dit raamwerk biedt voor elke fase van het opsporingsproces handvatten om op gestructureerde wijze om te gaan met ongestructureerde en/of grote hoeveelheden data. Het raamwerk gaat uit van de toegevoegde waarde die een datagedreven aanpak kan hebben voor de opsporing van georganiseerde criminaliteit (Van de Sandt et al., 2021). Het werkproces is ontstaan vanuit een behoefte om een betere informatiepositie op te bouwen door digitale sporen te bundelen en data te structureren. Op die manier kan informatie die is verzameld in opsporingsonderzoeken breder worden geanalyseerd en worden gebruikt in andere onderzoeken. Ook kan de informatie gebruikt worden om zicht te krijgen op cybercriminele fenomenen en bijdragen aan de ontwikkeling van nieuwe methoden en middelen bij het aanpakken en tegenhouden van cybercriminaliteit. Het werkproces bevat zowel een technische kant (bijvoorbeeld welke verdachten, c.q. werkwijzen, in meerdere onderzoeken voorkomen), als een tactische kant (op welk fenomeen een volgend onderzoek zich moet richten).

[70] Een bedrijf dat de mogelijkheid biedt volledig anoniem gebruik te maken van serverruimte en er daarmee van verdacht wordt bewust criminaliteit te faciliteren.

Een politiefunctionaris verwoordt de ontwikkeling om de aanpak van cybercriminaliteit op een meer datagedreven wijze vorm te geven als volgt:

> *'THTC werkt binnen het, en samen met cybercrimedomein van de politie aan het ontwikkelen en implementeren van datagedreven bestrijding om de toenemende complexiteit die criminaliteitsbestrijding in het informatietijdperk met zich meebrengt het hoofd te bieden. Het bijbehorende raamwerk CSAE is gebaseerd op verschillende bestaande technische standaarden, maar aangepast aan de specifieke doel- en taakstellingen van de politie. Het raamwerk omvat zowel het bedrijfsproces dat nodig is om datawetenschappelijke methoden en technieken te integreren in de bestrijding van misdaad, als de methodologie die daaraan verbonden kan worden. Het CSAE-raamwerk helpt om gegevens beter te ordenen en gericht tooling te ontwikkelen waarmee THTC beter in staat is om verbanden in data van verschillende (lopende of eerdere) onderzoeken te vinden en/of te correleren.'*

Het CSAE-raamwerk doet enigszins denken aan de 'Raffinaderij', een ICT-voorziening binnen de politie die het mogelijk maakt om snel grote hoeveelheden politiegegevens in samenhang met elkaar te analyseren en te visualiseren (De Vries, 2017). Om informatie op die manier te mogen verwerken en analyseren moet wel sprake zijn van gegevens die rechtmatig in een onderzoek zijn gebracht en verwerking die plaatsvindt met een duidelijke doelbinding. De Raffinaderij wordt bijvoorbeeld gebruikt in het kader van titel V-onderzoeken (georganiseerde misdaad) en titel VB-onderzoeken (terrorisme) (zie ook: Huisman et al., 2016, p. 9).

Bij het CSAE-raamwerk wordt de juridische grond gebaseerd op de Wet politiegegevens (Wpg). De juridische verantwoording voor de datagedreven manier van werken wordt door een politiefunctionaris als volgt verwoord:

> *'De Wpg geeft de wettelijke basis voor het, onder strikte voorwaarden, in combinatie verwerken van politiegegevens, teneinde vast te stellen of verbanden bestaan tussen deze gegevens. Dit met in achtneming van de specifieke WvSv-bepalingen die impact hebben op de verwerkingen onder het Wpg-regime. Indien zulke verbanden bestaan kunnen de gerelateerde gegevens – na instemming van een daartoe bevoegde functionaris – worden gebruikt voor een andere verwerking zoals een opsporingsonderzoek. De verwerkingstermijnen van deze politiegegevens zijn bij wet bepaald. De gebruikstermijn, bewaartermijn en termijn voor vernietiging, verschillen per categorie politiegegevens. Het voordeel van de meer centrale opslag en verwerking in het kader van het CSAE-raamwerk is dat het de politie in staat stelt om effectiever dergelijke termijnen, alsmede andere juridische waarborgen en verantwoordingsplichten, na te leven.'*

Zoals hierboven beschreven bestaat CSAE uit een viertal stappen. De eerste stap is '*collect'*, hierbij worden de data verzameld. De tweede stap is '*store'*, het eenduidig bewerken en opslaan van data en deze vervolgens bundelen tot stukjes informatie die relevant zijn voor de opsporing. De derde stap is '*analysis'*, het analyseren en minimaliseren van de beschikbare informatie met uiteenlopende *tools* en datamodellen. De informatie wordt met de juiste domeinkennis omgezet in wat de politie noemt '*intelligence'* over de meest relevante subjecten (datareductie), en wordt verrijkt met reeds bekende informatie. De informatie en kennis die hieruit wordt opgedaan kan worden ingezet bij de interventies in de vierde stap van het model. Die vierde stap is '*engagement'*, waarbij wordt overgaan tot daadwerkelijke interventies op basis van de geanalyseerde informatie. Hierbij wordt een breed bestrij-

dingsmodel gehanteerd dat zich zowel richt op de dader, als het slachtoffer, als de criminele infrastructuur (zie figuur 3.1). Het integrale bestrijdingsmodel – dat ook wordt gebruikt door de regionale cybercrimeteams – wordt ook wel het 'ballonnenmodel' genoemd en bestaat uit de volgende elementen:

a attributie (inclusief vervolging van daders);
b disruptie of verstoring van het criminele proces;
c slachtofferhulp;
d mitigatie of schadebeperking.

Figuur 3.1 Integrale bestrijdingsmodel

In één opsporingsonderzoek kunnen meerdere elementen uit dit ballonnenmodel worden 'doorgeprikt'. Dit komt omdat op servers vaak niet alleen dadersporen te vinden zijn, maar ook slachtofferinformatie en informatie over de modus operandi. Bij voorkeur hebben alle elementen uit het model een plek gekregen in een opsporingsonderzoek om zodoende een zo groot mogelijk effect te sorteren met de ingezette middelen.

Cybercrimeteams eenheden

Naast de (inter)nationale aanpak van cybercriminaliteit is men vanaf 2015 ook gestart met een aanpak op het niveau van de regionale politie-eenheden. Met de oprichting van speciale cybercrimeteams in de eenheden heeft de politie de ambitie om ook de regionale eenheden meer complexe opsporingsonderzoeken te laten doen, conform de resultaatafspraken die voortvloeien uit de Veiligheidsagenda, en via deze teams de digitale ontwikkeling binnen een politie-eenheid te stimuleren (Boekhoorn, 2020). De cybercrimeteams werken in een landelijke structuur samen met het THTC en ondersteunen districtsrecherches en basisteams bij de kennisopbouw voor de uitvoering van reguliere onderzoeken naar cybercriminaliteit. Op die manier is het de bedoeling dat regionale eenheden een groter aantal cyberzaken kunnen uitvoeren. Verder is het de bedoeling dat de cybercrimeteams publiek-private samenwerkingen aangaan en bestrijdingsaanpakken ontwikkelen voor de cybercriminele fenomenen die aan hen zijn toegewezen.[71]

Cybercrimeteams moeten vanuit de veiligheidsagenda focussen op cybercriminaliteit in enge zin, maar nemen in de praktijk ook veel meldingen over cybercriminaliteit in

[71] TK brief Voortgang integrale aanpak van cybercrime, 29 juni 2020.

ruime zin in behandeling omdat de scheidslijn tussen cybercriminaliteit in enge zin en in ruime zin niet altijd te trekken is (Boekhoorn, 2020).

De teams in de eenheden zijn naar het model van THTC multidisciplinair vormgegeven. De bezetting bestaat idealiter in elke eenheid uit: een teamleider, een digitaal coördinator, twee of drie digitaal rechercheurs, vier of vijf tactisch rechercheurs, een *OSINT*-rechercheur[72], een financieel rechercheur, twee analisten, een projectvoorbereider, een dossiervormer en een specialist PPS die zich specifiek bezighoudt met publiek-private samenwerking.[73] De insteek is dat ook deze teams gaan werken volgens het CSAE-raamwerk.

Bij de start van dit onderzoek stond de vorming van de regionale cybercrimeteams nog in de kinderschoenen. Hoewel de cybercrimeteams in de eenheden een andere rol hebben bij de aanpak van cybercriminaliteit dan THTC zijn er wel raakvlakken tussen en in sommige gevallen ook overlap met het type opsporingsonderzoek dat wordt gedaan. De bedoeling is ook dat de regionale cybercrimeteams in de toekomst meer complexe onderzoeken kunnen doen. Op het moment dat werd gestart werd met dit onderzoek waren de teams, zoals eerder geschreven, nog in opbouw en waren er weinig regionale opsporingsonderzoeken die binnen de scope van dit onderzoek vielen. Om die reden staan we in dit rapport alleen kort stil bij de rol en doelstelling van de cybercrimeteams in de eenheden en is slechts één regionaal opsporingsonderzoek meegenomen in het dossieronderzoek.

3.1.2 OM

Het Openbaar Ministerie (OM) heeft het gezag over de opsporing, en beslist over de aanpak van zaken, de inzet van bevoegdheden en de strafrechtelijke vervolging. Op landelijk niveau beschikt het OM over een landelijk officier van justitie cybercriminaliteit die is gespecialiseerd in de aanpak van complexere vormen van cybercriminaliteit. Alle parketten hebben een eigen cybercrime portefeuille. Dit is in de meeste gevallen een deeltijdfunctie. De regionale cyberofficieren zijn de experts die cybercrimezaken oppakken, maar kunnen ook collega-officieren helpen die aan reguliere zaken werken en met vragen zitten over de aanpak van cybercriminaliteit.

Ook het OM heeft kwalitatieve doelstellingen geformuleerd over de aanpak van cybercriminaliteit in het missie-visiedocument 'Aanpak van cybercrime 2019-2022'.[74] De verantwoordelijkheid voor de aanpak van cybercriminaliteit ligt primair bij de regioparketten, die hierin worden gefaciliteerd vanuit het Landelijk Parket. In overeenstemming met de doelen die voor en door de politie zijn geformuleerd wil ook het OM inzetten op een combinatie van incidentgerichte opsporingsonderzoeken en onderzoek naar fenomenen. In het visiedocument staat beschreven dat het OM naast het uitvoeren van de kerntaken opsporen en vervolgen, ook actief bijdraagt aan het tegenhouden van cybercriminaliteit, bijvoorbeeld door middel van publiek-private samenwerking. Daarnaast is het streven om bij de regioparketten ook zaken met een complexe technische of internationale component te laten oppakken, vergelijkbaar met de regionale cybercrimeteams bij de politie en conform de afspraken van de Veiligheidsagenda.

---

[72] OSINT staat voor *Open Source Intelligence* en gaat over het verzamelen van informatie middels open bronnen onderzoek, zoals in geschreven teksten, social media, foto, video- en audiofragmenten.

[73] Intern document politie.

[74] OM. Aanpak van cybercrime 2019-2022.

In het jaarbericht 2019 beschrijft het OM dat het aantal verdachten dat werd vervolgd voor cybercriminaliteit in dat jaar toenam met 26%. In totaal 381 verdachten moesten zich verantwoorden voor de rechter of kregen een straf opgelegd door het OM.[75] Ook is het aantal personen dat in verband met een cybercrimedelict werd veroordeeld tot een vrijheidsstraf hierin opgenomen. Het ging om in totaal 50 veroordelingen: 29 personen kregen een vrijheidsstraf tot één jaar; 9 een straf van één tot tweejaar; 11 een straf van twee tot vijf jaar en 1 persoon kreeg een straf van meer dan vijf jaar.

Boekhoorn (2020) beschrijft in zijn onderzoek naar de aanpak van cybercriminaliteit in drie regio's dat veel van de door de politie aangedragen cyberzaken bij het OM eindigen in een sepot. Veelal gaat het bij deze zaken om een technisch sepot. In dat geval gaat het OM niet over tot vervolging, omdat het vervolgingstraject kansloos wordt geacht, bijvoorbeeld wegens gebrek aan bewijs, of omdat de verdachte zich het buitenland ophoudt en niet kan worden aangehouden. Hiermee moet rekening worden gehouden als de cijfers van politie en OM met elkaar vergeleken worden; de politie draagt meer zaken aan bij het OM, dan het OM kan vervolgen.

3.2 Tegenhoudmaatregelen

Zoals eerder beschreven beperkt de aanpak van cybercriminaliteit zich niet tot opsporing en vervolging. Tijdens de opsporing en vervolging van cybercriminaliteit kunnen politie en OM met diverse uitdagingen te maken krijgen. Bovendien biedt het strafrecht lang niet altijd een adequate oplossing voor een geconstateerd criminaliteitsprobleem. Daarom wordt soms voor niet-strafrechtelijke oplossingen gekozen om een crimineel proces te ontwrichten of tegen te gaan. Dat gebeurt zowel bij reguliere opsporingsonderzoeken, als ook meer integraal, in de vorm van (soms langlopende) publiek-private samenwerkingsprojecten die gericht zijn op het tegengaan van bepaalde vormen van criminaliteit.

In de Veiligheidsagenda 2019-2022 wordt verstoring genoemd als onderdeel van het 'palet aan interventies' bij de aanpak van cybercriminaliteit. In het stuk is echter niet gespecificeerd wat er onder verstoring wordt verstaan. Het begrip 'verstoring' kent geen juridische of taalkundige definitie en ook in de praktijk blijkt het een breed begrip dat opsporingsfunctionarissen verschillend definiëren (Paulus, 2020). Soms wordt een smalle definitie gehanteerd waarbij het gaat om technisch ingrijpen, bijvoorbeeld door het offline halen van een server die gebruikt wordt bij het plegen van criminele activiteiten. In andere gevallen wordt het als een breed containerbegrip gebruikt waar verschillende tegenhoudmaatregelen onderdeel van uitmaken.

Ook in de literatuur wordt er geen eenduidige definitie gehanteerd. Zo plaatst Bjørgo (2019) verstoring in een palet van algehele preventieve maatregelen, wat impliceert dat verstoring als een onderdeel van preventie kan worden gezien. Kirby en Penna (2010) stellen daarentegen dat preventie moet worden gezien als het voorkomen van een toekomstig *crime event,* bijvoorbeeld door middel van situationele preventie, terwijl verstoring zich focust op een dader(groep) die bezig is delicten te plegen. Verstoring wordt door deze auteurs gezien als *'a flexible, transitory and dynamic tactic which can be used more generally to make the environment hostile for the organised crime group.'*

[75] OM: Jaarbericht 2019.

Veel onderzoek naar verstoring van criminaliteit gaat over het verstoren van criminele netwerken, waarbij verstoring voornamelijk wordt bereikt door het verwijderen van actoren uit een netwerk (Agreste et al., 2016; Duijn, Kashirin & Sloot, 2014; Bright et al., 2017). Ook dan wordt uitgegaan van een daderperspectief. Onafhankelijk van de vraag of criminaliteit wordt verstoord met een dadergerichte aanpak, of met een aanpak die gericht is op de criminele activiteit, lijken diverse auteurs het erover eens te zijn dat opsporing zich richt op het verleden, verstoring zich richt op het heden en preventie zich richt op de toekomst (Kirby & Snow, 2017).

In het onderzoek van Van de Sandt (2019) wordt dit onderscheid tussen opsporing en verstoring veel minder hard gemaakt, en wordt evenmin uitgegaan van één enkel perspectief op ofwel de dader, ofwel de activiteit. Hij ziet verstoring als het hinderen van (1) het proces van criminaliteit, (2) het verbergen van criminaliteit en (3) de crimineel, en geeft daarnaast aan dat verstoring niet los gezien kan worden van de opsporing en vervolging. Enkel de aanwezigheid van de mogelijkheden die opsporingsinstanties bezitten geven al een vorm van verstoring. Immers, door de dreiging die uitgaat van opsporingsinstanties die bevoegdheden kunnen inzetten waardoor daders betrapt en bestraft kunnen worden, moeten daders hun criminele processen beschermen en worden ze in hun handelen verstoord. De samenhang is echter nog veel sterker. Juist door het opsporingsonderzoek kan zicht ontstaan op het criminele proces en daarmee op mogelijkheden om dat proces te verstoren. Zonder actuele kennis over gebruikte criminele methoden die wordt opgedaan door middel van opsporingsonderzoeken kunnen ook geen efficiënte tegenhoudacties worden ingezet. Opsporing en verstoring gaan dus hand in hand bij de aanpak van cybercriminaliteit.

Hoewel er dus geen consensus is over het begrip verstoring in de literatuur, wordt verstoring over het algemeen gezien als een onderdeel van het brede palet aan interventies dat kan worden ingezet bij de aanpak van cybercriminaliteit. Dit palet aan interventies wordt binnen de politie ook wel samengevat in het eerder beschreven 'ballonnenmodel'. In het voorliggende onderzoek zullen we vanwege het gebrek aan consensus over het begrip 'verstoring' spreken over tegenhoudmaatregelen wanneer het gaat over een breder pakket aan niet-strafrechtelijke oplossingen bij de aanpak van cybercriminaliteit.

3.2.1 Inzet van tegenhoudmaatregelen door de opsporing

Ondanks de meerwaarde die tegenhoudmaatregelen kunnen hebben bij de aanpak van cybercriminaliteit, is soms twijfel over de juridische borging van de inzet van tegenhoudmaatregelen door de opsporing. Het gebrek aan controle achteraf is één van de zorgpunten van juristen en privacy-experts (Commissie-Koops, 2018). Deze controle ontbreekt wanneer opsporingsbevoegdheden alleen worden ingezet ten behoeve van tegenhoudmaatregelen, omdat de zaak dan immers niet voor de rechter wordt gebracht. In recent onderzoek heeft Paulus (2020) door middel van interviews onderzocht in hoeverre officieren van justitie bewust voor verstoringsmaatregelen kiezen om de rechterlijke toets te ontlopen. Dit bleek niet het geval te zijn. Desalniettemin is het gebrek aan rechtelijke toetsing van de opsporingsbevoegdheden die gebruikt worden ten behoeve van de inzet van tegenhoudmaatregelen een punt van zorg, temeer omdat het bij cybercrime-onderzoeken regelmatig voorkomt dat er geen dader geïdentificeerd of vervolgd kan worden waardoor het proces van opsporing en verstoring bij deze zaken achteraf niet wordt onderworpen aan een rechterlijke toetsing.

3.3 Publiek-private samenwerking

Publiek-private samenwerking (PPS) is een wezenlijk onderdeel van de integrale aanpak van cybercriminaliteit. Daarom wordt hieronder kort ingegaan op het ontstaan van publiek-private samenwerking in het veiligheidsdomein. In hoofdstuk 5 zal in nader worden ingegaan op voorbeelden van dit soort samenwerkingen bij de aanpak van cybercriminaliteit.

3.3.1 Oorsprong van publiek-private samenwerking

De opkomst van PPS voor de uitvoering van overheidstaken kent haar oorsprong in de jaren tachtig (Klijn & Van Twist, 2007) waarbij een kostenefficiënt overheidsoptreden het hoofdargument was (Van Montfortet al., 2012). Naast hervormingen op budgettair gebied vond er in deze periode ook onder andere meer privatisering plaats en werd de rol van de burger in het overheidsoptreden benadrukt (Schedler & Proeller, 2000; Gruening, 2001). Ook in Nederland was deze transitie zichtbaar. In het regeerakkoord van kabinet-Lubbers II werd het belang van PPS onderstreept en werden processen van privatisering, deregulering en verzelfstandiging gestimuleerd (De Waard & Scheepmaker, 2012; Klijn & van Twist, 2007). Bij de politie werd in deze periode tevens gestreefd naar een grotere verantwoordelijkheid van burgers en private partijen voor de Nederlandse veiligheidszorg (Raad van Hoofdcommissarissen, 2005).
Er ontstond echter ook kritiek op het fenomeen PPS. De resultaten van verschillende projecten bleken tegen te vallen (Klijn & Van Twist, 2007) en ook schortte het bij de samenwerkingen op het gebied van veiligheid aan een duidelijke visie op de kansen, bedreigingen en begrenzingen van PPS (De Waard & Scheepmaker, 2012). Dit resulteerde in een afnemende populariteit voor het aangaan van PPS.

De laatste twee decennia zijn publiek-private samenwerkingen echter weer in opkomst (Hagenaars & Bonnes, 2020, Van Montfort et al., 2012). In de afgelopen 25 jaar is een beweging zichtbaar waarbij bedrijven ook meer worden aangesproken op hun maatschappelijke verantwoordelijkheid en op hun zorgplichten ten aanzien van veiligheid (Hagenaars & Bonnes, 2020; Van Montfort et al., 2012; Kokkeler, 2017; Munnich, Kouw & Kool, 2007). Op het gebied van digitale veiligheid is dit eveneens van belang aangezien de digitale infrastructuur en de voornaamste digitale expertise in private handen is (Hagenaars & Bonnes, 2020). In 2005 publiceerde de Raad van Hoofdcommissarissen een uitgebreide visie op hoe PPS in relatie staat tot de politie en de veiligheidszorg. Hierin wordt PPS als middel behandeld om de doelen van het concept 'integraal veiligheidsbeleid' te behalen, zoals het in de definitie van integraal veiligheidsbeleid impliciet is verwoord:

> *'Integraal veiligheidsbeleid is, onder regie van het openbaar bestuur, het in samenhang inzetten van organisaties, middelen en instrumenten op verschillende beleidsterreinen, met als doel het bestrijden van onveiligheid dan wel het voorkomen en beheersen daarvan.'*
> (Raad van Hoofdcommissarissen, 2005)

Ook het concept 'tegenhouden' wordt door de Raad van Hoofdcommissarissen (2005) in verband gebracht met PPS. De wens bestaat om veiligheidsproblemen systeemgericht, multidisciplinair aan te pakken waardoor inbreuk op de veiligheid en maatschappelijke integriteit vroegtijdig wordt beëindigd. Deze benadering vereist volgens de Raad van Hoofdcommissarissen samenwerking met andere partijen buiten de politie.

3.3.2 Kanttekeningen bij publiek-private samenwerking

Hoewel PPS kansen biedt voor een effectiever en efficiënter overheidsoptreden, bestaan er ook risico's waar de partijen zich van bewust moeten zijn. Heldeweg en Sanders (2011) stippen aan dat bij enkele PPS-varianten publieke waarden en de legitimiteit gevaar lopen. Dit is met name het geval wanneer private partijen deelnemen aan de besluitvorming en daarmee medebepalend zijn voor de behartiging van het publieke belang. In beginsel is dat geen taak voor private partijen, terwijl private partijen hiermee wel invloed hebben op bindende gevolgen voor derden. Heldeweg en Sanders (2011) wijzen op de gevolgen voor de 'klassiek democratisch-rechtsstatelijke legitimiteit' en een potentieel gevaar van oneerlijke verdeling van voor- en nadelen. Ook verliest de overheid mogelijk een deel van haar zeggenschap bij het aangaan van PPS en kan de samenwerking met private partijen leiden tot een afnemende transparantie van overheidsbesluiten (Sanders, 2017).

Bij het aangaan van PPS in het kader van de strafrechtspleging is het van belang om vooraf stil te staan bij de botsende waarden tussen private en publieke partijen. Hierbij kan gedacht worden aan de vraag welke informatie private partijen vanuit de overheid krijgen, wat zij met deze informatie behoren te doen en wie erop toeziet dat de informatie enkel voor de beoogde doelen worden gebruikt. Publieke waarden kunnen onder meer worden geborgd door goed gebruik van regels (wetten, contracten, convenanten enz.) en een duidelijke hiërarchie tussen de partijen (Hoepman, Koops & Lueks, 2014; Scheltema et al., 2000). De politie werkt op het gebied van cybercriminaliteit graag samen met private partijen. Dit wordt in eerste instantie gedaan bij opsporingsonderzoeken waarbij de expertise van een private partij kan helpen bij het oplossen van een specifiek probleem. Ook dragen private partijen soms zaken aan waarna vervolgens wordt overgegaan tot een opsporingsonderzoek, zoals bijvoorbeeld het geval was in een aantal van de zaken die bestudeerd zijn voor dit onderzoek. In tweede instantie wordt de samenwerking meer structureel gezocht via langlopende projecten.

4 Opsporingsonderzoeken naar cybercriminaliteit

Voor dit onderzoek zijn acht cyberonderzoeken bestudeerd, een korte zaaksbeschrijving van deze opsporingsonderzoeken staat in paragraaf 4.1. In paragraaf 4.2 staat beschreven hoe opsporingsonderzoeken worden gestart en wat de keuzes zijn die een rol spelen bij het oppakken van een zaak. In paragraaf 4.3 staat beschreven welke opsporingsmiddelen en -methoden worden ingezet en met welk doel. In paragraaf 4.4 wordt ingegaan op de inzet van tegenhoudmaatregelen tijdens of na de opsporingsonderzoeken. Vervolgens wordt ingegaan op mogelijkheden tot vervolging die de opsporingsonderzoeken bieden. In bijlage 1 worden een aantal veelvoorkomende cyberdelicten toegelicht.

4.1 Casebeschrijvingen

Hieronder volgt een beschrijving van de zaken die voor dit onderzoek zijn bestudeerd. In tabel 4.1 staat een samenvatting van de strafbare feiten waar deze opsporingsonderzoeken zich op richtten.

4.1.1 DDoS-aanvallen

De politie ontving informatie van een buitenlandse politiedienst dat in Nederland een omvangrijke *bootersite*[76] werd gehost. De website stelde klanten in staat om DDoS-aanvallen uit te voeren. Meerdere beheerders van verschillende nationaliteiten (waaronder hoogstwaarschijnlijk één Nederlander) werden in de informatie genoemd. De site had maandelijks 150.000 klanten wereldwijd en er werd jaarlijks ongeveer 100.000 dollar via Bitcoin-betalingen verdiend.
Van de servers van deze bootersites zijn diverse kopieën gemaakt en door middel van een datatap ontstond een gedetailleerd overzicht van de gebruikers. Tot slot is de website uit de lucht gehaald. De rol van de Nederlandse beheerder bleek beperkt en hem is een alternatieve afdoening opgelegd. In dit onderzoek is door THTC samenwerking gezocht met de cybercrimeteams in de eenheden vanwege de regionale spreiding van de Nederlandse klanten van de website. Daarnaast was er ook een sterke internationale component: zowel beheerders als klanten bevonden zich (ook) in het buitenland. Hier is in internationaal verband actie op ondernomen via Europol. Naast veroordelingen zijn in Nederland ook personen benaderd in de vorm van *knock and talk* gesprekken[77]. Na het offline halen van de website zijn nog een aantal andere tegenhoudmaatregelen genomen. Op de website Reddit[78] is door THTC een pagina aangemaakt waar gebruikers vragen konden stellen over onder andere DDoS. Ook is er een Google Advertisement campagne opgestart om internetgebruikers erop te attenderen dat DDoS-aanvallen strafbaar zijn.

[76] Een *bootersite* voert niet op eigen initiatief een DDoS-aanval uit, maar faciliteert het in gang zetten daarvan na betaling door een klant.

[77] Bij *knock and talk* gesprekken worden personen thuis bezocht door de politie om in gesprek te gaan over de feiten en bewustwording te creëren over de strafbaarheid van handelingen.

[78] Een *social media website* waarop gebruikers links en tekst kunnen plaatsen.

4.1.2 Malware bij banken

Door een tip van een privaat bedrijf waar THTC vaker mee samenwerkt, kwam een zaak aan het licht waaruit bleek dat systemen van buitenlandse financiële instellingen succesvol waren geïnfecteerd met geavanceerde *malware* door middel van een *reverse shell*[79] en een *keylogger*[80]*.* Hierdoor was men in staat om vanuit het bedrijfsnetwerk van een bank financiële transacties te verrichten, veranderen of verwijderen. Door frauduleuze transacties is voor minstens 350.000 Britse Pond bankfraude gepleegd bij een Amerikaanse bank. De zaak wordt door THTC opgepakt omdat één *keylogger* server bij een Nederlandse provider werd gehost en de zaak een zeer innovatieve modus operandi liet zien. De data op de Nederlandse server is gevorderd en onderzocht. Twee banken zijn als gevolg van dit onderzoek genotificeerd over het risico dat zij liepen op een potentiële aanval via deze *malware*, en hebben hierop kunnen acteren. In de Verenigde Staten is een mogelijke verdachte geïdentificeerd, maar het is onbekend of deze persoon door de Amerikaanse autoriteiten is opgepakt of vervolgd.

4.1.3 Hack

Bij een hack op een Amerikaans bedrijf zou een aanzienlijke hoeveelheid gegevens zijn gestolen. Deze gegevens zouden bekend worden gemaakt als het bedrijf geen miljoenenbedrag aan *bitcoins* zou overmaken. De FBI is naar aanleiding hiervan een onderzoek gestart naar de onbekende daders die verdacht werden van computervredebreuk en afpersing van het bedrijf. De site waarop de gelekte gegevens stonden verwees naar een IP-adres in Nederland. Er is daarom een opsporingsonderzoek gestart met als doel het stoppen van strafbare feiten en het opsporen en vervolgen van verdachten die computervredebreuk hebben gepleegd en daarbij mede gebruik hebben gemaakt van de Nederlandse digitale infrastructuur. De server waarop de gegevens stonden is veiliggesteld. Na onderzoek bleek deze te fungeren als een soort database waarbij bedrijfsgevoelige informatie was opgeslagen van diverse slachtoffers. Volgens informatie van de FBI was de groepering achter deze hack mogelijk gelinkt aan een statelijke actor en zouden zij zich ook richten op Nederlandse instellingen. Op basis van deze informatie wilde THTC de getroffen instellingen notificeren. Juridisch bleek dit een uitdaging, omdat het NCSC een derde partij betreft en daar niet zomaar informatie mee kon worden gedeeld. In hoofdstuk 6 wordt uitgebreider ingegaan op de problemen rondom informatiedeling en slachtoffernotificatie die ook speelden in deze zaak. Er zijn in dit onderzoek door THTC geen verdachten geïdentificeerd of vervolgd.

4.1.4 Drugshandel op het darkweb

Van een private partij en een buitenlandse opsporingsdienst kwam een tip binnen over een Nederlandse server waar mogelijk een grootschalige illegale marktplaats van het darkweb op werd gehost. Op deze marktplaats werden illegale goederen zoals verdovende middelen verhandeld. Het doel van het onderzoek was initieel om de marktplaats te lokaliseren en offline te halen, maar tijdens het onderzoek bleek dat de marktplaats naar een buitenlandse server was verhuisd. Vervolgens bleek

---

[79] De *malware* maakte gebruik van een reverse shell die zichzelf peristent maakte (zich nestelde in de computer) door zich voor te doen als een service van Windows die opereert op de achtergrond

[80] Deze *keylogger* leidde gegevens weg naar het computersysteem van de aanvaller. Daarnaast zorgde de *keylogger* ervoor dat alle toetsaanslagen werden opgeslagen naar een bestand en werden weggeleid naar hetzelfde IP-adres.

men wel de identiteit van de beheerders en enkele sleutels te kunnen achterhalen. De opzet van het onderzoek is toen herzien en er is besloten om de markplaats over te nemen, om meer inzicht te krijgen in de werking van dit type marktplaats en mogelijkheden te zoeken om dit blijvend te verstoren. Samen met de FBI en verschillende Europese opsporingsdiensten is door THTC en een ander Nederlands politieteam de marktplaats op het darkweb overgenomen en voor twee weken in beheer gehouden door de Nederlandse opsporingsdiensten. De overname heeft geleid tot veel informatie over de werking van een darknet marktplaats. Verder heeft de interventie geleid tot verschillende veroordelingen van en *knock and talk* acties bij Nederlandse afnemers van de goederen. De twee Duitse hoofdverdachten, de beheerders van de marktplaats, zijn gearresteerd.

4.1.5 Cryptocommunicatie

Bij de politie is al langer bekend dat veel communicatie binnen de georganiseerde criminaliteit versleuteld plaatsvindt via PGP (Pretty Good Privacy) telefoons. Vanwege de populariteit van deze PGP-telefoons onder criminelen is besloten een Nederlandse aanbieder van cryptocommunicatiediensten nader te onderzoeken. Het bedrijf leverde aangepaste telefoons waarmee alleen versleuteld informatie kon worden verstuurd en waarmee niet kon worden gebeld. Volgens de politie is het aannemelijk dat de verdachte ervan op de hoogte was dat hij de telefoons aan criminelen verkocht. Daarmee ontving hij dus crimineel geld, waardoor hij werd verdacht van witwaspraktijken. Het opsporingsonderzoek had twee doelstellingen. Ten eerste werd onderzocht of de aanbieder van de cryptotelefoons (zowel het bedrijf als de persoon) strafrechtelijk aansprakelijk kon worden gesteld. Dit deel is strikt genomen geen cybercrimeonderzoek. Daarnaast werd gepoogd de versleutelde berichten inzichtelijk te maken, die mogelijk ook waardevolle informatie konden opleveren voor andere opsporingsonderzoeken naar georganiseerde criminaliteit. Tijdens het onderzoek is THTC erin geslaagd om toegang te krijgen tot de versleutelde berichten. De server van het bedrijf met de versleutelde berichten stond in Canada en deze is met toestemming van een Canadese rechter door de Nederlandse autoriteiten in beslag genomen. De informatie die uit de ontsleutelde berichten naar voren is gekomen, is voor meerdere (inter)nationale opsporingsonderzoeken naar zware criminaliteit gebruikt.

4.1.6 Ransomware

Een Nederlandse medewerker van een telecombedrijf meldt na een tip van een buitenlandse burger bij de politie dat hun server is misbruikt om op grote schaal *ransomware* te verspreiden. Op de betreffende server bleken van honderden slachtoffers gegevens aanwezig. Ook waren op de server codes aanwezig die konden worden gebruikt voor de ontsleuteling van bestanden. Het telecombedrijf heeft naar aanleiding van deze bevinding een link naar een back-up van de webserver overhandigd aan THTC, waarop de gegevens stonden. In deze zaak betreffende *ransomware* heeft geanalyseerd. Zij onderzochten de werkwijze van de criminelen en wijze van versleuteling van de data zodat een *decryptor* kon worden ontwikkeld. Om dit te kunnen doen is de technische data gedeeld met het bedrijf.[81] Uit het opsporingsonderzoek zijn de namen van twee Nederlandse verdachten naar voren gekomen, wat heeft geleid tot aanhoudingen en veroordelingen. De bevin-

[81] Inhoud van bestanden, met daarin bijvoorbeeld mogelijk persoonsgegevens, wordt niet gedeeld met private partijen.

dingen uit dit opsporingsonderzoek hebben tevens aan de wieg gestaan van het publiek-private samenwerkingsverband NoMoreRansom (zie hoofdstuk 5).

4.1.7 Malware via phishing

THTC krijgt van een medewerker van een antivirusbedrijf op informele wijze melding van een bankfraudezaak. In de zaak ging het om buitenlandse financiële instellingen die geïnfecteerd werden met *malware* door middel van *spearphishing*[82] emails. De *malware* zorgde ervoor dat het hele netwerk van een bank werd overgenomen. Vervolgens werden de financiële stromen en werkwijze van de bank grondig bestudeerd, om vervolgens de meest effectieve en efficiënte *cash-out* te bepalen. Dit kon bestaan uit het manipuleren van pinautomaten, maar ook het manipuleren van SWIFT-transacties, of het manipuleren van de databases van de bank om geld over te maken op rekeningen van de (geldezels van) de criminelen. Verschillende banken in Oost-Europa waren ten tijde van het openen van het onderzoek via dezelfde modus operandi slachtoffer geworden. De totale schade is opgelopen tot ongeveer een miljard euro. Volgens de melding zou de uitvoering van deze fraude via twee Nederlandse servers hebben gelopen. Naar aanleiding van de melding heeft THTC een strafrechtelijk onderzoek gestart naar een onbekend persoon. In samenwerking met het antivirusbedrijf is ook de modus operandi die is gebruikt bij het verspreiden van deze *malware* in kaart gebracht. De mogelijkheid bestond dat de *malware* ook bij andere Europese banken zou binnenkomen. Deze dreiging, gecombineerd met het besef dat het opsporen van de dader of dadergroep nog een lange tijd kon duren, heeft ertoe geleid dat er is overgegaan tot tegenhoudmaatregelen. De resultaten van het onderzoek van THTC en het antivirusbedrijf zijn internationaal gedeeld met financiële instellingen, met als doel dat deze partijen zich tegen de *malware* en de criminele werkwijze konden beschermen. Bovendien is een dreigingsrapport over deze cybercriminele aanval gepubliceerd.

4.1.8 Phishing

Uit naam van meerdere banken werden *phishingmails* verstuurd die gingen over het aanvragen van een nieuwe betaalpas. Na het klikken op een link in de mail werden slachtoffers naar een pagina geleid waar hen werd gevraagd om bankgegevens in te vullen. Ook werden slachtoffers telefonisch benaderd door één van de verdachten die zich voordeed als medewerker van de bank. De ingevulde bankgegevens werden gebruikt om een nieuwe betaalpas aan te vragen die vervolgens werd onderschept. Bij het innen van het geld werd gebruikgemaakt van meerdere geldezels. Door aangifte van een slachtoffer in één van de eenheden is een onderzoek gestart door één van de regionale cybercrimeteams. De zaak had een sterke online component in het opzetten en het versturen van de mails en het overboeken van geld. Daarnaast was er sprake van 'offline' delicten zoals fysieke diefstallen van bankpassen uit brievenbussen en het opnemen van geld bij betaalautomaten. Tijdens dit fenomeenonderzoek kon een zo volledig mogelijke beeld van de modus operandi bij het fenomeen *phishing* worden gekregen. Daarnaast is een crimineel samenwerkingsverband aangetoond en zijn de twee hoofdverdachten vervolgd.

[82] Spearphishing is een vorm van oplichting via e-mail of andere elektronische communicatie die specifiek is gericht op een individu, organisatie of bedrijf, dit in tegenstelling tot phishing, waarbij massa's e-mails tegelijk worden verzonden in de hoop dat iemand toehapt. Spearphishing is vaak gericht op het stelen van gegevens, maar de methode kan ook gebruikt worden om malware op gegevensdragers van de beoogde gebruiker te installeren.

Tabel 4.1 Strafbare feiten waarop de opsporingsonderzoeken zich richtten

	Wetsartikel	Delict	In hoe veel onderzoeken (n=8)
Computergestuurde delicten	138ab Sr	Computervredebreuk	6
	350a Sr, 350b Sr, 350d Sr	Computergegevens onbruikbaar/ontoegankelijk maken en voorbereidingshandelingen (o.a. *ransomware*)	4
	161sexies Sr	Computersystemen vernielen, beschadigen, onbruikbaar maken, verstoren	4
	139c Sr, 139d Sr	Aftappen en overnemen van gegevens (o.a. *malware*)	3
	138b Sr	Spam of bombing	3
	138c Sr	Opzettelijk wederrechtelijk overnemen niet-openbare gegevens	1
Computergerelateerde delicten	420bis Sr, 420ter Sr	(gewoonte)witwassen	4
	225 Sr	Valsheid in geschrifte	3
	310 Sr, 311 Sr en 312 Sr	Diefstal	3
	326 Sr	Oplichting	2
	231b Sr	Identiteitsfraude	1
Overig	140 Sr	Deelneming criminele organisatie	2
	45 Sr	Poging tot misdrijf	2
	317 Sr en 318 Sr	Afpersing of afdreiging	2
	416 Sr en 417 Sr	Heling	1
	10a opiumwet	Strafbare voorbereidingshandelingen	1

4.2 De start van een opsporingsonderzoek

Nederland heeft een snelle, stabiele en betrouwbare digitale infrastructuur, waar zowel nationaal als internationaal veelvuldig gebruik van wordt gemaakt. Die sleutelpositie geeft economische kansen, maar schept ook verplichtingen. Nederlandse *hosters* worden vaak gebruikt of misbruikt door criminelen om aanvallen uit te voeren of gestolen data tijdelijk te stallen. Dit biedt kansen voor de opsporing en voor het veiligstellen van informatie. De politie kan op twee manieren kennis nemen van een (vermoedelijk) delict. De eerste manier is door een melding of aangifte van een burger, de overheid of een bedrijf. De tweede manier is door zelfstandig onderzoek te doen en informatie te verzamelen. De eerste categorie zaken worden brengzaken genoemd, de tweede categorie haalzaken (De Poot et al., 2004).

In tegenstelling tot de regionale cybercrimeteams werkt THTC vrijwel niet aangifte gestuurd. Hoewel het in theorie mogelijk is dat een THTC-onderzoek start op basis van een aangifte, laat de praktijk zien dat van *hightech crime* zelden aangifte wordt gedaan. Ondanks dat het geen aandachtspunt was van ons onderzoek werd het lage aantal aangiftes van *hightech crime* toch regelmatig benoemd in de interviews wanneer het ging over hoe zaken onder de aandacht van de politie komen. Redenen die werden genoemd voor de lage aangiftebereidheid zijn onder meer angst voor imagoschade bij bedrijven wanneer openbaar wordt dat ze slachtoffer zijn geworden

van een cyberaanval en een mogelijk gebrek aan vertrouwen om het probleem via de juridische weg op te lossen. Wanneer een bedrijf bijvoorbeeld slachtoffer is van een *ransomware*-aanval waardoor bedrijfsprocessen stil komen te liggen kan het voordeliger zijn het losgeld te betalen en snel weer operationeel te zijn dan de resultaten van een politieonderzoek af te wachten en in die tijd niets te kunnen doen. Tot slot geldt specifiek voor *facilitators* dat er vaak niet één duidelijke direct gedupeerde is waardoor er tegen deze dienstverleners weinig aangifte wordt gedaan.

Dat de aangiftebereidheid van cyberdelicten laag is blijkt ook al verschillende jaren uit diverse onderzoeken (zie bijvoorbeeld Beerthuizen, Sipma & Van der Laan, 2020; Domenie et al., 2012,). Recent onderzoek van Van de Weijer et al., (2020) onder burgers en MKB-bedrijven laat zien dat met name delicten die gericht zijn op ICT-systemen, zoals *malware*, *ransomware*, *hacken* en DDoS-aanvallen, zelden worden aangegeven. Dit is ook het soort delicten waar THTC voornamelijk onderzoek naar doet.

Het beeld dat hierboven is beschreven is ook terug te zien in de dossiers die zijn bestudeerd voor dit onderzoek. Het enige onderzoek dat is gestart naar aanleiding van een aangifte is de *phishing* zaak bij een regionale eenheid. Van de zeven bestudeerde THTC-onderzoeken zijn zes onderzoeken gestart naar aanleiding van een tip van een private partij en/of buitenlandse politiedienst. Dit sluit ook aan bij bevindingen uit eerder onderzoek van Odinot et. al. (2017), waarin geen enkele beschreven zaak werd gestart op basis van aangifte van een burger, maar zaken werden gestart op basis van meldingen van bedrijven, tips uit de online community en tips van buitenlandse opsporingsdiensten. Aangiftes geven dus een beperkt beeld van wat er speelt op het gebied van cybercriminaliteit. Daarnaast speelt nog mee dat digitale informatie vluchtig is en dat op het moment dat aangifte wordt gedaan men soms al te laat is om de informatie nog te kunnen achterhalen.

Veel zaken worden daarom gestart op grond van informatie die wordt verzameld uit openbare bronnen of door tips van een private partij of buitenlandse opsporingsdienst. Om hun informatiepositie te vergroten monitort THTC de actuele ontwikkelingen binnen de cybercriminaliteit. Dit wordt bijvoorbeeld gedaan door het bundelen van data uit eerdere opsporingsonderzoeken, middels het CSAE-raamwerk, contacten met andere nationale opsporingsdiensten en internationale politiediensten, maar ook door kennis te nemen van de verschillende dreigingsrapporten die periodiek verschijnen en het doen van strafrechtelijk onderzoek naar gesloten cybercriminele fora. Deze informatie wordt verzameld en mede op basis daarvan wordt een analyse gemaakt van wat er speelt en waar op in moet worden gezet door de opsporingsdiensten. Daarnaast wordt gebruikgemaakt van rapporten van beveiligingsbedrijven en Europol om een beeld te krijgen wat voor trends zich voordoen binnen de cybercriminaliteit.[83] Deze informatie kan betrekking hebben op delicttypen, *malware*typen en criminele groeperingen met een specifieke modus operandi.

Dat men het bij de aanpak van cybercriminaliteit belangrijk vindt om op een slimme manier gebruik te maken van informatie die voorhanden is en die informatie met andere partijen te delen wordt ook geïllustreerd door de volgende uitspraak van een politiemedewerker:

[83] Europol (2019); Kaspersky (2019), *Advanced threat predictions for 2020*.

'De opsporing is wat wij noemen intelligence led, dus gebaseerd op informatie die intelligence wordt initieer je onderzoeken. Een normaal recherche onderzoek is er wordt een moord gepleegd en de plaats delict wordt afgezet en de rechercheurs komen om te kijken wat er gebeurd is. In cyber is dat niet meer het geval, je kijkt naar wat er voor informatie voor handen is op het gebied van cybercrime en je probeert daar dreigingen uit te halen en die dreigingen die probeer je vervolgens te counteren met behulp van opsporingsonderzoek. (…) Een aantal grote onderzoeken die hier publiek zijn geworden zijn gebaseerd op een aanwijzing die komt vanuit een private partner.'

Zowel binnen THTC als binnen de regionale eenheden wordt ingezet op samenwerking met private partijen om de informatiepositie van beide partijen te vergroten en cybercriminaliteit effectiever aan te kunnen pakken. Hierbij kan gedacht worden aan cybersecurity bedrijven, telecombedrijven en de bancaire sector. Deze samenwerkingen zijn zowel op individuele basis (bijvoorbeeld door persoonlijke contacten met medewerkers in het bedrijfsleven), als meer structureel via formele publiek-private samenwerkingsverbanden. Op deze publiek-private samenwerkingsverbanden wordt in hoofdstuk 5 nader op ingegaan.

4.2.1 Keuzes voor het wel of niet oppakken van een zaak

Omdat zich meer zaken aandienen dan opgepakt kunnen worden, moeten keuzes worden gemaakt over welke zaken opgepakt worden door de opsporingsdiensten. Of een zaak wordt opgepakt hangt zowel af van de beleidsprioriteiten die zijn gesteld als van de ernst van een zaak. De beleidsprioriteiten geven zicht op wat de kernthema's van politie en OM zouden moeten zijn. Daarnaast doen zich zaken voor die een dusdanig probleem vormen voor de samenleving dat ze los van de beleidsprioriteiten opgepakt moeten worden. Daarbij kan gekeken worden naar de financiële impact, de persoonlijke impact, de maatschappelijke impact, of de internationale impact van een cyberdelict. De ernst kan ook zitten in de schaalgrootte van een zaak, iets wat bij cybercriminaliteit snel het geval kan zijn.

Een onderzoek kan ook uit strategisch oogpunt worden gestart, bijvoorbeeld vanuit een wens om meer kennis te verzamelen over een cybercrimineel fenomeen of een bepaalde criminele werkwijze met als doel die kennis te kunnen benutten bij het opsporen en tegenhouden van deze vorm van criminaliteit. Zoals ook geïllustreerd door een politiemedewerker in onderstaand voorbeeld:

'Dat was een MO die nog redelijk nieuw was, en we wilden die MO gewoon eens uitlopen zeg maar aan de hand van de servers. Waarom? Om te kijken van nou is dit een nieuwe innovatieve vorm waar we als team iets mee moeten? En als we meer over die MO weten, kunnen we daar iets mee naar anderen die daar baat bij kunnen hebben? Dus daarom hebben we die servers veiliggesteld. Dat is de aanleiding van het onderzoek.'

Door onderzoek te doen naar fenomenen of criminele werkwijzen kan er beter zicht op worden verkregen en kan een inschatting worden gemaakt van de potentiele grootte van de dreiging of schade en is de kans groter dat bijvoorbeeld een aanbieder van een criminele dienst kan worden geïdentificeerd. In de interviews is door politiemedewerkers diverse malen benoemd dat deze manier van werken soms wel omschakelen is voor de rechercheurs die een tactische achtergrond hebben, zoals ook blijkt uit onderstaand citaat van een politiemedewerker:

'Je merkte wel dat bij de tactische mensen die wat later aansloten dat dat wel vervelend was. Omdat die gewend waren om meteen achter een verdachte aan te gaan en die vonden het eigenlijk te lang duren, (…). Terwijl wij zoiets hadden, laten we nou eerst het fenomeen eens onderzoeken en je ziet daar wel het probleem ontstaan in de opsporing en fenomeenonderzoek doen omdat dat heel erg afwijkt van de traditionele manier hoe onderzoeken worden uitgevoerd.'

Zoals al werd beschreven in hoofdstuk 3 is het de bedoeling dat THTC de meest complexe zaken uitvoert en de kennis die zij opdoen overdragen aan de cybercrimeteams in de eenheden. Het gaat daarbij niet strikt om cybercrime zaken in de enge zin van het woord, zoals bijvoorbeeld de zaak over cryptocommunicatie die is beschreven in paragraaf 4.1.5. Daarbij was een reden om de zaak op te pakken het feit dat er in de georganiseerde criminaliteit veel gebruik werd gemaakt van cryptotelefoons en dat dit de reguliere opsporingsonderzoeken belemmerde. De techniek achter de telefoons was echter zo complex dat het onderzoek bij THTC terecht kwam. Hoewel in de interviews een aantal keer benoemd is dat het soms wat lastig uit te leggen is dat THTC ook dit soort zaken oppakt, zelfs binnen de eigen gelederen, is er wel een bredere overtuiging dat het juist belangrijk is om ook dit soort zaken te doen, omdat de impact hiervan wel degelijk groot is.

Sturing

De bovenstaande overwegingen om zaken wel of niet op te pakken lijken allemaal een rol te spelen bij de beslissing om een individuele zaak op te pakken. Er is beleid dat er specifieke aandachtsgebieden of beleidsprioriteiten zijn waar THTC en de cybercrimeteams zich op richten, maar de keus voor het wel of niet oppakken van een individuele zaak door THTC is uiteindelijk sterk afhankelijk van de betrokken officier van justitie.

Er lijkt dus sprake te zijn van vrij autonome besluitvorming, zonder gekaderde sturing en weging van zaken zoals gebeurt bij opsporingsonderzoeken in de eenheden. Die betrekkelijke autonomie is mogelijk te verklaren door het feit dat THTC vergeleken met de regionale eenheden een team met een specialistische focus is, met een gespecialiseerde officier van justitie die een bepaald type criminaliteit als aandachtsgebied heeft. Dat er ruimte is voor autonomie in de besluitvorming over de aanpak van zaken wil niet zeggen dat THTC volledig autonoom opereert. Ook THTC heeft te maken met het OM als gezag, en stemt in steeds grotere mate af met het LOCO en de eenheden. Het voordeel van de betrekkelijk autonome besluitvorming is dat de lijnen tussen de officier van justitie en THTC kort zijn, THTC snel kan schakelen, flexibel is en goed het momentum kan pakken bij een onderzoek. Wat van belang is bij vluchtige data, zoals ook wordt geïllustreerd door onderstaande citaat van een politiemedewerker:

'Daarom vind ik het wel superbelangrijk in een onderzoek dat je gewoon agile blijft, wendbaar blijft, want je kunt er wel een hele studie van maken of je er überhaupt aan moet beginnen. Zo gaat het namelijk vaak bij recherche-onderzoeken. Project pre-weeg, krijg je eerst een projectvoorstel, krijg je een hele cyclus van dingen. Nou dan ben je maanden verder, terwijl die data staat nu hier, maar morgen niet meer.'

Een nadeel hiervan is echter dat er relatief veel ruimte lijkt voor individuele keuzes en wij (daarmee) vrij beperkt zicht hebben gekregen op de afwegingen en besluitvormingsprocessen die aan de gemaakte keuzes ten grondslag lagen. Hoewel vastere beoordelingskaders misschien wenselijk zouden zijn als houvast bij de

besluitvorming en om die te documenteren, blijkt uit eerder onderzoek ook dat al te uitgebreide wegingsprocedures niet per se zinvol zijn. Ze hebben niet altijd de beoogde meerwaarde om de meest kansrijke onderzoeken te selecteren (Bokhorst, Van der Steeg & De Poot, 2011). Voor de cybercrimeteams in de eenheden speelt het LOCO een coördinerende rol bij het wegen en verdelen van zaken.

Overdracht aan de operationele teams bij THTC
Zoals eerder beschreven bestaat THTC uit drie operationele teams en een voor-onderzoeksteam. Bij het vooronderzoeksteam wordt actief op zoek gegaan naar nieuwe zaken en worden onderzoeken 'opgewerkt' tot ze kunnen worden overgedragen aan de operationele teams. Bij het 'opwerken' van de onderzoeken door het vooronderzoeksteam wordt van hetzelfde wettelijk kader gebruikgemaakt als in andere strafrechtelijke onderzoeken.

Niet alle onderzoeken die het vooronderzoeksteam start leiden ook daadwerkelijk tot opsporingsonderzoeken. Vaak is bij de start van een onderzoek nog niet duidelijk wat er precies aan de hand is en hoe kansrijk een opsporingsonderzoek is. Dat wordt meestal pas gaandeweg bekend. Bij veel van de onderzochte zaken gold dat er sprake was van Nederlandse servers en begon het onderzoek met het vorderen van gegevens en achterhalen welke informatie precies op deze servers staat. Afhankelijk van wat daarop wordt aangetroffen breekt er een nieuw beslismoment aan. Namelijk of het opsporingsonderzoek vervolg krijgt en zo ja wat de richting van het onderzoek wordt. Als de inschatting wordt gemaakt dat een strafrechtelijk onderzoek kansrijk is wordt deze doorgegeven aan één van de operationele teams die het opsporingsonderzoek verrichten. Het vooronderzoek kan maanden of jaren duren, maar soms kan een zaak ook bijna direct worden doorgezet naar een operationeel team. In de interviews komt naar voren dat de overdracht niet altijd vlekkeloos verloopt. Soms moet een operationeel team nog overtuigd worden van het nut van een onderzoek, of hebben zij bijvoorbeeld eigen ideeën over de aanpak van een zaak, zoals beschreven door een politiemedewerker:

> *'Je merkte dat je best wel, we hebben best wel ons best moeten doen om dat hier te verkopen dat we dat hier moesten oppakken die zaak. Je hoorde echt letterlijk mensen in het operationele team zeggen van ja er zijn geen Nederlandse daders of Nederlandse slachtoffers, waarom moeten we dit doen? (…) Sindsdien hanteren we eigenlijk ook veel duidelijker het gegeven van: om een zaak op te pakken moet die het liefst wel iets van een Nederlandse component hebben. Dus we kijken nu eigenlijk heel grofweg, is er sprake van een Nederlandse dader, slachtoffer of infrastructuur? Infrastructuur wordt ook echt als een kenmerk gezien om een onderzoek te starten.'*

4.2.2 Onderzoeksdoelen

Bij de start van een opsporingsonderzoek wordt een plan van aanpak opgesteld waarin onder meer de doelstelling(en) van het onderzoek staan beschreven.
Een opsporingsonderzoek wordt officieel alleen gestart als er opsporingsindicatie is – sporen waarmee mogelijke verdachten kunnen worden opgespoord en vervolgd – omdat alleen dan opsporingsbevoegdheden mogen worden ingezet. Dat is vaak ook het primaire onderzoeksdoel, maar bij lang niet alle onderzoeken wordt bij een verdachte uitgekomen. Soms is dat al snel bij aanvang van een onderzoek duidelijk en dan wordt nagedacht of er met de verkregen informatie ook andere doelen bereikt kunnen worden. Een voorbeeld hiervan is het zicht krijgen op een bepaald criminaliteitsfenomeen, om die kennis in volgende opsporingsonderzoeken te kunnen gebrui-

ken of om tegenhoudmaatregelen in te zetten. Dat er naast het primaire doel (zicht krijgen op een verdachte) ook andere doelen in een onderzoek zijn, wordt ook beschreven door een politiemedewerker:

> *'Ja. Nou hij is binnengekomen met een hele brede doelstelling. Je hebt primaire doelstelling en secundaire doelstelling, waarbij de primaire doelstelling is om te kijken of er een verdenking geschreven kon worden […]. De secundaire doelstelling, de pot met goud, is wat is er mogelijk met [die techniek] en de ultieme doelstelling was wel al vrij snel van zouden we dat inzichtelijk kunnen krijgen. Dus zouden we kunnen zien wat er op die apparaten gebeurt onderling en meer vat kunnen krijgen op de communicatie van criminelen. Maar die eerste doelstelling om die 27 Sv te schrijven is cruciaal. Als je dat niet zou kunnen schrijven, dan heb je geen zaak.'*

Bij de aanpak van cybercriminaliteit hanteert THTC het in hoofdstuk 3 beschreven ballonnenmodel. Elk element uit dat model kan gezien worden als een (sub)doel van een opsporingsonderzoek, waarbij attributie uiteindelijk wel het primaire doel is. Alternatieve onderzoeksdoelen kunnen bijvoorbeeld tegenhoudmaatregelen zijn, zoals het verstoren van de criminele infrastructuur of mitigatie. Deze tegenhoudmaatregelen worden vaak ook al bij de start van een onderzoek opgenomen als subdoel. Bij voorkeur hebben alle elementen uit het model een plek gekregen in een opsporingsonderzoek om zo een zo groot mogelijk effect te sorteren van de ingezette middelen.

Onderzoeksdoelen hoeven niet altijd uitsluitend betrekking te hebben op opsporen en tegenhouden. In één van de bestudeerde dossiers was een van de subdoelstellingen bij de start van het onderzoek ook om een goede relatie op te bouwen met een private partij, in de hoop daar bij vervolgonderzoeken de vruchten van te kunnen plukken met bijvoorbeeld informatie-uitwisseling.

Met de vooraf opgestelde onderzoeksdoelen wordt in de praktijk flexibel omgegaan, ook omdat van tevoren nog niet bekend is welke informatie het onderzoek zal opleveren en dus welke doelen ermee kunnen worden gediend. Met het verkrijgen van extra informatie gedurende het onderzoek kunnen doelen wijzigen. Zo kan blijken dat het niet lukt om een verdachte te identificeren of vervolgen waardoor de nadruk komt te liggen op de inzet van tegenhoudmaatregelen. Ook kan gedurende een onderzoek blijken dat er juist meer mogelijk is dan men van tevoren dacht, zoals bij het onderzoek naar drugshandel op het *darkweb* in paragraaf 4.1.4. Dat onderzoek was er oorspronkelijk primair op gericht om zicht te krijgen op de infrastructuur van de website waar illegale goederen en diensten op werden verhandeld. Uiteindelijk leverde dit onderzoek veel meer op dan men bij aanvang verwachtte, namelijk zicht op verdachten en de mogelijkheid tot overnemen van de website.

4.3 Opsporingsmiddelen en -methoden

De opsporingsactiviteiten in de bestudeerde dossiers bestonden, vooral in de startfase van een onderzoek, voornamelijk uit het vorderen en veiligstellen van servergegevens. Nader onderzoek aan servergegevens geeft inzicht in het soort data dat op een server staat opgeslagen en over het gebruik van een server. Soms werd deze vordering gedaan door een server fysiek veilig te stellen en andere keren door het maken van een forensische kopie of een 'snapshot'. Daarna worden de

digitale sporen nader onderzocht. Deze werkwijze wordt ook beschreven door een officier van justitie:

> *'Is ook hoe we deze hebben aangevlogen, we hebben gezegd, er was dus gestart met […], daarin hebben jullie ook gezien dat er ontzettend veel vorderingen zijn gedaan, in het begin hebben we geprobeerd alles uit te lopen in die zaak. Dat heeft ons uiteindelijk heel veel gebracht toevallig, maar je ziet dat heel veel informatie vergaard is, en dat je echt gelukstreffers moet hebben om bij fouten uit te komen of bij verdachten uit te komen.'*

De inzet van een aantal specifieke bevoegdheden zoals beschreven in hoofdstuk 2 is terug te zien in bijna alle onderzochte dossiers. Zo zijn in bijna alle opsporingsonderzoeken servers veiliggesteld en/of gekopieerd op basis van artikel 125i Sv, werd een diversiteit aan gegevens gevorderd zoals omschreven in de artikelen 126n tot en met 126ng Sv, zijn er internettaps geplaatst zoals beschreven in artikel 126m Sv en werd er onderzoek gedaan naar netwerkverkeer. De informatie die hiermee werd opgedaan, kon worden gebruikt om de verdere richting van een opsporingsonderzoek te bepalen. Ook worden deze gegevens bestudeerd om na te gaan of de verdachte ergens een fout heeft gemaakt die zijn of haar identiteit onthult. Hierbij moet worden opgemerkt dat de inzet van deze middelen niet bij elk onderzoek evenveel informatie opleverde. Naast het verschil in hoeveelheid en typen gegevens die op servers stonden speelt ook de mate van versleuteling van data een rol bij het bepalen van de bruikbaarheid van de gegevens.

De min of meer standaard handelingen die in bijna elk bestudeerd dossier beschreven werden zijn ook mooi op een rij gezet door één van de geïnterviewde politiemedewerkers:

> *'Het standaard riedeltje is dat je gaat voor inhoudsdata en metadata. (…) Inhoudsdata is dus de kopie van de server en eventueel een internettap, dus een full tap waarmee je dus alles ziet wat er in en uit die server gaat. Inclusief inlogpogingen, maar ook welke data wordt geüpload of gedownload of dat soort dingen en meer meta-achtig is bijvoorbeeld alle klantgegevens van degene die de server huurt, die kunnen we vorderen bij het bedrijf. Dus de tenaamstelling, wie heeft dat ding gehuurd? Betalingsgegevens, heeft hij met bitcoins betaald of gewoon met geld. Waar kwam dat geld vandaan? Daar kun je weer op doorrechercheren. En we kunnen ook netflow vorderen en netflow is een soort metatap. Wat ik daar mee bedoel is als je echt een volledige internettap draait dan zie je echt alle bestanden. Dan kun je dat letterlijk weer reproduceren. Bij een metatap, een netflow, zie je alleen van welk IP-adres er wordt ingelogd en wanneer.'*

De meerwaarde die metadata kan hebben voor een opsporingsonderzoek staat ook beschreven in een recent artikel van Henseler en De Poot (2020). Soms is het net zo belangrijk, of belangrijker, om informatie op activiteitniveau te achterhalen zoals met wie er is gecommuniceerd en wat een persoon heeft gedaan, dan alleen de identiteit van een persoon te bepalen.

Verder is in de onderzochte dossiers terug te zien dat wanneer er nog geen verdachte in beeld is, er eigenlijk uitsluitend digitale opsporingsmiddelen worden ingezet. Wanneer er Nederlandse verdachte(n) in beeld komen wordt veelal overgegaan tot een meer tactisch opsporingsonderzoek waarbij ook meer traditionele ('offline') opsporingsmiddelen en -methoden worden ingezet. Zo worden naast

internettaps ook telefoontaps geplaatst die inzicht gaven in contacten die verdachten hadden met elkaar en anderen en zaken die hen bezighielden. Dit wordt vaak gecombineerd met financieel onderzoek om geldstromen in kaart te brengen om aan te tonen dat er sprake is van bijvoorbeeld witwassen, een verdenking die in vier van de bestudeerde dossiers was opgenomen (zie tabel 4.1), en om bij verdachten uit te komen, zoals het geval was in de *phishing*zaak.

Ook is in de vijf bestudeerde dossiers waarin Nederlandse (hoofd)verdachten in beeld kwamen gebruikgemaakt van bevoegdheden die vallen onder het werken onder dekmantel zoals pseudokoop, infiltratie en stelselmatige informatie-inwinning. Deze bevoegdheden werden zowel online als offline, bijvoorbeeld door het plaatsen van een baken op een voertuig van de verdachte, ingezet. Dit is opvallend, gezien het geringe aantal offline zaken waarin deze bijzondere opsporingsbevoegdheden normaliter worden ingezet (zie Kruisbergen, De Jong, & Kouwenberg, 2010), maar sluit wel aan bij bevindingen uit eerder onderzoek naar de opsporing van georganiseerde vormen van cybercriminaliteit door Odinot et al. (2017). Ook in de opsporingsonderzoeken die Odinot et al., (2017) bestudeerden werd gebruikgemaakt van bijzondere opsporingsmiddelen als infiltratie en stelselmatige observatie. De mogelijke verklaring die in dat onderzoek werd gegeven voor de inzet van deze, in Nederland als zwaar beschouwde, middelen was de zwaarte van de misdrijven. Maar misschien speelt ook mee dat bij de aanpak van dit soort nieuwe delicten ook nieuwe gedachtenvorming plaatsvindt over de inzet en zwaarte van al bestaande opsporingsbevoegdheden (zie hierover ook Oerlemans,2018).

Tot slot wordt in aanvulling op de hierboven genoemde bevoegdheden in veel gevallen gebruikgemaakt van open bronnen onderzoek. Over wat deze onderzoeken opleveren is echter weinig terug te vinden in de dossiers die wij hebben bestudeerd. Toch lijkt deze manier van rechercheren veel mogelijkheden te bieden in het digitale tijdperk waarbij verdachten zowel zakelijk als privé veelal gebruikmaken van het Internet en daarmee door bijvoorbeeld bepaald taalgebruik of terugkerende *nicknames* informatie over hun identiteit prijsgeven. Er zijn echter ook kritische besprekingen te vinden in de literatuur die ingaan op de vraag hoe ver de politie mag gaan bij deze wijze van informatie verzamelen. Ook op het internet gelden juridische beperkingen (zie bijvoorbeeld Koops, 2012b).

4.4 Mogelijkheden tot vervolging

Zoals eerder beschreven kan de vervolging van cyberdaders om verschillende redenen lastig zijn. Ten eerste door moeilijkheden om de (hoofd)verdachte(n) te identificeren op het internet. Ten tweede doordat de verdachte zich in het buitenland bevindt. Ook wanneer het wel lukt om de identiteit van een dader te achterhalen kan strafrechtelijke vervolging in Nederland alsnog niet altijd plaatsvinden. Het kan bijvoorbeeld gaan om een dader in een land waar Nederland geen uitleveringsverdrag mee heeft. Zoals één van de geïnterviewden opmerkte ben je als cybercrime-onderzoeker 'onderdeel van de wereldpolitie'. Bij de start van een onderzoek is vaak niet bekend uit welk land een aanval of verdachte komt. Een deel van de opsporingstaak kan dan ook zijn om bijvoorbeeld met de informatie die naar voren komt uit een onderzoek naar de in Nederland gebruikte infrastructuur, een ander land in stelling te brengen om over te kunnen gaan tot vervolging. Dat kan bijvoorbeeld het land zijn waarin de verdachte woont, of een land waarin slachtoffers zijn gemaakt en dat betere kaarten heeft om over te kunnen gaan tot uitlevering of vervolging. Daarbij speelt ook nog het probleem van mogelijk aan

statelijke actoren gelieerde groeperingen en het complexe onderscheid tussen een statelijke actor en een 'gewone' buitenlandse criminele groepering. In het CSBN 2020 staat beschreven dat de grootste dreiging uitgaat van sabotage en spionage door statelijke actoren (NCSC, 2020). Vaak is bij een opsporingsonderzoek echter helemaal niet duidelijk waar dreiging precies vandaan komt. Daarnaast kan de criminele actor een zekere bescherming genieten van de statelijke actor, wat vervolging eveneens lastig maakt.

Een vierde beperking doet zich voor wanneer er juist te veel daders zijn om te kunnen vervolgen. Dit speelt met name wanneer een onderzoek de identiteit van een grote groep afnemers van criminele diensten of goederen oplevert, zoals bij de drugshandel op het *darkweb* in paragraaf 4.1.4 en de afnemers van DDoS-aanvallen in paragraaf 4.1.1. Daarbij speelt ook de vraag of vervolging in al deze gevallen de meest effectieve maatregel is. In een aantal gevallen gaat het om jonge daders die zich niet altijd bewust zijn van de impact of de strafbaarheid van hun acties, ook al werden door hun handelingen veel mensen gedupeerd. In verschillende interviews is genoemd dat het daarom ook belangrijk is om te kijken naar de intentie die een verdachte had en in welke fase van de criminele loopbaan hij of zij zich bevindt en op grond daarvan eventueel gebruik te maken van alternatieve interventies zoals *knock and talk* gesprekken of het cyber recidive preventieprogramma 'Hack_ Right'[84].

De bovengenoemde moeilijkheden bij de opsporing en vervolging spelen met name bij de politie, maar ook het OM wordt geconfronteerd met een aantal specifieke uitdagingen. Zo is in interviews met politiemedewerkers een aantal keer kritiek geuit op de doorlooptijd van zaken. Volgens de geïnterviewden duurt het lang voordat zaken voor de rechter komen. In één geval kwam een zaak te laat op zitting waardoor door de rechter geen gevangenisstraf is opgelegd, vanwege de lange doorlooptijd van de zaak. Ook is er niet altijd begrip bij politiemedewerkers voor de lage straffen, zeker in zaken waarbij veel slachtoffers zijn gemaakt. Een mogelijke oplossing die werd genoemd door een officier van justitie is om voor de rechter beter inzichtelijk te maken om wat voor problematiek het gaat, bijvoorbeeld door middel van een presentatie, omdat alleen een verbale uitleg van de technische handelingen in dit soort zaken te abstract kan zijn. Daarnaast zijn de systemen van het OM niet toegerust op massaal slachtofferschap dat zich bij cybercrimedelicten vaker voordoet. Er is nu een maximum gesteld aan het aantal slachtoffers dat aan een parketnummer kan worden gekoppeld. Als dit aantal wordt overschreden moet een tweede of derde parketnummer worden aangemaakt, wat veel bureaucratische handelingen met zich meebrengt en tijd kost.

4.4.1 Vervolging in de bestudeerde zaken

In dit onderzoek werden in vijf van de acht bestudeerde dossiers verdachten geïdentificeerd. In vier zaken ging het om Nederlandse hoofdverdachten. Drie van deze zaken leidden inmiddels tot veroordelingen; een *ransomeware*zaak, een *phishing*zaak, en een cryptocommunicatiezaak. In de *ransomware*zaak werden taakstraffen en een voorwaardelijke gevangenisstraf opgelegd. In de *phishing*zaak gevangenisstraffen van vijf jaar. Dat is tevens de hoogst opgelegde straf voor dit specifieke delict. In de zaak die betrekking had op cryptocommunicatie is de

[84] Hack_Right is een Nederlands recidive preventieprogramma dat ontwikkeld is door politie en OM, in samenwerking met de Reclassering, HALT en de Raad voor Kinderbescherming. Het richt zich speciaal op jonge hackers tussen de 12 en 23 jaar oud.

hoofdverdachte door de rechtbank veroordeeld tot een gevangenisstraf van 4,5 jaar. In de vierde zaak, over de DDoS-aanvallen, is vanwege de jonge leeftijd van de verdachte een alternatieve afdoening opgelegd en zijn *knock and talk* gesprekken gevoerd met de afnemers van de dienst. In de *darkweb*zaak met twee buitenlandse hoofdverdachten zijn de grootste Nederlandse aanbieders van de illegale producten strafrechtelijk vervolgd. Bij een deel van de overige aanbieders en afnemers heeft de politie *knock and talk* gesprekken ingezet.

Hoewel met name de THTC-onderzoeken niet altijd leiden tot vervolgbare verdachten, kan de strafrechtelijke aanpak voor deze moeilijk vervolgbare delicten wel degelijk van meerwaarde zijn. Een criminele infrastructuur is voor autonome, zelfstandig opererende, groeperingen makkelijk te vervangen. Als interventies zich alleen op de verstoring van de infrastructuur zouden richten heeft dit kortdurend effect, omdat nieuwe infrastructuren ontstaan en activiteiten elders worden voortgezet (zie bijvoorbeeld Ladegaard,2019) over het offline halen van diverse criminele marktplaatsen). Het is daarom juist van belang om een opsporingsonderzoek op te blijven zetten dat er op gericht is om een verdachte te identificeren en vervolgen. Verder leveren de THTC-onderzoeken naar *facilitators* in een aantal gevallen geen hoofdverdachte op, maar wel informatie over andere vormen van criminaliteit die vervolgens in andere opsporingsonderzoeken kon worden gebruikt, of informatie die kon worden gebruikt bij de inzet van tegenhoudmaatregelen.

4.5 Encryptie

Een beperking die in zijn algemeenheid vaak wordt genoemd wanneer het gaat over de aanpak van cybercriminaliteit is de versleuteling van data, of encryptie. In de door ons bestudeerde zaken zien we dat dit geen grote problemen in de onderzoeken heeft opgeleverd. Ofwel men vond een technische oplossing om toch bij de informatie en verdachten te komen of men kwam via een andere weg bij dezelfde informatie uit. Daarnaast kan het ook zo zijn dat voor de zaken die wij hebben bestudeerd encryptie geen belemmerende rol speelde omdat, zoals eerder al beschreven is, voor dit onderzoek met name zaken zijn bestudeerd waar de opsporing in enige mate succesvol is verlopen. Zaken die in een vroeg stadium stukliepen door bijvoorbeeld encryptie hebben misschien de zaakselectie niet gehaald.
Daarnaast kan worden opgemerkt dat in dit onderzoek vooral naar door THTC uitgevoerde opsporingsonderzoeken is gekeken. Bij dit team is hoogwaardige specialistische technische kennis aanwezig. Door het hoge kennisniveau zijn in THTC-onderzoeken soms oplossingen beschikbaar die voor andere teams niet haalbaar zijn. Dat neemt niet weg dat encryptie ook voor THTC als gevolg heeft dat opsporingsonderzoeken complexer zijn en meer tijd of moeite vergen om succesvol te kunnen afronden. Omdat gewone criminaliteit steeds verder digitaliseert, ondersteunt THTC ook steeds vaker ook bij reguliere opsporingsonderzoeken waar een complex technisch vraagstuk speelt. Dit kost echter capaciteit van THTC die ten koste gaat van de eigen onderzoekscapaciteit.

4.6 Tegenhoudmaatregelen in de opsporing

Zoals eerder beschreven in hoofdstuk 3 behoren tegenhoudmaatregelen tot het brede palet aan interventies dat wordt gebruikt bij de aanpak van cybercriminaliteit. In opsporingsonderzoeken is naast opsporing en vervolging van daders (attributie)

waar mogelijk ook aandacht voor preventie, schadebeperking, verstoring en/of slachtoffernotificatie. Deze brede blik is van belang omdat het bij de aanpak van cybercriminaliteit niet alleen relevant is te kijken naar wie de handelingen uitvoert, maar ook wat er gebeurt en hoe de delicten worden uitgevoerd en wie er slachtoffer van worden. Dit was ook terug te zien in de beschreven onderzoeksdoelen van de opsporingsonderzoeken waarbij tegenhoudmaatregelen vaak als subdoel waren opgenomen. In de praktijk worden opsporingsonderzoeken vaak verricht in samenwerking met andere opsporingsdiensten, terwijl tegenhoudmaatregelen vaak plaatsvinden in samenwerking met private partijen.

Op de vraag of tijdens de onderzoeken vooral werd ingezet op opsporing of op tegenhouden antwoordden geïnterviewden eigenlijk zonder uitzondering dat deze processen hand in hand gaan, omdat dat de meest effectieve manier is om cybercriminaliteit aan te pakken. Hierbij werd ook verwezen naar de aanpak bij ondermijning, waar de aanpak heel specifiek is gericht op het criminele verdienmodel. Het samenspel tussen opsporen en tegenhouden is van belang omdat kennis uit de opsporingsonderzoeken gebruikt kan worden om inzicht te krijgen in hoe die modellen in elkaar zitten en om deze kennis up-to-date te houden. Met alleen tegenhoudmaatregelen blijft alleen een klein deel van het proces zichtbaar, terwijl met een aanhouding of inbeslagname het hele proces gereconstrueerd kan worden. Opsporen zorgt niet alleen voor kennisopbouw, maar heeft ook door de afschrikkende werking een verstorend effect, zoals deze officier van justitie illustreert:

> *'Het kan heel verleidelijk zijn om in dat segment vooral te willen verstoren, maar dat heeft ook wel een heel beperkt afschrikwekkend effect. Dus in die zin moet er ook wel voldoende strafrechtelijk worden gehandhaafd om daar normstelling en normhandhaving over aan te houden.'*

Van de elementen uit het ballonnenmodel komen vooral attributie en slachtofferhulp, of slachtoffernotificatie duidelijk naar voren in de dossiers en interviews als thema's in de opsporingsonderzoeken. Slachtoffernotificatie lijkt met name een lastig punt voor de opsporing, hier wordt in paragraaf 6.2.3 nog uitgebreider op ingegaan. Er is geen duidelijke partij die verantwoordelijk is voor slachtoffernotificatie, het delen van informatie om slachtoffers te notificeren kan zowel juridisch als praktisch lastig zijn en de hoeveelheid slachtoffers van bijvoorbeeld een hack is regelmatig zo groot dat de opsporing het notificeren van deze slachtoffers er niet zomaar bij kan doen. Deze problemen zijn niet alleen maar theoretisch. In één van de onderzochte zaken kostte het notificeren van de (Nederlandse) slachtoffers zo veel moeite dat het eigenlijk al bijna te laat was om effectief te zijn.

Juridisch gezien levert het uitvoeren van tegenhoudmaatregelen in de opsporingspraktijk soms discussies op. De politie heeft een bredere taak dan OM, omdat de politie ook preventie in het takenpakket heeft. Op grond van artikel 3 van de Politiewet kan de politie preventiemaatregelen inzetten. Voor tegenhoudmaatregelen zijn soms ook BOB-middelen nodig die een machtiging vereisen van een officier van justitie of rechter-commissaris. Dat kan problematisch zijn wanneer bij de start van een onderzoek al snel duidelijk is dat er geen dader geïdentificeerd kan gaan worden, terwijl de maatschappelijke impact van een cyberdelict wel erg groot is. Bijvoorbeeld bij een grootschalige hack. Een belangrijk doel van het onderzoek wordt dan de inzet van tegenhoudmaatregelen, omdat dit het meest effectieve bestrijdingsmiddel is.

Desalniettemin kunnen de benodigde bevoegdheden niet enkel voor dat doel worden ingezet. Voor de inzet van opsporingsbevoegdheden ten behoeve van verstoring bestaat tot op heden geen wettelijke grondslag. Uit de interviews blijkt dat in de praktijk niet tot problemen te leiden, maar soms wordt hiermee wel een grijs gebied opgezocht.

5 Publiek-private samenwerking

Publiek-Private Samenwerking (PPS) speelt een belangrijke rol bij de aanpak van cybercriminaliteit. In de visie van de Nationaal Cyber Security Agenda (NCSC, 2018) staat PPS aan de basis van de Nederlandse cybersecurity aanpak. Ook binnen de opsporing wordt PPS als een belangrijk middel gezien voor het bestrijden van cybercriminaliteit (Hagenaars & Bonnes, 2020). Dit hoofdstuk gaat verder in op de rol van PPS in de aanpak van cybercriminaliteit.
In paragraaf 5.1 wordt stilgestaan bij drie recente PPS-projecten op het gebied van cybercriminaliteit. Hierin wordt uiteengezet hoe deze samenwerkingsverbanden eruitzien, op welk criminaliteitsfenomeen ze zich richten, en hoe de samenwerking is verlopen. In paragraaf 5.2 wordt aan de hand van interviews die gehouden zijn in dit onderzoek en literatuur beschreven hoe PPS er bij de aanpak van cybercriminaliteit eruitziet. Hierbij wordt ingegaan op de totstandkoming, motieven, succesfactoren en knelpunten.

5.1 Publiek-private samenwerkingsprojecten op het gebied van cybercriminaliteit

In deze paragraaf worden drie voorbeelden besproken van publiek-private samenwerkingsverbanden op het gebied van cybercriminaliteit: de Brede Coalitie ter verstoring van de Tech Support Scam in Nederland, de Anti-DDoS Coalitie en NoMoreRansom. Deze projecten zijn door respondenten aangewezen als vooraanstaande samenwerkingsverbanden op het gebied van cybercriminaliteit in de afgelopen jaren. In de deelparagrafen wordt eerst ingegaan op het criminaliteitsfenomeen waar de samenwerking zich op richt en vervolgens wordt de samenwerking inhoudelijk beschreven.

5.1.1 Brede Coalitie ter verstoring van de Tech Support Scam

In 2018 is een samenwerkingsverband opgezet tussen veertien publieke en private partijen om het fenomeen van helpdeskfraude tegen te gaan. Helpdeskfraude (ook wel bekend als de *Tech Support Scam* of de *Microsoft scam*) is een vorm van oplichting waarbij een slachtoffer contact legt met een zogenoemde medewerker van een groot bedrijf.[85] De dader probeert door middel van *social engineering*[86] het slachtoffer ervan te overtuigen dat hij of zij een medewerker van het bedrijf is. Vervolgens laat de dader aan het slachtoffer weten dat er problemen gevonden zijn op zijn of haar computer en dat deze verholpen moeten worden. Door het slachtoffer naar de *event logger*[87] te dirigeren wordt de indruk gewekt dat er iets mis is met de computer. In werkelijkheid is er niks bijzonders aan de hand en zijn deze 'foutmeldingen' aanwezig bij de meeste computers.

---

[85] In het verleden veelal Microsoft, maar er bestaan ook nieuwere varianten met andere bedrijven zoals Google en Ziggo.

[86] *Social engineering* is het misbruiken van menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen, hebzucht, angst of onwetendheid (veiligbankieren.nl). Door op deze wijze op mensen in te spelen, worden zij verleid tot het afgeven van vertrouwelijke informatie waar vervolgens misbruik van kan worden gemaakt.

[87] Een event logger is een onderdeel van het Windows besturingssysteem waarin gebeurtenissen, berichten, waarschuwingen en foutmeldingen worden weergegeven. Deze foutmeldingen zijn aanwezig bij de meeste computers en betreffen het normale kenmerken van een computer.

In veel gevallen wordt het slachtoffer vervolgens gevraagd om software te installeren waarmee de medewerker de controle over de computer over kan nemen zodat de vermeende problemen worden opgelost. Vervolgens wordt aan het slachtoffer gevraagd om te betalen voor de geboden hulp of wordt verteld dat een bepaalde licentie van de beveiligingssoftware is verlopen. Daarnaast komt het voor dat de daders het slachtoffer inloginformatie of codes van internetbankieren afhandig maken, of tijdens de betaling via internetbankieren het bedrag ongezien verhogen (Politie.nl, z.d.a.).

Volgens de politie zijn er drie vaak voorkomende manieren waarop dader en slachtoffer met elkaar in contact komen zijn: (1) Het slachtoffer wordt opgebeld door de medewerker (*cold calling*), (2) het slachtoffer heeft een helpdesknummer van een bedrijf gezocht en is daarbij op een nagemaakte site met een telefoonnummer van de fraudeurs terechtgekomen en (3) het slachtoffer krijgt een pop-up melding in het beeldscherm te zien met de mededeling dat er een virus is aangetroffen. Op deze pop-upmelding staat een telefoonnummer dat kan worden gebeld.

De laatste jaren is helpdeskfraude verder ontwikkeld, zowel op technisch als niet-technisch gebied. Zo wordt vaker gebruikgemaakt van nagebootste websites van bedrijven, waarop het telefoonnummer van de oplichters staat. Deze nagemaakte websites worden zo geprogrammeerd dat zij hoog in de resultaten van de zoekmachines terechtkomen. Daarnaast meldt het OM dat de kwaliteit van *social engineering* is verbeterd. In het verleden kwam het voor dat daders gebrekkig Engels spraken, maar daar is nu steeds minder sprake van (OM.nl, 2020; Borwell, et al., 2020).

In 2020 was de totale gemelde schade van de helpdeskfraude bij de politie 2,6 miljoen euro (Borwell, et al., 2020). Dit betreft jaarlijks ongeveer 2.000 slachtoffers, waarvan 70% ouder is dan 50 jaar. In de periode 2015-2018 is de helpdeskfraude volgens politieregistraties tevens het meest voorkomende type cybercrimedelict (Borwell & Bos-Riepma, 2018). In totaal gaat het om 3.526 geregistreerde gevallen, wat neerkomt op 21% van het totale aantal geregistreerde cyberdelicten. Omdat de aangiftebereidheid van cyberdelicten laag is (zie hierover ook paragraaf 4.1) is de totale omvang van helpdeskfraude waarschijnlijk groter.

De opsporing van helpdeskfraude is moeilijk doordat de daders niet of nauwelijks vanuit Nederland opereren. Uit onze interviews en uit openbare berichten van de politie komt naar voren dat de daders voornamelijk afkomstig zijn uit India.[88] Dit betekent dat een samenwerking met de Indiase autoriteiten nodig is om succesvol tot vervolging over te kunnen gaan. Deze samenwerking verloopt echter om verschillende redenen moeizaam. Zo komen slachtoffers meestal niet uit India en hebben de Indiase autoriteiten weinig middelen en andere prioriteiten[89] (Borwell & Bos-Riepma, 2018). Volgens een van de geïnterviewden kan ook corruptie binnen de Indiase autoriteiten een complicerende factor vormen.

[88] https://www.politie.nl/themas/helpdeskfraude.html

[89] Desalniettemin zijn in India meerdere arrestaties verricht na meldingen van Microsoft. Microsoft heeft onder de naam Digital Crime Unit (DCU) een eigen team dat onderzoek doet naar cybercriminaliteit, waaronder de helpdeskfraude. De DCU poogt de helpdeskfraude aan te pakken door systematisch alle meldingen van helpdeskfraude te verzamelen en netwerken op te bouwen in verschillende landen. Dit heeft ertoe geleid dat dit misdrijf ook strafrechtelijk kan worden aangepakt. Zo zijn er in 2017 en 2018 invallen gedaan in 28 callcenters, waarbij in totaal minstens 39 daders zijn aangehouden (Gregoire, 2017, 2018).

Samenwerking
Omdat helpdeskfraude vaak voorkomt, terwijl dit misdrijf moeilijk kan worden opgespoord is besloten tot een niet-strafrechtelijke aanpak van dit fenomeen. Hiertoe is op initiatief van het Openbaar Ministerie, Arrondissementsparket Rotterdam, samen met de Nationale Politie en de Autoriteit Consument en Markt (ACM) een samenwerking gezocht met elf private partijen uit de telecom, software en financiële sector met als doel gezamenlijk verschillende soorten maatregelen te treffen om het slachtofferschap van de helpdeskfraude tegen te gaan en uit te bannen.

Tijdens de samenwerking is gepoogd om het volledige crime script van de helpdeskfraude via de *book of crime*[90] methodiek in kaart te brengen. Vervolgens is per stap onderzocht of er passende barrières en verstoringsmaatregelen konden worden bedacht met het doel:[91]

- onrechtmatig gebruik van Nederlandse telefoonnummers door *scammers* te verstoren;
- technologische detectie van frauduleuze situaties te verbeteren;
- inningsmogelijkheden van scammers te verstoren;
- de scam te verstoren door bancaire processen aan te passen aan de modus operandi van de scammers.

Inmiddels zijn enkele functionaliteiten op het gebied van software die veelvuldig werden misbruikt verwijderd. Een voorbeeld hiervan is dat TeamViewer, een bedrijf achter een veelgebruikt *remote access tool,* de gratis versie van hun software heeft ingeperkt, door de functionaliteiten te blokkeren wanneer er een verbinding werd opgezet vanuit India richting een Europees land. Verder wordt er aandachtiger gekeken naar verdachte belpatronen voor fraudedetectie en worden frauduleuze inbelnummers uit de lucht gehaald. Een ander voorbeeld is dat de mogelijkheid wordt verkend voor het laten verschijnen van *red flags*, bijvoorbeeld wanneer men online bankiert terwijl de besturing van de computer is overgenomen. Deze *red flags* zouden de partijen die betrokken zijn in het betalingsproces in specifieke gevallen alerter moeten maken voor mogelijke oplichting.

Naast verstoring wordt ook ingezet op preventieve maatregelen. Afgesproken is dat ieder jaar minstens één publieke partij en minstens één private partij een *awareness* campagne zal verzorgen om de bewustwording van het bestaan en de handelswijze van de helpdeskfraude te vergroten. Andere partijen zullen bijdragen aan de campagne door het bereik verder te vergroten. Via Facebook en de NPO zijn inmiddels meerdere campagnes gestart die specifiek gericht zijn op 50-plussers wegens de verhoogde kwetsbaarheid van deze groep voor deze vorm van oplichting (Intentieverklaring, 2018; Borwell & Bos-Riepma, 2018). Ook verschillende banken hebben hun campagne over veilig bankieren verder uitgebreid waardoor nu ook wordt gewaarschuwd voor helpdeskfraude (Hagenaars & Bonnes, 2020).

Tot slot houdt de politie zicht op zowel de modus operandi van de *scammers*, als de effecten van de genoemde maatregelen, en deelt ze deze informatie met andere partijen. Daarnaast worden ook andere partijen aangemoedigd om nieuwe bevin-

[90] De *book of crime* methodiek houdt in dat de stappen van een delictsvorm zo volledig en nauwkeurig mogelijk in kaart worden gebracht om zodoende tot passende interventies of barrières te komen.

[91] Deze informatie is gebaseerd op de intentieverklaring van de Brede Coalitie ter verstoring van Tech Support Scams in Nederland, geraadpleegd op 26-10-2020: https://docplayer.nl/141132487-Brede-coalitie-ter-verstoring-van-tech-support-scams-in-nederland.html

dingen zo snel mogelijk te delen (Intentieverklaring, 2018). Door zicht te houden op de modus operandi is een verschuiving zichtbaar geworden van *cold calling* naar nagebouwde websites waar slachtoffers via zoekmachines belanden (Borwell et al., 2020). Op grond van deze analyse wordt door de politie meer aandacht besteed aan het offline halen van deze websites (Hagenaars & Bonnes, 2020).
De effecten van het samenwerkingsverband zijn moeilijk te kwantificeren. Qua financiële schade is wel een afname zichtbaar sinds het bestaan van de samenwerking. Waar in 2017 ongeveer 5 miljoen euro aan schade is gerapporteerd, laten de cijfers van 2018 en 2019 respectievelijk 2,4 en 2,9 miljoen euro schade zien (OM.nl., 2020, Borwell et al., 2020). In interviews met betrokken partijen (publiek en privaat) wordt gesteld dat het aantal slachtoffers en de hoogte van de bedragen is gedaald. Het is echter niet duidelijk uit de stukken op te maken in welke mate deze daling kan worden toegeschreven aan deze gezamenlijke aanpak.

5.1.2 Anti-DDoS Coalitie

Bij de politie is met verschillende bedrijven en instellingen een samenwerking aangegaan om distributed-denial-of-service-aanvallen, ook wel DDoS-aanvallen genoemd (zie Bijlage 1 voor meer informatie over DDoS-aanvallen), tegen te gaan. De motieven voor het uitvoeren van DDoS-aanvallen kunnen zeer divers zijn. In de interviews geven meerdere politiemedewerkers aan dat vooral jonge daders relatief eenvoudig een DDoS-aanval laten uitvoeren op scholen of op concurrenten in de online *gaming*, waarbij een duidelijk financieel motief achterwege blijft en voornamelijk emoties als wraakzuchtigheid en de 'kick' naar voren komen als motief. Hoewel DDoS-aanvallen in veel gevallen relatief onschuldig lijken, met name wanneer er voldoende bandbreedte is om een aanval op te vangen, bestaan er ook voorbeelden van zaken waarbij bedrijven door middel van DDoS-aanvallen worden afgeperst en waarbij een financieel motief wel helder naar voren komt.

Hoewel veel grote instanties, zoals banken, regelmatig last hebben van DDoS-aanvallen, is het doen van een aangifte volgens de geïnterviewden niet vanzelfsprekend is. Mede door de hoge frequentie van DDoS-aanvallen melden instanties deze lang niet allemaal. Dit leidt tot een gebrek aan kennis over het fenomeen bij opsporingsinstanties. Een ander probleem dat geïnterviewden noemen is de complexiteit van de onderzoeken naar DDoS-aanvallen, waarbij technische sporen zelden leiden tot een concrete dader. Tot slot biedt ook het offline halen van *booters*[92] geen oplossing, omdat daders hier flexibel op inspelen. Zo bleek na het offline halen van de site webstresser.org, een *bootersite* waarop krachtige DDoS-aanvallen konden worden gekocht, het aantal DDoS-aanvallen binnen slechts enkele dagen weer op het gebruikelijke niveau te zitten. Daar komt bij dat de politie niet zomaar alle *bootersites* offline mag halen. Het aanbieden en aankopen van stresstestsen is op zichzelf niet strafbaar, wanneer de DDoS-aanvallen gebruikt worden om de 'DDoS-bestendigheid' van een eigen netwerk of site te testen en wanneer daar de eigen infrastructuur voor wordt gebruikt. Er moet dus eerst aangetoond worden dat een *booter* onrechtmatige DDoS-aanvallen faciliteert, voordat overgegaan kan worden tot een *take-down.*

[92] Een *booter* is een andere benaming voor een website waar DDoS-aanvallen worden aangeboden (Chromik etal., 2015)

Samenwerking
Omdat DDos-aanvallen vaak voorkomen en moeilijk te bestrijden zijn is de Nationale Politie in 2017 gestart met het project NoMoreDDoS, dat als doel heeft deze aanvallen tegen te gaan. No More DDoS richt zich op het verstoren van DDoS-aanvallen door dit fenomeen vanuit verschillende invalshoeken te bestrijden (No More DDoS, z.d.). De politie heeft hiervoor vijf pijlers geformuleerd:

- kennisnetwerk opbouwen van partners;
- informatiepositie verbeteren;
- verbeteren digitale opsporing;
- alternatieve interventies opzetten;
- outreach/communicatie.

De eerste pijler van No More DDoS, het opbouwen van een kennisnetwerk van partners, en heeft in 2018 vorm gekregen onder naam van de 'Anti-DDoS Coalitie'[93]. Voor dit initiatief zijn door het Nationaal Cyber Security Centrum (NCSC) 25 partijen[94] bij elkaar gebracht. Lopende projecten zoals No More DDoS van de Nationale Politie en de NaWas[95] van de Nationale Beheersorganisatie Internet Providers (NBIP) zijn hierdoor samengevoegd in dit nieuwe initiatief. Het initiatief heeft de partners onderverdeeld onder vijf verschillende werkgroepen, waaronder de werkgroep Clearing House die als doel heeft om een database te ontwikkelen waarin karakteristieken van DDoS-aanvallen in de vorm van zogenoemde *fingerprints*[96] kunnen worden opgeslagen. Deze kunnen vervolgens worden gedeeld en worden gebruikt voor onderzoek, ontwikkelen van mitigerende maatregelen, het identificeren van gebruikte infrastructuren en eventueel opsporing en vervolging.

De tweede pijler richt zich op het verbeteren van de informatiepositie van de politie. Het hierboven beschreven Clearing House is hier een belangrijk onderdeel van. Daarnaast wordt er geparticipeerd in wetenschappelijk onderzoek en geïnvesteerd in *forensic readiness*, wat inhoudt dat bij verschillende instanties de data van een DDoS aanval forensisch juist moeten kunnen worden vastgelegd. Verder is een *reporting tool* ontwikkeld om het voor instanties toegankelijker te maken om DDoS aanvallen te melden. Bij deze *reporting tool* geven instanties een maandelijks overzicht van de DDoS aanvallen die zij hebben gehad. Dit zorgt ervoor dat niet voor elke DDoS aanval een aangifte hoeft worden gedaan en dat de politie alsnog kennisneemt van deze aanvallen.

Het verbeteren van de digitale opsporing wordt besproken onder de derde pijler. Dit wil de politie eveneens doen aan de hand van het eerder beschreven Clearing House waar *fingerprints* in opgeslagen zijn. De wens hierbij is dat de techniek van

---

[93] Er is een onderscheid tussen No More DDoS en de Anti-DDoS Coalitie. No More DDoS is de projectnaam van de Nationale Politie om DDoS aanvallen te bestrijden, waar de Anti-DDoS coalitie de samenwerking tussen de 25 partijen betreft.

[94] Agentschap Telecom, AMS-IX, Belastingdienst, Betaalvereniging, De Nederlandsche Bank, De Volksbank, ministerie van Defensie, Stichting Digitale Infrastructuur Nederland (DINL), ministerie van Economische Zaken en Klimaat, The Hague Centre for Strategic Studies, ING, KPN, Logius, Stichting Nationale Beheersorganisatie Internet Providers (NBIP), NCSC, Nederland ICT, NL-iX, No More DDoS**,** Rabobank, Schuberg/Philips, SIDN, SURFnet, Tele2, Utwente, VNO-NCW, Vodafone/Ziggo

[95] NaWas staat voor Nationale Wasstraat. Dit is een afweersysteem voor DDoS-aanvallen en stuurt het digitale verkeer via de apparatuur van het NBIP waar het 'vuile' verkeer eruit wordt gewassen en het 'schone' en legitieme verkeer doorgang krijgt. (NBIP.nl)

[96] Bij een *fingerprint* worden karakteristieken van een DDoS aanval geëxtraheerd zoals bronadressen, pakketgroottes, duur van de aanval en protocoltypen (nomoreddos.org)

fingerprints accuraat genoeg wordt om booterservices te kunnen criminaliseren, websites offline te kunnen halen en een onderzoek te kunnen starten voor vervolging. In de realisatie van deze pijler wordt Europees samengewerkt.

Het offline halen van een *stresser* heeft weinig impact op de totale markt van DDoS, wat vraagt om alternatieve interventies, de vierde pijler. Bij alternatieve interventies kan worden gedacht aan maatregelen gericht op het ontmoedigen van de grootste doelgroep die DDoS aanvallen aanschaft. Voorbeelden hiervan zijn 'Hack_right',[97] *knock and talk* acties[98] en het gebruikmaken van *Google Advertisements* om de strafbaarheid van DDoS aanvallen te benadrukken.

Onder de pijler *outreach* valt het doel om de kennis over DDoS en het project breed naar buiten toe uit te dragen. Dit gebeurt ten eerste via de website van de politie en in de tweede plaats via de website van NoMoreDDoS. De *outreach* wordt gerealiseerd aan de hand van media campagnes en workshops.

In hoeverre de anti-DDoS coalitie er voor heeft gezorgd dat er minder DDoS-aanvallen worden gepleegd, kan nu nog niet gezegd worden. De ontwikkeling van een *clearing house* is momenteel bezig op kleine schaal met tien deelnemers en het is de bedoeling dat dit in de toekomst landelijk operationeel wordt. Voordat dit mogelijk is, zal het *clearing house* technisch nog moeten ontwikkelen en zullen er ook niet-technische stappen moeten worden gezet, bijvoorbeeld op het gebied van juridische overeenkomsten. Op langere termijn is het de ambitie om het *clearing house* ook op Europees niveau te laten opereren. Voor zover bekend is er over dit lopende project geen beoogde einddatum gecommuniceerd.

5.1.3 NoMoreRansom

NoMoreRansom is een samenwerkingsproject dat in juli 2016 is opgericht door THTC, Europol's European Cybercrime Center, Kaspersky en McAfee om slachtoffers van *ransomware* te helpen en voorlichting te bieden (zie bijlage 1 voor een uitgebreidere uitleg over *malware* en *ransomware*).
Ransomware heeft zich ontwikkeld als een serieus probleem op het gebied van cybercriminaliteit. In 2016 wordt een aanzienlijke stijging van deze *malware* waargenomen door het antivirusbedrijf Kaspersky. Het aantal meldingen was van 131.000 in 2014-2015 gestegen naar 718.000 in 2015-2016 (Europol, 2016). Concrete statistieken van Europol van de afgelopen jaren zijn niet bekend, wel geeft Europol aan dat er een aanmerkelijke daling van het aantal aanvallen heeft plaatsgevonden in 2018 (Europol, 2019). Europol veronderstelt dat deze daling wordt veroorzaakt doordat aanvallen gerichter plaatsvinden en dus minder wijdverspreid worden ingezet. Andere bronnen rapporteren in 2019 een stijging, die

[97] "Hack_Right is een alternatief of aanvullend straftraject. Jongeren van 12 tot 23 jaar die voor het eerst voor een cybercrimedelict worden veroordeeld, kunnen hiervoor in aanmerking komen. Het doel van Hack_Right is om recidive te voorkomen en het cybertalent van jongeren, binnen de kaders van de wet, verder te ontwikkelen. De strafrechtketenpartners, cybersecuritybedrijven en de hacker community ontwikkelen de interventie en voeren deze uit (politie.nl).

[98] Bij *knock-and-talk* acties worden personen waarvan de identiteit is achterhaald (in het geval van DDoS zijn dit vaak kopers van de diensten) door de politie benaderd voor een gesprek over hun strafbare gedragingen. Het doel hiervan is om de betreffende personen bewust te maken van de strafbaarheid, risico's en consequenties van hun gedrag. (politie.nl)

uiteenloopt van 50% tot 365%.[99] Wat duidelijk wordt uit deze bronnen is dat *ransomware* één van de grootste cyberdreigingen is vanwege de toenemende omvang van de schade. De focus op (grote) bedrijven zorgt ervoor dat hogere bedragen kunnen worden geëist wat resulteert in een grotere economische impact (Europol, 2019). In een recente survey van Sophos (2020) geeft 51% van de bedrijven uit 26 landen aan slachtoffer te zijn geworden van *ransomware* in 2019.

Samenwerking
In verschillende interviews met medewerkers van de politie en uit de private sector is over de totstandkoming van het project NoMoreRansom gesproken. Het project is ontstaan naar aanleiding van een opsporingsonderzoek waarbij THTC een tip kreeg over een Nederlandse server die gehackt zou zijn. Deze server bleek te fungeren als een soort administratieserver waarbij digitale sleutels opgeslagen waren. Deze sleutels konden worden gebruikt voor het ontsleutelen van bestanden op computers die door *ransomware* waren geïnfecteerd. Volgens de geïnterviewden is naar aanleiding van deze bevindingen de samenwerking gezocht met de eerder genoemde partijen om een platform te creëren waarbij digitale sleutels gratis aan slachtoffers zouden kunnen worden verstrekt.

Het doel van dit project is tweeledig. Enerzijds dient het project om slachtoffers van *ransomware* te helpen door deze kosteloos van sleutels te voorzien waarmee de versleutelde bestanden toegankelijk kunnen worden gemaakt. Anderzijds heeft het project ook een preventief doel door gebruikers te informeren over de werking van *ransomware* en de mogelijke maatregelen hiertegen.

Vier jaar na het oprichten van NoMoreRansom is het project uitgebreid naar een samenwerking van 163 partners uit zowel het private als het publieke domein. Verder blijkt de website meer dan vier miljoen bezoekers uit 188 verschillende landen te hebben geholpen. De betrokken partijen claimen dat het project ervoor heeft gezorgd dat een bedrag van 623 miljoen euro niet in criminele handen is gekomen (Politie.nl, 2020). Het gaat hierbij om het bedrag dat anders door slachtoffers zou zijn betaald. Hierbij moet uiteraard een slag om de arm worden gehouden aangezien moeilijk te zeggen is of deze slachtoffers daadwerkelijk tot een betaling zouden zijn overgegaan. Voor zover bekend is er over dit project geen einddatum gecommuniceerd.

5.2 PPS bij de aanpak van cybercriminaliteit

In deze paragraaf wordt ingegaan op Publiek Private Samenwerking bij de aanpak van cybercriminaliteit. Hierbij worden bevindingen uit de interviews met respondenten uit de private en publieke sector besproken, aangevuld met informatie uit de literatuur.

In de interviews werd zowel over de drie beschreven samenwerkingsprojecten gesproken, als over publiek-private samenwerking in het algemeen. Hierbij kwam een verscheidenheid in aanpak en totstandkoming naar voren, en werd duidelijk

[99] https://blog.*malware*bytes.com/reports/2019/08/labs-quarterly-report-finds-*ransomware*s-gone-rampant-against-businesses/
https://blog.checkpoint.com/2020/10/06/study-global-rise-in-*ransomware*-attacks/
https://www.welivesecurity.com/2020/08/07/small-medium-sized-businesses-big-targets-*ransomware*-attacks/

dat een samenwerkingsverband geen vast stappenplan kent en dat elk samenwerkingsverband tot op zekere hoogte een uniek karakter heeft. In deze paragraaf staan we stil bij de totstandkoming van de samenwerking, de motieven om samen te werken, de succesfactoren en de knelpunten.

5.2.1 Totstandkoming samenwerking

In de interviews kwam naar voren dat veel publiek-private samenwerkingen op het gebied van cybercriminaliteit ontstaan vanuit al bestaande netwerken. Cybersecurity wordt omschreven als een 'klein wereldje' waar men elkaar snel tegenkomt en waar de 'lijntjes' tussen verschillende personen en partijen kort zijn. Dit heeft in het verleden tot vele ad hoc-samenwerkingen geleid tussen publieke en private partijen en hier zijn politiemedewerkers in het algemeen positief over gestemd. Toch is er vanuit het OM en de politie de wens ontstaan om in de publiek-private samenwerkingsverbanden verder te professionaliseren. Deze professionalisering moet ervoor zorgen dat samenwerkingsverbanden beter gestructureerd worden. Dit moet voorkomen dat projecten door elkaar heen gaan lopen en ertoe leiden dat de politie een meer betrouwbare samenwerkingspartner wordt. Een gevaar in de ad hoc-samenwerkingsverbanden is dat een project of onderzoek 'doodbloedt' en de samenwerkingspartner uiteindelijk geen contact meer met de politie heeft. Door meer structuur in de samenwerkingsverbanden te krijgen, kan dit mogelijk worden voorkomen. Een mogelijk nadeel van meer professionalisering is echter dat het spontane karakter waarmee nu soms in eerste aanleg contact wordt gezocht verdwijnt waardoor het aangaan van samenwerking juist wordt bemoeilijkt. Hoewel er onder politiemedewerkers begrip is voor de wens de samenwerking meer te professionaliseren, geven meerdere politiemedewerkers aan waarde te hechten aan het spontaan tot stand komen van samenwerkingsverbanden en zouden ze het vervelend vinden als dit volledig verdwijnt. In het verleden heeft spontane samenwerking mooie resultaten opgeleverd en de snelheid waarmee dergelijke samenwerking tot stand kan komen heeft voordelen, zoals is gebleken bij NoMoreRansom. Ook wordt benadrukt dat het van belang is om vrije ruimte te hebben in de werkzaamheden om dit soort projecten te kunnen starten of een bepaald momentum te kunnen pakken in een onderzoek, als samenwerking nuttig blijkt. Een politiemedewerker schetst het dilemma van meer professionalisering:

> *'Ik ben wel eens bang dat als je dingen te veel gaat definiëren en afkaderen en institutionaliseren dat misschien ook wel een beetje van die bottom-up spontaniteit verdwijnt, dat zou kunnen. Maar je ziet bij PPS dat je uiteindelijk wel een stukje aan professionalisering moet gaan doen. Ook naar je partners toe. Want het risico bestaat dat iemand een tijdje een onderzoek doet met een partner en dat de partner daarna helemaal niks meer hoort van de politie.'*

De verschillende manieren van totstandkoming van een samenwerking zijn zichtbaar in de drie beschreven samenwerkingsprojecten. Het project NoMoreRansom kenmerkt zich door de sterke ad hoc benadering die de start van het project kende. Dit project is ontstaan vanuit de kansen die voortgekomen zijn uit het veiligstellen van een server waar veel digitale sleutels voor *ransomware* op aanwezig waren. Deze sleutels konden gedeeld worden met slachtoffers van de betreffende *ransomware* en naar aanleiding daarvan is in een kort tijdsbestek nagedacht over de manier waarop dit het beste gedaan kon worden. Door middel van 'korte lijnen' in het netwerk van enkele politiemedewerkers is contact gezocht met een medewerker van anti-virusbedrijf Kaspersky en vervolgens is het platform van NoMoreRansom opgezet.

Hoewel er bij de anti-DDoS coalitie eveneens sprake was van een enigszins spontane totstandkoming, lijkt in de aanloop daarvan meer professionalisering aanwezig. Na het neerhalen van een grote *bootersite* door THTC ontstond het besef dat dusdanige take-downs op de lange termijn weinig effect hadden en dat DDoS aanvallen op een bredere manier bestreden moest worden. De eerste stappen naar een samenwerking zijn gezet door individuen vanuit de politie en de bancaire sector. Vervolgens zijn via het NCSC meerdere partijen gezocht voor de samenwerking. Een belangrijk aspect in de totstandkoming betreft de timing van deze werving van samenwerkingspartners, waar duidelijk werd dat er ingespeeld werd op de actualiteit waarin bij verschillende partijen commotie ontstond over de impact van DDoS-aanvallen.

Helpdeskfraude was voorafgaand aan de samenwerking oververtegenwoordigd in de aangiftes wat de urgentie om het aan te pakken benadrukte. De schade was vaak groot bij individuele slachtoffers en een problematisch gegeven hierbij was dat er geen duidelijke tussenpartij was die zich over deze slachtoffers ontfermde. Het arrondissementsparket in Rotterdam heeft uiteindelijk het voortouw genomen om de modus operandi van de helpdeskfraude te onderzoeken en partijen te benaderen om gezamenlijk een aanpak te creëren. Hierbij is een intentieverklaring tot stand gekomen waar op voorhand uitgebreid over gecommuniceerd is door de betrokken partijen.

5.2.2 Motieven voor het aangaan van samenwerking

Er zijn een aantal motieven te identificeren die maken dat de politie naar samenwerking met externe partijen zoekt. Door snelle ontwikkelingen op het gebied van technologie en daarmee ook cybercriminaliteit, bestaat bij de politie het gevaar dat er een gebrek aan kennis en expertise is (Koops, 2010; Harkin, Whelan & Chan). Deze kennis en expertise kan in sommige gevallen gevonden worden in de private sector. Een voorbeeld hiervan is het uitgeven van *malware-samples* voor analyse aan anti-virusbedrijven, die daarover meer expertise bezitten dan de politie. Ook het internationale karakter van cybercriminaliteit bemoeilijkt de handhavingstaken van de politie (Boes & Leukfeldt, 2017). Een samenwerking met private partijen kan op dit gebied meer mogelijkheden bieden voor een alternatieve aanpak om criminaliteit tegen te gaan, zoals te zien bij NoMoreDDoS, de Anti-DDoS Coalitie en de Brede Coalitie ter verstoring van Tech Support Scams. Bij de private sector wordt met name gekeken naar economische of kostenbesparende voordelen en het verkrijgen van nuttige informatie van publieke partijen als motieven (ENISA, 2010; Hagenaars & Bonnes, 2020). Meer specifiek voor IT-bedrijven geldt ook dat ze hun reputatie kunnen verhogen door aan te geven dat ze (succesvol) samenwerken met de politie.

In de kamerbrief 'Integrale aanpak cybercrime' (2018) wordt door de Minister vooral benadrukt dat private en publieke partijen elkaar nodig hebben om cybersecurity te verbeteren en cybercriminaliteit te bestrijden. Dit wordt in het onderhavige onderzoek in de interviews onderschreven. Veel van de genoemde motieven gaan in op de wisselwerking tussen de private en publieke sector waarbij alle betrokken partijen vroeg of laat profiteren van de samenwerking.
Private bedrijven zoals IT-securitybedrijven zien welke impact MO, *tooling*, en aanvalsinfrastructuur heeft op de slachtofferzijde. Politie ziet vooral het verband tussen de dader en de MO, *tooling*, aanvalsinfrastructuur. PPS op het gebied van cybercriminaliteit is er vanuit de politiezijde op gericht om deze twee perspectieven (dader- en slachtofferperspectief) samen te voegen en zo het hele plaatje te kunnen

zien. Tot slot het aangaan van een samenwerking ook zorgen voor een groter netwerk, en daarmee een groter bereik.
Ook voor private partijen zijn er duidelijke beweegredenen om de samenwerking met politie te zoeken op het gebied van cybersecurity. Zo komt in de interviews naar voren dat private partijen zelf schade ondervinden van cybercriminaliteit en daardoor baat hebben bij een effectieve bestrijding ervan. Daarnaast beschikt de politie over specifieke informatie en verdergaande bevoegdheden wat voor private partijen kan bijdragen aan een betere bescherming van eigen klanten.

Ook wordt door private partijen de maatschappelijke verantwoordelijkheid en de positieve effecten op de reputatie van een bedrijf genoemd als één van de redenen die bijdragen aan het aangaan van een samenwerking. Uit de interviews komt ook naar voren dat private bedrijven steeds vaker de weg naar de politie weten te vinden. Met enige regelmaat wordt een politieonderzoek naar cybercriminaliteit gestart na een melding van een privaat bedrijf.

Tot slot geldt voor alle partijen dat een samenwerking een aantal praktische voordelen oplevert. Structurele samenwerkingen kunnen ervoor zorgen dat beslissingsprocessen gestroomlijnder lopen, sneller actie kan worden ondernomen en dat de 'lijntjes naar elkaar korter zijn'. Naast de kortere lijntjes betekent een samenwerking ook dat er gebruik kan worden gemaakt van elkaars netwerk wat uiteindelijk zorgt voor een betere informatiepositie voor zowel publieke als private partijen. Uit de interviews is tevens naar voren gekomen dat versterken van banden met een private partij een belangrijke motivatie kan zijn om een samenwerkingsverband aan te gaan, mits de politie verwacht dat die samenwerking in de toekomst voordelen op kan leveren.

Samengevat zien politiediensten in een samenwerking mogelijkheden om tot een effectievere aanpak van cybercriminaliteit te komen en worden private partijen gemotiveerd door de voordelen die ontstaan uit deze effectievere aanpak gecombineerd met positieve publiciteit. Voor beide sectoren geldt dat geprofiteerd kan worden van elkaars informatiepositie op het gebied van cybercriminaliteit. Hierbij moet wel in acht worden genomen dat het delen van informatie soms problematisch kan zijn, zoals is beschreven in de knelpunten in paragraaf 5.3.4.

5.2.3 Succesfactoren

In de interviews is uitgebreid ingegaan op de factoren die volgens de literatuur en de respondenten uit het onderhavige onderzoek een PPS succesvol maken. In deze paragraaf wordt ingegaan op de meest genoemde succesfactoren die grofweg onder te verdelen zijn in de onderwerpen, (1) vertrouwen, (2) gedeelde belangen, (3) communicatie en (4) overige factoren. Deze succesfactoren sluiten ook aan bij factoren die in eerder onderzoek zijn geïdentificeerd als ingrediënten voor een succesvolle samenwerking (zie voor een uitgebreid overzicht over de effectiviteit van PPS: Staats, Meerts, Kleemans & Huisman, 2021).

Vertrouwen
In de literatuur wordt meermaals verwezen naar het belang van vertrouwen tussen de partijen in een samenwerking (Boes & Leukfeldt, 2017; Hagenaars & Bonnes, 2020). Zo kan veel onderling vertrouwen zorgen voor een grotere handelingssnelheid en daarmee een efficiëntere samenwerking (Covey & Merrill, 2012). Vertrouwen tussen de partijen wordt vergroot wanneer er kwalitatief goede informatie met elkaar wordt gedeeld, concrete resultaten worden behaald en volledige trans-

parantie over verwachtingen. Ook de continuïteit in de deelname van de samenwerking is een factor die vertrouwen kan vergroten, zeker wanneer vaste mensen betrokken blijven en elkaar regelmatig blijven ontmoeten. Op het gebied van continuïteit lijken publieke partners niet altijd betrouwbaar omdat deelname in sommige gevallen afhankelijk kan zijn van politiek, reorganisaties en bezuinigingen (Hagenaars & Bonnes, 2020).

Informatie moet in de eerste plaats gedeeld mogen worden, maar men moet het ook willen delen met elkaar. In de interviews werd het bestaan van onderling vertrouwen in een samenwerkingsverband het vaakst genoemd als succesfactor. Geïnterviewden bedoelen hiermee dat partijen elkaar informatie kunnen toevertrouwen en dat men van elkaar weet hoe er met de informatie moet worden omgegaan en dat hier geen misbruik van wordt gemaakt. Ook gaat het om het besef van, oog voor, en rekening houden met elkaars belangen in de samenwerking. De aanwezigheid van vertrouwen zorgt ervoor dat het laagdrempeliger is om een samenwerking aan te gaan met bekende partijen. Dit was bijvoorbeeld het geval bij het samenwerkingsverband NoMoreRansom. De politie had bij eerdere opsporingsonderzoeken al met succes samengewerkt met dit cybersecuritybedrijf waardoor de vertrouwensband al aanwezig was. Wat hierbij belangrijk is, is dat er sprake is van continuïteit van de aanwezige personen in de samenwerking zodat de betrokkenen met bekende mensen aan tafel blijven zitten.

Hoewel vertrouwen volgens respondenten vaak stijgt naarmate een samenwerking vordert, kunnen vooroordelen jegens elkaar afbreuk doen aan het vertrouwen zoals een respondent uit de private sector illustreert:

> *'Wat ik heel vaak merk bij de politie, ook wel bij andere sectoren maar bij de politie zeker, is dat ze denken dat het veel erger is dan dat het is en dat je allerlei dingen niet vertelt. Andersom had ik dat ook. Toen ik bij [bedrijf] kwam dacht ik nou nu kom ik echt achter de grote complotten en de grote geheimen, maar er gebeurde niks. De politie denkt altijd dat er heel veel bij de banken mis is en dat ze dat net niet vertellen en dat is dus niet zo. Je moet er uiteindelijk ook een beetje vertrouwen in hebben dat het misschien helemaal niet zo erg is allemaal. Er zijn veel mensen bij de politie die denken van jullie vertellen het ons toch niet.'*

Het is aan de hand van interviews niet na te gaan in hoeverre daadwerkelijk alle relevante informatie wordt gedeeld tussen de partijen. Wel komt uit de gesprekken met respondenten van de politie en het OM naar voren dat het idee bestaat dat private partijen soms relevante informatie achterhouden als dat hen beter uitkomt. Hoewel niet benoemd zal ook het omgekeerde het geval zijn: de politie zal ook niet alles delen. Wellicht dat private partijen zich dat ook realiseren, maar dat is meer geaccepteerd is. Daarnaast speelt nog mee dat niet alles wat men misschien wil delen ook gedeeld mag worden volgens de Wpg of AVG.

Gedeelde belangen en doelen

In de literatuur worden gedeelde belangen als een belangrijke voorwaarde voor een succesvolle samenwerking gezien. Dit houdt onder meer in dat het goed is dat de noodzaak van samenwerken wordt onderkend en dat de meerwaarde van de samenwerking duidelijk is voor alle partijen. Om deze reden kan het verstandig zijn om de samenwerking te zoeken met partijen die eveneens hinder ervaren van het gestelde probleem. Verder kan het bevorderend kan werken als partijen zich verdiepen in elkaars belangen en motieven om op deze manier de samenwerking beter op elkaar te kunnen afstemmen. Op deze manier kan worden nagegaan op

welke punten partijen eventueel tegen hun belangen in moeten handelen (Boes & Leukfeldt, 2017; Hagenaars & Bonnes, 2020).

Ook de personen die we interviewden voor dit onderzoek benoemen de rol van de belangen die de betrokken partijen hebben bij de samenwerking. Zo wordt genoemd dat het belangrijk is dat de aanwezige partijen een duidelijk eigen doel of belang hebben waarin ze willen investeren omdat anders het risico bestaat dat er niet intensief meegewerkt wordt aan het project. Hoewel de belangen van partijen in zekere zin bij kunnen dragen aan het succes van een samenwerking, kan het ook een belemmering vormen wanneer deze belangen niet met elkaar overeenkomen. In de projecten die wij hebben bestudeerd heeft dit echter geen onoverkomelijke problemen opgeleverd. Om die reden wordt door enkele geïnterviewden wel genoemd dat de wederkerigheid in een samenwerking op orde moet zijn. Daarnaast moeten de partijen een bepaalde mate van flexibiliteit hebben zodat dat er uiteindelijk een gemeenschappelijk draagvlak ontstaat waarbij alle partijen hetzelfde doel voor ogen hebben. Hierbij werd tevens genoemd dat het kan helpen als een samenwerking een einddatum heeft, zoals het geval is bij de Brede Coalitie ter verstoring van Tech Support Scams. Daarnaast kan het volgens Schuilenburg (2012) helpen als de samenwerking een concrete zaak of probleemstelling betreft met een duidelijk doel en niet een abstract vooruitzicht. Dit wordt ook onderschreven door de geïnterviewden.
Onduidelijk gedefinieerde doelen kunnen volgens Boes en Leukfeldt (2017) afbreuk doen aan het collectieve enthousiasme in de samenwerking.

Naast dat het goed is wanneer een samenwerking een concrete zaak of probleemstelling betreft, is het volgens respondenten ook belangrijk dat de resultaten van het project zichtbaar en meetbaar zijn. Hierbij valt op dat de respondenten vanuit de publieke sector voornamelijk kijken naar de daling van de criminaliteitsvorm, terwijl respondenten uit de private sector het succes ook afmeten aan de hand van interne doelen.

Gedeelde belangen en doelen als succesfactor houden niet in dat deze bij alle partijen hetzelfde moeten zijn. Belangen en doelen kunnen bij een samenwerking verschillen tussen de partijen en naast elkaar bestaan indien deze bijdragen aan de voortgang van de samenwerking. Vanuit de politie en het OM is het heersende principe dat bij een samenwerking het gedeelde publieke belang moet prevaleren boven het belang van een enkele private partij.

Communicatie
Een goede communicatie is volgens de literatuur een andere belangrijke voorwaarde voor een succesvolle samenwerking (Schuilenburg, 2012; Boes & Leukfeldt, 2017; Hagenaars & Bonnes, 2020). Het gaat hier onder andere om het plaatsvinden van goede informatie-uitwisseling en snelle informele contactmomenten, wat onderschreven wordt door respondenten. Hierbij wordt bedoeld dat de partijen elkaar snel kunnen vinden als er nuttige informatie gedeeld moet worden en er duidelijk gecommuniceerd wordt over de afspraken die men met elkaar maakt. Het oprichten van gezamenlijke operationele teams kan de samenwerking en informatie uitwisseling bevorderen (Hagenaars & Bonnes, 2020).

Verder wordt ook de nadruk gelegd op onderlinge transparantie, openheid en eerlijkheid in de communicatie. Dit is bijvoorbeeld belangrijk bij het sturen van verwachtingen, zoals beschreven is door Hagenaars en Bonnes (2020). Volgens de geïnterviewden leidt goede en eerlijke communicatie tot meer begrip en

duidelijkheid over de verwachtingen naar elkaar. Dit betekent eveneens dat communicatie niet of nauwelijks los gezien kan worden van de aanwezigheid van onderling vertrouwen. Wanneer verwachtingen goed uitgesproken worden, is tevens snel zichtbaar of een samenwerking toekomst heeft en dat niet het risico bestaat dat er geruime tijd langs elkaar wordt gelopen zonder dat er progressie geboekt wordt. Indien dat laatste het geval is kan beter vroegtijdig worden besloten dat het beter is om de samenwerking te stoppen.

Goede communicatie kan worden belemmerd als private partijen met een onderlinge concurrentiepositie niet alle informatie inzichtelijk willen maken. Geïnterviewden van private partijen geven aan dat zij een leidende rol van de overheid in dat geval als prettig ervaren doordat zij op deze manier gevoelige informatie met een neutrale partij kunnen delen. Zo wordt in de Anti-DDoS Coalitie gebruikgemaakt van een *reporting tool* waarbij banken aan de politie kunnen melden hoeveel DDoS aanvallen zij in een periode meemaken zonder dat dit gedeeld wordt met concurrenten.

Overig
In de literatuur komen nog enkele andere succesfactoren naar voren. Zo wordt het erkennen van elkaars expertise in een samenwerking belangrijk geacht, alsook het verdelen van de taken naar deze expertises (Hudson et al., 1999; Boes & Leukfeldt, 2017). Hagenaars en Bonnes (2020) beschrijven dat de praktische kant van een samenwerking niet moet worden vergeten. Voor een goede PPS zijn voldoende middelen nodig waarbij tevens gelijkwaardige input wordt geleverd. Daarnaast moet aan de hand van beproefde methodes worden gewerkt. Hagenaars en Bonnes wijzen hierbij zelf naar barrièremodellen en het opstellen van een *book of crime*, zoals bijvoorbeeld is gebeurd bij de Brede Coalitie ter verstoring van Tech Support Scams.

Andere aangewezen succesfactoren betreffen een lange termijn focus met geduld en een 'veranderaanpak' bij de partijen wanneer het gaat om langlopende samenwerkingsverbanden (Hagenaars & Bonnes, 2020). Daarnaast wijzen de geïnterviewden op het belang van de aanwezigheid van proactieve personen ('kartrekkers') en de 'juiste mensen' die hun eigen gebruiken, opvattingen en beleid voldoende kunnen en willen aanpassen ten gunste van de samenwerking.

5.2.4 Knelpunten

Naast succesfactoren zijn ook knelpunten benoemd die de samenwerking tussen private en publieke partijen bemoeilijken. De knelpunten die de geïnterviewden noemden zijn grofweg onder te verdelen in tegenstrijdige belangen, juridische knelpunten en een groep overige knelpunten.

Tegenstrijdige belangen
Een mogelijke keerzijde van PPS is dat belangen uit de publieke sector verstrengeld raken met belangen uit de private sector. Private partijen hebben een achterliggend economisch belang dat over het algemeen vaak heeft meegewogen bij het aangaan van de samenwerking, terwijl publieke partijen het maatschappelijk belang horen te dienen. Hierbij kan gedacht worden aan een zo efficiënt mogelijke besteding van publiek geld (Feng et al., 2018) en het bewaken van publieke waarden en grondrechten (Sanders, 2017). Deze belangen kunnen naast elkaar bestaan, maar ook tot problemen leiden in een samenwerking wanneer deze niet verenigbaar zijn. Sanders (2017) beschrijft verder de zorgen die kunnen ontstaan wanneer private partijen meewerken om een publiek belang te dienen. Nadelige effecten kunnen optreden op het gebied van transparantie, legitimiteit en verminderde overheidszeggenschap

wanneer een publiek probleem gedeeltelijk wordt toegeëigend door de private sector. Ook bestaan er bezwaren ten opzichte van de publieke sector bij het aangaan van PPS. De bedrijfsmatige visie zoals in de ideeën van *New Public Management* wordt gesteld kan ongepast zijn voor een overheidsinstelling, aange-zien deze zich om meer waarden moet bekommeren dan bedrijfsmatige waarden als kosteneffectiviteit (Bryson, Crosby & Bloomberg, 2014).

In een samenwerking kan volgens de geïnterviewden ook een moeilijk moment ontstaan wanneer tegenstrijdige belangen aan het licht komen. Zoals eerder benoemd bij de bespreking van de succesfactoren, is het belangrijk dat men duidelijk en open is over elkaars belangen en deze tot op zekere hoogte accepteert. Er zijn echter momenten wanneer dit minder makkelijk gaat en het tot knelpunten leidt. Zo wordt in interviews met politiemedewerkers meermaals het commercieel belang van de private partijen als een dilemma gezien, omdat dit het belang van de politie of het maatschappelijk belang mogelijk in de weg kan zitten. De aanwezigheid van deze belangen wordt over het algemeen begrepen, maar kan leiden tot frustraties wanneer dit het belang van de politie of van de samenwerking in de weg zit. Dit kan in sommige gevallen leiden tot het stoppen van een samenwerking, zoals één geïnterviewde politiemedewerker hieronder beschrijft:

> *'Zo'n bedrijf stapt er in en die heeft een bepaald commercieel belang. Ze willen best samenwerken, maar dat moet uiteindelijk hun product voor de toekomst naar klanten vaak versterken. Wij hadden uiteindelijk niet echt het gevoel dat dat bedrijf er ook heel erg in zat om algemene dreigingen weg te nemen. Het kostte bijzonder veel moeite om uiteindelijk belangrijke informatie van dat bedrijf te krijgen om die te analyseren en dan tot conclusies te komen. Dat heeft ertoe geleid dat we uiteindelijk hebben gezegd van ja weet je het houdt op, dit lukt niet.'*

Commerciële belangen kunnen er volgens OM- en politiemedewerkers toe leiden dat bedrijven niet genoeg informatie willen verstrekken of dat ze onvoldoende bereid zijn hun diensten of werkwijzen aan te passen aan het belang van de politie of het samenwerkingsverband in het geheel. De angst voor een starre houding van bedrijven kan er ook toe leiden dat een samenwerking in eerste instantie al niet wordt gezocht. Een voorbeeld hiervan is de reactie van een officier van justitie die geen potentie zag in een samenwerking met webshops wegens de te sterke focus op winst en marktwaarde die deze bedrijven zouden hebben ten opzichte van het bestrijden van criminaliteit.

Opvallend is dat de uitspraken over de problemen omtrent commerciële belangen allemaal gaan over eerdere, fictieve of hypothetische samenwerkingsverbanden en dat dit in de drie bestudeerde projecten NoMoreRansom, de anti-DDoS coalitie en de samenwerking omtrent de helpdeskfraude niet als een belangrijk knelpunt wordt genoemd.

Positieve publiciteit kan een belangrijke motivatie zijn voor private partijen om deel te nemen aan een samenwerking met de politie. De werkwijze van de politie kan echter botsen met deze belangen. Met name wanneer een partij naar buiten wil treden met een rapport, blog of overige berichtgeving, kan dit leiden tot bezwaren bij de politie om te voorkomen dat er onderzoeksbelangen worden geschaad. Omgedraaid geldt dat private partijen soms het gevoel hebben dat de politie 'te simpel' denkt over de rol van publiciteit in een samenwerkingsverband. Private

partijen geven aan dat deze publiciteit echter een belangrijke drijfveer kan zijn om een samenwerking aan te gaan.

Tegengestelde belangen kunnen een samenwerking dus in de weg zitten, waardoor het belangrijk is dat partijen kennis hebben van elkaars belangen, zoals een van de geïnterviewden uit de private sector beschrijft:

> *'Je merkt wel als je begint dat je elkaars wereld toch niet altijd goed kent. En dat dat toch wel wat uitdagingen geeft. […] Dus dat stukje begrip voor elkaar, dat je vooraf van elkaar snapt van hoe werkt het nou, zou misschien helpen. […] Als ik zo terugdenk dan was het meestal de dingen waar het dan wat stroever liep, zat het dan toch heel vaak in het begrip van elkaars processen, organisatie, technologie, dienstenpakket, het hele stuk.'*

Door gebrek aan inzicht in elkaars wereld is het mogelijk dat er onbegrip en vooroordelen jegens elkaar ontstaan, wat een succesvolle samenwerking in de weg kan staan. Dit kan volgens geïnterviewden worden ondervangen door de aanwezigheid van voldoende vertrouwen en geven van openheid van zaken.

Een ander mogelijk knelpunt omtrent commerciële belangen betreft de keuze om samen te werken met een specifiek bedrijf. Zo wordt door een politiemedewerker het dilemma omschreven dat samenwerken met een private partij ook direct betekent dat je de concurrenten van deze partij uitsluit en daarmee de samenwerkingspartner op een manier commercieel bevoordeelt. Hierbij vroeg deze medewerker zich hardop af of dit wel wenselijk is.

Juridische knelpunten rondom het delen van informatie

Bij een publiek-private samenwerking moet rekening worden gehouden met juridische kaders. Een van de uitdagingen in dit verband is het delen van informatie, waarvan in de praktijk blijkt dat het niet altijd direct helder is voor alle samenwerkende partijen aan welke regels zij moeten voldoen (Kop, 2017). De wet stelt hierbij strikte eisen aan gegevens die te herleiden zijn naar natuurlijke personen. Andersoortige informatie, zoals het uitwisselen van informatie over nieuwe criminele ontwikkelingen, kan over het algemeen met elkaar kunnen worden gedeeld. Bij het delen van persoonsgegevens zijn een aantal aspecten waar rekening mee moet worden gehouden. Ten eerste is de Algemene Verordening Gegevensbescherming (AVG) leidend. Persoonsgegevens mogen volgens de AVG gedeeld worden wanneer dit met toestemming van de betrokkene is of als de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang. (Hagenaars & Bonnes, 2020). De komst van de personen die wij interviewden ook een complicerende factor geworden op dit gebied:

> *'Het voordeel was dat toen alleen nog de wet persoonsgegevens er was en nog niet die nieuwe AVG. Daardoor konden we iets makkelijker IP-adressen delen bijvoorbeeld, dat is nu allemaal wat strikter en moeilijker. Eerder was het zo dat een persoonsgegeven een persoonsgegeven was als het makkelijk te herleiden was naar de persoon. Een IP-adres kun je alleen maar herleiden naar een persoon als je de ISP bent van die persoon.'*
> Medewerker politie

> *'De AVG zelf is niet zo erg, maar het interpreteren van die wet is schijnbaar heel ingewikkeld. Wat je merkt is dat niemand meer goed weet waar die aan toe is. Heel vaak betekent dat dat ze in de modus gaan zitten van dan deel ik maar niks*

meer want ik weet niet zeker of het mag. Dat is ongelofelijk ingewikkeld. Het wordt er niet beter van omdat we een toezichthouder hebben die ook niet heel duidelijk is in wat wel en wat niet mag. Dan raak je in spagaat.'
Medewerker private sector

Door geïnterviewden is genoemd dat het probleem niet enkel de striktheid van de wet- en regelgeving betreft, maar dat ook de interpretatie ervan kan leiden tot tijdrovende discussies onder juristen. De complexiteit van de wet- en regelgeving zorgt tevens voor een grotere terughoudendheid bij betrokken partijen om informatie te delen, omdat zij niet exact op de hoogte zijn wat precies wel en niet gedeeld mag worden. In het geval van langdurige samenwerkingen, wordt het daarom belangrijk geacht om juristen in een vroeg stadium te betrekken. Op deze manier kan de wettelijke basis van het delen van informatie worden herkend en worden ondervangen met een convenant.
Private partijen hebben verder mogelijk nog te maken met sectorale afspraken, geheimhoudingsplichten en de Wet bescherming persoonsgegevens (Wbp). De Wbp stelt dat de verwerking van persoonsgegevens een wettelijke grondslag dient te hebben en dat deze gerechtvaardigd en voor een specifiek belang moet zijn (Gerritsma-Breur & Verveld-Suijkerbuijk, 2013). Gegevens die voor bedrijfsbelangen verzameld zijn, mogen dus niet per definitie gedeeld worden voor opsporingsdoeleinden. De politie en het OM zijn daarnaast ook gebonden aan enkele wettelijke bepalingen. De wet politiegegevens (Wpg) stelt dat er over lopende onderzoeken geen informatie gedeeld mag worden aan derden. Deze bepaling, die betrekking heeft op het verstrekken van politiegegevens, is opgenomen in artikel 1 van de Wpg. Uitzonderingen hierop zijn artikel 18, 19 en 20 Wpg. Artikel 18 gaat over de structurele verstrekking van gegevens aan derden. Artikel 19 regelt informatieverstrekking aan derde partijen op incidentele basis en artikel 20 gaat in op informatieverstrekking op structurele basis in het geval van een samenwerkingsverband. Alle artikelen vereisen een zwaarwegend algemeen belang en stellen dat informatie-uitwisseling enkel voor de volgende doeleinden mogelijk is: (1) het voorkomen en opsporen van strafbare feiten, (2) het handhaven van de openbare orde, (3) het verlenen van hulp aan hen die deze behoeven en (4) het uitoefenen van toezicht op het naleven van regelgeving.

Op het gebied van internetoplichting komen in de toekomst nieuwe mogelijkheden voor het delen van informatie tussen de politie en Nederlandse banken. Bij de derde aangifte met eenzelfde rekeningnummer kan de politie een melding geven bij de betreffende bank, zodat deze passende maatregelen kan treffen (Ministerie van Justitie en Veiligheid, 2020). Ook zal volgens de kamerbrief van de Minister van Justitie en Veiligheid verder onderzoek worden uitgevoerd naar de versterking van gegevensdeling tussen de politie en de banken op het gebied van internetoplichting. Tot slot wordt slachtoffers de mogelijkheid geboden dat zij, mits er aangifte is gedaan, na 21 dagen de NAW-gegevens van de fraudeur kunnen ontvangen om zodoende een civiele procedure te starten. Er wordt nader onderzocht in hoeverre slachtoffers hun schade kunnen verhalen en welke rol van ondersteuning de banken en de politie hierbij kunnen spelen.

Uit onderzoek van Gerritsma-Breur en Verveld-Suijkerbuijk (2013) blijkt dat in de praktijk de wetgeving regelmatig voor problemen zorgt rondom het delen van informatie. Ook bij de respondenten van het onderhavige onderzoek komt duidelijk de mening naar voren dat het delen van informatie te ingewikkeld is gemaakt, zoals de geïnterviewden uit zowel de publieke als de private sector verwoorden:

'Bij specifieke onderzoek is het grootste struikelblok dat wij politie informatie hebben en zijn dus gehouden aan de politiewet en verder hebben alle bedrijven zich te houden aan de privacywetgeving en ook nog hun eigen business. Die drie hordes moet je allemaal overwinnen voordat je die informatie-uitwisseling in de praktijk uitvoert.'
Medewerker politie

'Het is niet zo'n lolletje tegenwoordig om informatie uit te wisselen. Hoe belangrijk ik privacy ook vind, soms loop je tegen allerlei obstakels aan waarvoor de wetgeving niet bedoeld is. De grootste obstakels op dit moment hebben te maken met wet- en regelgeving. Heus niet alleen privacy.'
Medewerker private sector

De strenge wet- en regelgeving omtrent het delen van informatie zorgt ervoor dat in sommige gevallen informatie met een omweg bij de politie moet komen. Zo kan de politie overgaan tot een vordering of worden betrokken personen als getuige gehoord om op een rechtmatige manier tot overdracht van informatie te komen. Onder de geïnterviewden van de politie en het OM worden de juridische moeilijkheden omtrent het delen van informatie als één van de belangrijkste hindernissen gezien bij het aangaan en het verloop van succesvolle publiek-private samenwerkingen, zoals te lezen is in het volgende citaat van een respondent vanuit het OM:

'Strikt genomen is de wet zo opgebouwd dat – de wet politiegegevens – dat wij in een lopend onderzoek geen informatie mogen delen. Dus daarmee is het antwoord wel gegeven. Er is een hele grote hobbel om informatie te delen. Wat mij betreft ook een van de belangrijkste hobbels om weg te nemen omdat we met z'n allen wel moeten realiseren dat dit soort bedrijven over informatie beschikken en over tools en mensen beschikken die dingen beter kunnen dan wij. […] Het zit voornamelijk in dat de wet politiegegevens het besluit dat daar onder hangt zo algemeen van aard is dat die eigenlijk niet goed aansluit bij de praktijk van dit soort zaken waar je gewoon heel erg afhankelijk bent van samen optrekken. Ik roep al een tijdje en ik hoop dat daar in ieder geval politiek draagvlak voor komt dat ze zeggen: in dit soort zaken snappen we best dat je met bedrijven moet samenwerken.'

Er wordt door OM- en politiemedewerkers benadrukt dat cybercriminaliteit niet door de politie alleen kan worden aangepakt en dat de samenwerking met bedrijven en publieke partners zoals het NCSC, en daarmee het delen van informatie, cruciaal is. In de praktijk is dit volgens een politiemedewerker ook nadelig voor de opsporingsonderzoeken:

'Nu ook voor een zaak wil ik even kijken of ik één van die partijen kan laten invliegen, maar ja wat mag ik wel en wat mag ik niet delen. Dat maakt het gewoon zo verdomd lastig. Ik wil gewoon eigenlijk.. jullie zijn betrokken bij dit onderzoek, jullie kunnen gewoon naar alle data kijken. Maar dat kan niet zomaar. (…) Wat ik echt heel belangrijk vind is het delen van gegevens. Want dat is echt cruciaal binnen cybercrime, zeker internationaal maar ook dus landelijk zeg maar binnen private partijen. Dat is echt een ding. Daar lopen wij eigenlijk in elk onderzoek tegenaan. Van wat kunnen we nou wel en wat kunnen we niet. En veel kunnen we niet want dat mogen we niet delen of dat kan niet, en dat loopt vertraging op.'

Overige knelpunten
Overige knelpunten in de literatuur hebben betrekking op de verschillen die bestaan tussen de private en publieke sector op het gebied van cultuur, opvattingen en methodiek (zie Boes & Leukfeldt, 2017; Boonstra, 2007). Aangezien het verschil tussen de sectoren ook juist een reden is om de samenwerking aan te gaan, is het daadwerkelijke knelpunt de onmogelijkheid of onwelwillendheid om over deze verschillen heen te stappen.

De geïnterviewden uit zowel de private als de publieke sector hebben verder ook enkele losstaande knelpunten genoemd. Zo wordt de onoverzichtelijke internet-sector als een belemmering gezien, aangezien deze sector zeer omvangrijk is in zijn geheel. Dit zorgt ervoor dat het niet eenvoudig is om voor een criminaliteitsvorm 'alle' partijen in de keten bijeen te krijgen, aangezien er simpelweg te veel partijen zijn. Verder wordt genoemd dat men bij samenwerking waakzaam moet zijn voor trage beslissingsprocessen door te veel polderen, wegvallende interesse en gebrek aan tijd of investering van de betrokken partijen.

Een aantal geïnterviewden benoemen daarnaast knelpunten die expliciet betrekking hebben op de rol van de politie. Zo benoemt een politiemedewerker dat de 'afge-kaderde' politiementaliteit niet altijd bijdraagt aan het fundament voor een goede publiek-private samenwerking, waar juist ruimdenkende mensen voor nodig zijn. Een samenwerking met private partijen kan met een 'afgekaderde' mentaliteit bijvoorbeeld als eng of onwennig ervaren worden waarbij men snel bang is voor het afbreukrisico van lopende zaken. Dit knelpunt sluit aan bij de vraag naar een flexibele houding die eerder bij het onderdeel over de succesfactoren van PPS is omschreven. Verder wordt door een politiemedewerker het probleem genoemd dat de politie op regionaal niveau nog vrij klassiek is ingesteld op incident gedreven opsporingsonderzoek. Hierdoor zou er minder ruimte over zijn om samenwerkingen op te zetten die preventief van aard zijn om op deze manier meer te bereiken in het aanpakken van een criminaliteitsvorm.

Tot slot is in één van de samenwerkingsverbanden een voorbeeld naar voren gekomen waarbij een politieke situatie leidde tot een wegvallend vertrouwen en het tijdelijk stopzetten van een samenwerking. Alhoewel er op het gebied van de samenwerking tussen de partijen geen problemen waren en de politieke onrust ook niet over het samenwerkingsverband ging, heeft deze situatie ertoe geleid dat de betrokken private partij tijdelijk niet meer verder wilde. In dit voorbeeld wordt duidelijk welke invloed externe factoren kunnen hebben en dat de politieke context in acht genomen moet worden bij de beslissing om met partijen een samenwerking aan te gaan.

6 Dilemma's bij de aanpak van cybercriminaliteit

Om cybercriminaliteit effectief aan te pakken zijn zoals eerder beschreven verschillende beleidsdoelstellingen geformuleerd. Daarnaast zijn tijdens dit onderzoek diverse wensen uitgesproken door de opsporing. In een aantal gevallen leveren deze wensen en doelstellingen een spanningsveld op. In dit hoofdstuk worden een aantal dilemma's die spelen bij de aanpak van cybercriminaliteit op een rij gezet.

6.1 Informatiepositie politie

Door de schaalgrootte van cybercriminaliteit en het grote aanbod aan zaken moeten keuzes worden gemaakt ten aanzien van de zaken waar de opsporing op inzet. Om slim op te sporen en onderbouwde keuzes te maken is een goede informatiepositie belangrijk. Het OM en de politie mogen echter geen opsporingsbevoegdheden inzetten puur ten behoeve van het verbeteren van hun informatiepositie. Als informatie wordt veiliggesteld gebeurt dat vanuit een strafvorderlijke context. In het kader van de Wpg kan informatie eventueel wel, met toestemming, ook in andere onderzoek worden gebruikt. Deze uitgangspositie is soms lastig. Immers, als er goed zicht is op wat er speelt, is het onderzoeksteam ook beter in staat daar gericht op te reageren. Het belang van een goede informatiepositie om criminaliteit effectief aan te kunnen pakken wordt al langer benadrukt (zie Den Hengst, Ten Brink & Ter Mors,2017 voor een overzicht).

Eén van de gestelde beleidsdoelen voor de politie en het OM is dan ook het verbeteren van hun informatiepositie. De politie zou graag los van concrete onderzoeken samen met andere partijen (zoals andere opsporingsdiensten) activiteiten van (internationale) criminele groeperingen, *facilitators* en andere daders willen blijven monitoren om haar kennis over nieuwe werkwijzen actueel te houden. Sommige van deze daders zijn dusdanig professioneel en wereldwijd verspreid dat ze bijna niet door individuele landen kunnen worden aangepakt en internationale samenwerking vereist is. Andere groeperingen zijn meer fluïde van structuur of grootte. Een betere informatiepositie kan helpen om de juiste strategie te bepalen om een specifieke groepering of *facilitator* aan te pakken. Naast internationale samenwerking speelt, zoals in het vorige hoofdstuk uitgebreid is beschreven, ook publiek-private samenwerking een grote rol bij het verbeteren van de informatiepositie. Tot slot draagt ook het gebruik van het in hoofdstuk 3 beschreven CSAE-raamwerk bij aan een meer datagedreven aanpak van cybercriminaliteit door de politie. Door middel van dit werkproces wordt restinformatie uit (eerdere) onderzoeken en andere bronnen gebundeld en omgezet naar informatie die kan worden geanalyseerd ten behoeve van opsporingsonderzoeken. Zo kan gekeken worden of er verbanden kunnen worden gelegd tussen data uit verschillende onderzoeken om bijvoorbeeld na te gaan of er overeenkomsten zijn tussen betrokken personen of werkwijzen van groeperingen.

6.1.1 Kwantitatieve beleidsdoelstellingen

Om die informatiepositie op te bouwen is het dus onder andere van belang om cybercriminele fenomenen goed te kunnen doorgronden, bijvoorbeeld door het doen van zogenoemd fenomeenonderzoek, waarbij eenheidsoverstijgende cybercriminele fenomenen en dadergroepen centraal staan en breder worden onderzocht. Hier is

ook ruimte voor gemaakt in de Veiligheidsagenda. Deze vaak meerjarige onderzoeken kosten echter veel tijd en capaciteit en de resultaten van deze onderzoeken zijn vaak (vooral) gelegen in het tegenhouden en verstoren van cybercriminaliteit en minder op vervolgen van daders (als deze al geïdentificeerd kunnen worden). De minder goed meetbare alternatieve of tegenhouddoelen schuren soms met de resultaatverplichtingen in de veiligheidsagenda. Met name in de eenheden hebben 'zaken met bloed spoed', waardoor die voor cybercrimezaken gaan. Daarnaast kan het bij cybercrimezaken soms aantrekkelijker zijn om in te zetten op het oppakken van geldezels die onderdeel zijn van een crimineel samenwerkingsverband om zodoende meerdere afgeronde onderzoeken aan te leveren en te voldoen aan de kwantitatieve doelstellingen in de Veiligheidsagenda, dan meer tijd en middelen te steken in het identificeren en aanhouden van één of twee verdachten die hoger in de hiërarchie van een crimineel samenwerkingsverband zitten. Ook kan het aantrekkelijker zijn om capaciteit in te zetten voor het oppakken van makkelijk te pakken te krijgen verdachten in plaats van in te zetten op tegenhoudmaatregelen terwijl die mogelijk wel een groter effect hebben in een specifieke casus. De kennis die met een uitgebreider opsporingsonderzoek kan worden opgedaan over het specifieke fenomeen en de werkwijze van de daders kan in vervolgonderzoek worden gebruikt om efficiënter op te sporen en om belangrijke infrastructuren, hoofdverdachten en/of *facilitators* te identificeren.
De keus tussen voldoen aan kwantitatieve doelen of het vergroten van de kennispositie is niet altijd zo zwart-wit, maar zorgt in de praktijk toch regelmatig voor een worsteling, zowel bij officieren van Justitie als voor politiemedewerkers. In onderstaande tekst volgen hiervan twee voorbeelden van respectievelijk een officier van justitie en een politiemedewerker:

> *'Ja dat vind ik ook heel moeilijk. Ik vind wel, maar ik heb daar het antwoord niet op, maar dat we daar wel slimmer over na moeten denken (..). Dat willen wij ook vanuit […] graag. Kijk want de definitie van fenomeenonderzoek is natuurlijk ook heel globaal. Ja dan weet je nog niet of iets maatschappelijke impact heeft gehad, terwijl dat is waar het om moet gaan natuurlijk. En tegelijk vind ik die streepjes zetten op parketnummers, dus het aantal verdachten, vind ik ook best wel suffig. Die kun je makkelijk scoren met hele kleine feitjes die ook geen maatschappelijke impact hebben. Maar aan de andere kant snap ik ook wel vanuit het ministerie dat je wilt sturen op cijfers of iets, want anders is het ook heel erg lastig om iets gedaan te krijgen.'*

> *'Ja zeker, en dat is besproken, (…) van dat het gewoon veel beter zou zijn om impactanalyses te doen op verdachten. Want dat vertelt veel meer over de impact die je kunt hebben op een bepaald fenomeen. Alleen je moet er wel over nadenken. Uiteindelijk wordt men aangerekend op het aantal verdachten. Dus je moet in de loop van je onderzoek gaan denken, ik moet die 17, of ja het worden er ieder jaar steeds meer, die moet je aanleveren bij het OM. Dus dat is wel een groot probleem. (…) ook qua capaciteit is het heel moeilijk om mensen te krijgen om dit uit te voeren.'*

6.1.2 Juridische problemen bij het opbouwen van een betere informatiepositie

Naast de vraag of er met de kwantitatieve resultaatverplichtingen voldoende ruimte is om capaciteit te steken in het opbouwen van een verbeterde informatiepositie is een andere vraag hoe ver de politie mag gaan om haar eigen informatiepositie te verbeteren. De politie heeft, in tegenstelling tot inlichtingen- en veiligheidsdiensten,

geen bevoegdheid om opsporingsmiddelen in te zetten puur ten behoeve van het verkrijgen van een betere informatiepositie. Het dilemma is dat een goede informatiepositie voor de opsporing erg belangrijk is, maar dat deze formeel alleen kan worden gecreëerd door het uitvoeren van opsporingsonderzoeken, die zich weer moeten richten op vervolging en niet op informatievergaring of tegenhoudmaatregelen.

De informatiepositie die de politie nu heeft is daarom vooral ad hoc en gefragmenteerd. Voor het verbeteren van de informatiepositie wordt nu deels geleund op PPS, deels op clustering van kennis en *books of crime* en deels op de datagedreven methodiek van het CSAE-raamwerk. Bij PSS zijn echter een aantal belangrijke kanttekeningen te plaatsen, zoals ook al beschreven in hoofdstuk 5. Zo hebben private partijen geen wettelijke taak of opsporingsbelang en hebben zij te maken met andere wet- en regelgeving als het gaat om het delen van informatie dan de politie. Verder hebben private partijen een commercieel belang en zijn de politie en het OM afhankelijk van wat partijen kunnen en willen delen.
Een ander punt is dat data maar een beperkte periode mag worden gebruikt. Geïnterviewden geven aan dat het kunnen bewaren van data van belang is voor het opbouwen van een informatiepositie, omdat in de opsporingspraktijk wordt gezien dat dezelfde verdachten, soms in wisselende samenstellingen, jarenlang actief zijn.

Het is nu daarom soms zoeken wat de juiste juridische grondslag is wat betreft het verzamelen van informatie en het verwerken van die data. In principe mogen BOB-middelen alleen worden ingezet als dat ten behoeve van opsporing en vervolging is en niet met als enkel doel om de informatiepositie te verbeteren. De Wpg geeft de wettelijke basis voor het verwerken van politiegegevens om na te gaan of er verbanden bestaan tussen deze gegevens. Indien zulke verbanden bestaan kunnen de gerelateerde gegevens, na instemming van een daartoe bevoegde functionaris, wel worden gebruikt voor een andere verwerking zoals een opsporingsonderzoek.

Verschillende geïnterviewden merken op dat het wettelijk kader nu niet toereikend is als het gaat om informatieverzameling. Wat met name lastig is zijn online informatieknooppunten die niet overduidelijk crimineel zijn, maar waar wel relevante informatie op te vinden is. Zoals een technisch forum met een kleine subpagina over *hacking*. Er is geen duidelijk kader dat voorschrijft hoe met dat soort informatie mag worden omgegaan. Dat komt ook omdat de Nederlandse opsporing, in tegenstelling tot bijvoorbeeld Groot-Brittannië of de Verenigde Staten, geen aparte intelligence tak heeft die zich richt op het verstevigen van haar informatiepositie.

6.2 Informatie-uitwisseling

Informatie-uitwisseling is van groot belang bij de aanpak van cybercriminaliteit. Zowel strategisch bij het opbouwen van een goede informatiepositie, als op individueel niveau bij opsporingsonderzoeken. Dit geldt zowel nationaal als internationaal en voor het opsporen en tegenhouden van cybercriminaliteit. Toch zitten hier in een aantal gevallen haken en ogen aan. Wat wel en niet gedeeld kan worden is soms een grijs gebied. Er is behoefte aan duidelijkere of herziene (juridische) kaders rondom het delen van informatie. In hoofdstuk 5 zijn de knelpunten bij publiek-private samenwerking al uitbereid toegelicht. Hieronder volgen een aantal andere voorbeelden van situaties waarbij informatie-uitwisseling niet altijd vlekkeloos verloopt.

6.2.1 Nationaal

Zoals in hoofdstuk 5 al uitgebreid is beschreven, wordt de privacywetgeving door de opsporing als groot knelpunt gezien bij de samenwerking met andere partijen, omdat het de mogelijkheden tot informatiedeling inperkt en daarmee de mogelijkheid tot handelen. Informatie over modus operandi van criminelen is vaak wel probleemloos te delen, maar persoonsgegevens niet. Ook IP-adressen en domeinnamen worden als persoonsgegevens gezien.
Op basis van artikel 19 van de Wpg mogen onder bepaalde omstandigheden incidenteel politiegegevens worden gedeeld met derden, maar alleen als er een zwaarwegend belang is. Artikel 19 verstrekkingen worden dan ook niet makkelijk goedgekeurd, ook omdat betrokkenen op voorhand genotificeerd moeten worden over deze verstrekking. Dat is niet altijd wenselijk in de opsporing en bij cyberzaken extra lastig omdat vaak niet duidelijk is welke persoon of bedrijf achter een IP-adres zit. Daarnaast is het – ook als dit wel duidelijk is – praktisch gezien niet altijd haalbaar. Het komt voor dat er honderdduizenden slachtoffer IP-adressen in één databatch zitten en dat deze slachtoffers zich verspreid over de hele wereld bevinden. Ook de betrokken verdachten zouden op basis van de eisen in artikel 19 Wpg op de hoogte moeten worden gebracht.

Eén van de maatregelen die is aangekondigd in de Nederlandse Cybersecurity Agenda is om het landelijk cyberbeeld 'te versterken met de inrichting van een samenwerkingsplatform om op die manier binnen de wettelijke kaders meer en sneller handelingsperspectief met belanghebbende organisaties te kunnen delen' (NCSA, 2018, p. 20). In juni 2020 is het nieuwe samenwerkingsverband met de naam Cyber Intel/Info Cel (CIIC) gestart.[100] Het platform moet ervoor moet zorgen dat de inlichtingendiensten samen met justitie en politie sneller informatie kunnen uitwisselen. In de praktijk bleek namelijk dat er door verschillende partijen regelmatig informatie werd verzameld die niet altijd op de juiste plek terecht kwam. Naast politie en justitie werken ook het Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Cyber Security Centrum (NCSC) aan het platform mee. De AIVD is de juridisch verantwoordelijke van het platform. De CIIC valt daarmee onder de Wet op de inlichtingen- en veiligheidsdiensten (Wiv)[101]. De leden van de CIIC zijn formeel ondergebracht bij de AIVD om aan de voorwaarden van informatiedeling onder de WIV te kunnen voldoen. Er vindt structureel overleg plaats waardoor de informatie die gedeeld wordt bij elkaar kan worden gelegd en besloten kan worden of het nodig is deze informatie te delen tussen de leden. Om dit te faciliteren zitten de leden van de CIIC fysiek bij elkaar op een gedeelde locatie. Namens de politie neemt de inlichtingendienst van de Landelijke Eenheid (IDLE) aan het overleg deel. Vanuit OM is in deeltijd een beleidsadviseur aanwezig vanuit team inlichtingen. De insteek van het platform is vooral om op operationeel niveau informatie te delen. Deze informatie blijft dan binnen het platform. Voor de opsporing kan worden gedacht aan IP-adressen, *nicknames*, maar ook *malware-samples* en meldingen van slachtoffers. De CIIC is er dan vooral voor bedoeld om het grijze gebied op te klaren wanneer niet duidelijk is vanuit welke hoek een dreiging afkomstig is en het bijvoorbeeld zowel zou kunnen gaan om een statelijke actor, als om een criminele groepering.

[100] *Staatscourant* 2020, 30702 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)

[101] De Wet op de inlichtingen- en veiligheidsdiensten (Wiv) beschrijft de rechten en plichten van de AIVD (en MIVD).

6.2.2 Internationaal

Bij de aanpak van cybercriminaliteit is men in veel gevallen afhankelijk van internationale samenwerking. Zelfs aan de kleinere zaken zit vaak een internationaal component, waardoor er een rechtshulpverzoek moet worden ingediend en men afhankelijk is van informatiedeling van andere landen. De rechtshulpverzoeken zijn een 'enorm geouwehoer en getouwtrek', aldus een politiemedewerker. Als een land niet bereid is om mee te werken aan een verzoek kunnen de opsporingsdiensten met lege handen komen staan.

Wanneer een land wel bereid is gehoor te geven aan het verzoek is een veelgenoemd probleem de wisselende doorlooptijd van de rechtshulpverzoeken. In het cybercrimeverdrag is geregeld dat landen die dit verdrag hebben ondertekend binnen een bepaalde termijn na binnenkomst van het verzoek hier uitvoering aan moeten geven. Dat betekent echter niet dat de informatie daarmee meteen is vrijgegeven en ook is overhandigd aan het onderzoeksteam. Elk land heeft maar beperkte rechtshulpcapaciteit. Dat geldt ook voor Nederland. Eén van de geïnterviewden geeft ook aan dat het voor veel landen zo moeilijk is om aan de vele verzoeken te voldoen dat ze 'op de grote stapel' terecht komen. De harde realiteit is dan dat men in sommige gevallen pas reageert op het moment dat de informatie al lang weg is.

In de interviews komt naar voren dat de internationale samenwerking verbeterd is ten opzichte van een aantal jaar geleden, omdat er meer kennis in diverse landen is en ook de contacten met veel landen steeds beter worden. Dit heeft er bijvoorbeeld voor gezorgd dat de nationale politie tijdelijk beschikte over een Nederlandse cyberliaison om de Nederlandse belangen te behartigen. Andersom is er ook een vertegenwoordiger van de FBI aanwezig op de VS-ambassade in Nederland. Deze FBI-liaison ondersteunt THTC met de rechtshulpverzoeken en houdt contact over internationale politiesamenwerking tussen Nederland en de VS.

6.2.3 Slachtoffernotificatie

Een ander onderwerp waarbij de beperkingen rondom het delen van informatie als probleem worden gezien, is slachtoffernotificatie. In een aantal bestudeerde opsporingsonderzoeken kwam het opsporingsteam gedurende het onderzoek gegevens tegen van grote aantallen slachtoffers. Deze personen wilde men notificeren om ze erop te wijzen dat hun gegevens waren buitgemaakt bij bijvoorbeeld een *hack*, vertellen dat hun systemen waren gecompromitteerd, of waarschuwen voor een aanstaande cyberaanval. Dat notificeren gebeurt als het aan de politie en het OM ligt bij voorkeur via een partij als een (nationale) CERT,[102] omdat het notificeren en verschaffen van informatiebeveiligingsadviezen wordt gezien als een vak apart. Het notificeren bleek in een aantal gevallen om verschillende redenen problematisch.

Ten eerste is het NCSC belast met het notificeren van vitale infrastructuur en Rijksoverheid, maar het is op dit moment niet goed geregeld wie verantwoordelijk is voor het delen van informatie aan partijen die buiten de vitale structuur vallen. Hier werkt de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) en de wijze waarop deze wordt geïnterpreteerd niet altijd even goed mee. De constatering dat het delen van (dreigings)informatie met niet-vitale partijen een struikelblok is en er

[102] Computer Emergency Response Team. In Nederland is dit het NCSC.

door de strikte scheiding van vitale en niet-vitale partijen ook veel bedrijven of instanties tussen wal en schip vallen, wordt ook beschreven in een recent rapport van Brennenraedts et al. (2020) en artikel van De Poot en McKim (2020).
Een tweede probleem speelt bij slachtoffernotificatie via een derde partij als het NCSC. Als de politie slachtoffergegevens tegenkomt mag zij rechtstreeks de betrokkenen notificeren, omdat er dan geen informatieverstrekking aan derden plaatsvindt. In individuele gevallen heeft de politie voldoende middelen om dit te doen. Bij een *hack* zijn echter regelmatig tienduizenden tot honderdduizenden IP-adressen (wereldwijd) buitgemaakt en dan zijn de middelen bij de politie te beperkt om zelf te notificeren. Een derde partij zou in deze situaties uitkomst kunnen bieden. Notificatie via een derde partij kan echter alleen met een artikel 18, 19 of 20 Wpg-verstrekking. Naast het feit dat er dus op dit moment geen duidelijke derde partij is die slachtoffernotificatie namens de politie op zich kan nemen, is men sinds een arrest van de Raad van State ook huiverig voor het beroepen op artikel 19 Wpg, omdat de politie alle betrokken partijen op voorhand moet notificeren over die verstrekking aan de derde partij. Wanneer er een slachtofferlijst is met duizend IP-adressen is het voor de politie onwerkbaar om die allemaal te notificeren voordat ze aan een derde partij als een nationale CERT overhandigd gaan worden en kan dus niet aan de notificatie-eis uit het arrest van de Raad van State worden voldaan. Bovendien is het erg omslachtig om partijen te moeten notificeren dat ze genotificeerd gaan worden. Tot slot kan het dan ook zijn dat de criminele groepering zelf genotificeerd wordt wat het opsporingsonderzoek weer kan verstoren. Ten derde speelt nog mee dat gegevens uit lopende strafrechtelijke onderzoeken in principe niet gedeeld mogen worden. Wanneer tijdens een lopend onderzoek te zien is dat cybercriminelen nog in de ICT-systemen zitten zou men misschien een slachtoffer daarop willen attenderen. Maar daar kleven nu veel praktische en juridische bezwaren aan.

De problemen rondom slachtoffernotificatie speelden ook in één van de opsporingsonderzoeken. Men kwam er als bijvangst achter dat er een actuele dreiging was voor Nederlandse universiteiten. Op basis van deze informatie wilde THTC de getroffen instellingen notificeren. De wens was om dit via het NCSC te doen, omdat deze partij betere nazorg kon leveren en de slachtoffers kon voorzien van informatie over bijvoorbeeld preventie, beveiliging en schadebeperking. Universiteiten vallen echter niet onder vitale infrastructuur waardoor het notificeren problematisch was en onnodig lang heeft geduurd. Uiteindelijk zijn de betrokken universiteiten door het Landelijk Parket genotificeerd omdat het om een overzichtelijk aantal ging. Deze procedure is echter niet wenselijk voor het OM als structurele oplossing en had ook niet gekund bij een groot aantal slachtoffers. Ook voor het OM geldt dat de middelen hiervoor te beperkt zijn.

In het voorjaar van 2021 speelde een casus waarin een andere oplossing werd gekozen voor dit probleem. Tussen de in beslag genomen gegevens die zijn verzameld voor operatie *Ladybird*, naar het gebruik van Emotet *malware*, vond de politie ook buitgemaakte e-mailadressen, gebruikersnamen en wachtwoorden. In plaats van die gebruikers actief te benaderen heeft de politie ervoor gekozen een website open te stellen waarop mensen hun eigen e-mailadres kunnen vullen om te controleren of dat overeenkomt met de inbeslaggenomen inlog-gegevens.[103]
Ondanks het feit dat men dus actief op zoek gaat naar oplossingen voor de hierboven geschetste moeilijkheden, zijn ze daarmee niet verdwenen.
In het geval van de hiervoor geschetste oplossing konden alleen individuele mailadressen worden ingevoerd en geen hele *batches* van of door bedrijven, wat het

[103] Controleer of uw e-mail en wachtwoord gestolen zijn door de Emotet malware | politie.nl

proces alsnog bewerkelijk maakte. Voor de problematiek rondom notificeren blijft het daarom van belang dat er een meer structurele oplossing komt.

7 Slotbeschouwing

Het doel van dit onderzoek was om meer inzicht te krijgen in de aanpak van geavanceerde vormen van cybercriminaliteit door politie en OM. Daarnaast is gekeken in hoeverre het opsporingsonderzoek bijdroeg aan een betere informatiepositie jegens (in het online domein vaak anonieme) verdachten en hun modus operandi en hoe deze informatie kon worden gebruikt om acties te verrichten, die niet alleen gericht zijn op opsporing en vervolging van verdachten maar ook op het tegenhouden van illegale online activiteiten. Voor de meest complexe opsporingsonderzoeken naar cybercriminaliteit beschikt de politie op landelijk niveau over het specialistische Team High Tech Crime (THTC). Dat is dan ook het team waar voor dit onderzoek de meeste gegevens zijn verzameld. Daarnaast heeft elke eenheid een eigen cybercrimeteam. De bedoeling is dat ook deze teams in de toekomst nog meer complexe onderzoeken kunnen doen en dat kennis over cybercriminele fenomenen en werkwijzen wordt gebundeld.

Zoals in de inleiding is beschreven heeft de Kamer de ambitie uitgesproken om cybercriminaliteit meer integraal aan te pakken. Uit het onderzoek blijkt dat deze integrale aanpak binnen de opsporing ook terug te zien is. Zo zijn in aansluiting op THTC van de landelijke eenheid de multidisciplinaire cybercrimeteams in de andere eenheden verder geprofessionaliseerd. Verder wordt in de opsporingsonderzoeken naast het opsporen en vervolgen van daders van cybercriminaliteit ook actief gezocht naar andere manieren om impact te hebben op criminele activiteiten, bijvoorbeeld door de inzet van tegenhoudmaatregelen. Ook wordt er veel gebruikgemaakt van samenwerkingen met buitenlandse opsporingsdiensten en private partijen, zowel in afzonderlijke onderzoeken, als in meer structurele vorm.

In dit onderzoek zijn een aantal factoren naar voren gekomen die bijdragen aan een succesvolle aanpak van cybercriminaliteit. Daarnaast zijn er factoren naar voren gekomen die belemmerend werken. Deze succesfactoren en knelpunten worden in onderstaande paragrafen nader toegelicht.

7.1 Succesfactoren

Meerdere keren is benoemd door respondenten dat het waardevol is om te werken met multidisciplinaire teams bij de aanpak van cybercriminaliteit, zoals THTC dit al langer doet. Men kan van elkaar leren en elkaar helpen om breed te kijken, terwijl iedereen hetzelfde einddoel voor ogen heeft. Zo hebben tactische mensen bijvoorbeeld het bredere opsporingsperspectief scherper in beeld en de technische mensen hebben beter zicht op de technische mogelijkheden die er zijn om informatie te vergaren of met elkaar te verbinden.

Het internationale karakter van cybercriminaliteit wordt vaak als een belangrijk knelpunt gezien omdat het de opsporing bemoeilijkt. Met verschillende Europese opsporingsdiensten, zoals in Engeland en Duitsland, wordt door THTC echter veelvuldig en goed samengewerkt. Datzelfde geldt voor de Amerikaanse FBI. Daarbij kan gedacht worden aan het verkrijgen van opsporingsinformatie, het gecoördineerd opsporen en aanhouden van verdachten en het gecoördineerd ontplooien van verstoringsactiviteiten. Men is niet terughoudend om elkaar op te

zoeken. Ook de aanwezigheid van een cyberliaison helpt hierbij, omdat het de lijnen in de communicatie korter maakt. Verder wordt de samenwerking met private partijen in veel gevallen gezien als een waardevolle toevoeging omdat men van elkaars kennis, kunde, informatiepositie en netwerk kan profiteren.

In de praktijk blijkt dat Nederlandse servers regelmatig worden gebruikt voor criminele activiteiten. Dit zijn vaak informatieknooppunten met veel waardevolle opsporingsinformatie. Hoewel de aantrekkelijkheid van de Nederlandse infrastructuur voor criminele activiteiten op zich niet per se een positief punt is, geeft het de Nederlandse opsporingsdiensten wel de mogelijkheid doortastend te werk te kunnen gaan in onderzoeken.

Tot slot is het belang van een meer datagedreven of 'intelligentere' opsporing vaak aangehaald. Het type zaak waar de teams binnen THTC aan werken komt vaak niet op basis van een aangifte binnen. De zaken die door politie en OM als de grootste successen werden gezien zijn pro-actief opgestart, bijvoorbeeld door tips van private partijen of buitenlandse opsporingsdiensten actief op te volgen en uit te zoeken, of door gebruik te maken van de analyses van eerder onderzoeksmateriaal met behulp van het CSAE-raamwerk. Daarnaast onderscheiden deze zaken zich door het feit dat het zaken zijn waarbij de tijd is genomen om te achterhalen wat de grootste dreiging was of wie de kopstukken achter een aanval waren zodat die opgepakt konden worden. Dat kostte tijd en capaciteit, maar had vaak wel het beoogde resultaat. Het achterhalen van kopstukken hoeft niet altijd te leiden tot vervolging, ook het enkel vaststellen welke groepering achter een aanval zit kan helpen bij vervolgonderzoek of de inzet van tegenhoudmaatregelen.

7.2 Knelpunten en eerder onderzoek

Hoewel goede internationale samenwerking successen kan brengen, wordt de lange doorlooptijd van internationale rechtshulpverzoeken als één van de grootste knelpunten genoemd. Er is grote variatie in hoe lang een team moet wachten op de resultaten van zo'n verzoek. Dit sluit aan bij eerdere bevindingen van Odinot et al. (2017). Geïnterviewden in dat onderzoek waren positief over de rol van Europol, maar zeiden ook dat het succes sterk afhankelijk was van de capaciteit en prioriteiten in samenwerkende landen. Rechtshulpverzoeken werden 'behandeld met een tempo dat onverenigbaar is met de snelheid van het internet' (Odinot et al., 2017, p. 81). Dat beeld lijkt niet wezenlijk veranderd ten tijde van de uitvoering van ons onderzoek.

Een ander knelpunt dat werd genoemd in het onderzoek van Odinot et al. (2017) waren de gebrekkige mogelijkheden tot identificatie en vervolging. Met name wanneer het ging om buitenlandse daders. In het huidige onderzoek zijn bij vijf van de acht zaken wel verdachten aangehouden. Dat lijkt dus niet helemaal te stroken met beeld dat uit eerder onderzoek naar voren komt. Hierbij moet echter opgemerkt worden dat voor dit onderzoek dossiers zijn aangedragen waarbij een goed beeld van de besluitvorming tijdens het traject van opsporing en vervolging en tegenhouden kon worden verkregen. Dat zijn dus niet de onderzoeken die al in een eerder stadium spaak liepen vanwege daders die niet te identificeren of vervolgen waren. Uit eerdere onderzoeken naar georganiseerde criminaliteit is bekend dat ongeveer de helft van de zaken geen succesvolle vervolging oplevert (Bokhorst et. al., 2011). Ook tijdens de gesprekken die zijn gevoerd voor ons onderzoek is door geïnterviewden benoemd dat vooral de *hightech* crime groepen die opereren in het

buitenland bijzonder moeilijk aan te pakken zijn. Wat niet expliciet aan bod is gekomen tijdens het onderhavige onderzoek, maar mogelijk wel een verschil is tussen vervolgingsproblemen bij cybercriminaliteit en andere vormen van georganiseerde criminaliteit, is dat het bij cybercriminaliteit vaak wel duidelijk is wat de criminele handelingen zijn, maar dat het vooral lastig is om de verdachte te identificeren. Bij traditionele georganiseerde criminaliteit is dat vaak precies andersom, er is vaak wel een aardig beeld van wie betrokken zijn bij een crimineel samenwerkingsverband en bij criminele activiteiten, maar het bewijzen van criminele handelingen is lastig.

Wat niet in eerder onderzoek naar voren kwam, maar in dit onderzoek wel nadrukkelijk wordt genoemd zijn de problemen rondom (nationale) informatiedeling. Ten eerste bij slachtoffernotificatie. Er is op dit moment geen duidelijke partij die daar verantwoordelijk voor is. De hoeveelheid slachtoffers van bijvoorbeeld een *hack* is regelmatig zo groot dat de opsporing het notificeren van deze slachtoffers er niet zomaar bij kan doen. Daarbij is het proces van notificeren complex. Vaak zijn abstracte datasets zoals lijsten met IP-adressen het uitgangspunt. Deze moeten worden geduid. Uit welke land zijn ze afkomstig? Van welke organisatie? Gaat het om vitale infrastructuur? Vervolgens moeten de slachtoffers via de juiste kanalen worden bereikt. Als men de slachtoffers heeft kunnen contacteren zullen ze vragen hoe ze hun systemen weer veilig kunnen krijgen. Dat reikt buiten de taakstelling en expertise van de politie. Verder kan het delen van deze informatie juridisch lastig zijn. Wat in de praktijk logisch en voor de hand liggend lijkt om te doen, blijkt juridisch niet altijd haalbaar. Dit zorgt voor onduidelijkheid en inefficiëntie. In één van de bestudeerde onderzoeken betekende dit dat meerdere Nederlandse partijen later werden genotificeerd dan wenselijk was en dat het notificeren via een lastige omweg plaatsvond. Daardoor zijn deze Nederlandse partijen onnodig langere tijd blootgesteld aan potentieel gevaar.

Ten tweede spelen problemen rondom informatiedeling bij publiek-private samenwerking. Een samenwerking met private partijen biedt de mogelijkheid om andere expertise in de aanpak van cybercriminaliteit te brengen en extra informatie te vergaren voor zowel de politie als de private partij. Toch kleven hier ook praktische bezwaren aan. Publieke en private partijen hebben andere, en mogelijk tegenstrijdige, belangen. Het is goed als partijen zich hier gedurende de gehele looptijd van de samenwerking bewust van te zijn. Ook kan de wet- en regelgeving omtrent het delen van informatie een samenwerking bemoeilijken. Zo heeft men naast de Wet Politiegegevens (Wpg) ook te maken met de Algemene Verordening Gegevensbescherming (AVG), Wet Beveiliging Netwerk- en Informatiesystemen (Wbni), de Wet Bescherming Persoonsgegevens (Wbp) en eventueel geheimhoudingsplichten. Hoewel het goed is om enige mate van terughoudendheid te hanteren bij het delen van informatie kan onduidelijkheid bij partijen over de wetgeving tot gevolg hebben dat er te terughoudend wordt omgegaan met het delen van informatie.

7.3 Tot besluit

Bij de vormen van cybercriminaliteit die voor dit onderzoek zijn bestudeerd, is het opsporen van verdachten geen sinecure. Daders kunnen goed anoniem opereren en zijn in staat hun identiteit en de locatie van waaruit ze werken goed af te schermen. Dat levert extra problemen op bij de aanpak van dit type criminaliteit. In lang niet alle zaken lukt het om daders op te sporen en te vervolgen, en dus via het strafrecht op deze criminaliteitsvormen te reageren. De aanpak is daarom niet alleen

gericht op opsporing en vervolging, maar ook op het verstoren en tegenhouden van deze vormen van criminaliteit. Het valt op dat in alle bestudeerde zaken waarin verdachten in beeld kwamen en konden worden vervolgd, ook gebruik is gemaakt van de inzet van bevoegdheden die vallen onder werken onder dekmantel. Dit is opvallend gezien de terughoudendheid die doorgaans bij de inzet van deze bijzondere opsporingsbevoegdheden wordt betracht (Kruisbergen & De Jong, 2010). Deze bevinding sluit echter wel aan bij het vergelijkbare beeld dat wordt geschetst in het rapport van Odinot et al., (2017) en roept de vragen op of dit alleen te maken heeft met de zwaarte van de delicten, of dat er bij de aanpak van cybercriminaliteit behoefte is aan een andere manier van werken door de opsporingsdiensten die om nadere gedachtenvorming vraagt over de inzet en zwaarte van al bestaande opsporingsbevoegdheden.

Dit onderzoek laat zien dat het steeds belangrijker wordt om (cyber)criminele fenomenen te begrijpen om zo effectief en efficiënt mogelijk in te kunnen grijpen. Dat roept de vraag op of de fundamentele taak van politie en het OM zoals die nu is geformuleerd toereikend is (zie ook Stol, 2020) en of de huidige juridische grondslagen voor het verzamelen, verwerken en analyseren van informatie afdoende zijn voor een meer datagedreven aanpak van cybercriminaliteit. Als het opsporen en vervolgen van daders het uitgangspunt is, dan is het inzetten van opsporingsmiddelen geen probleem. In de praktijk is opsporen en vervolgen van daders echter niet altijd haalbaar en wordt er daarom ook voor gekozen om tegenhoudmaatregelen in te zetten. Het niet uitsluitend inzetten op opsporen en vervolgen bij de aanpak van cybercriminaliteit betekent ook dat soms in juridisch opzicht een grijs gebied wordt opgezocht. Bijvoorbeeld bij de inzet van opsporingsmiddelen tijdens een onderzoek, terwijl eigenlijk al duidelijk is dat dit niet zozeer een opsporingsdoel, als wel een verstoringsdoel dient. Of bij het verrichten van een opsporingsonderzoek om zicht te krijgen op de modus operandi van een criminele groepering. Het is op voorhand niet altijd duidelijk welke informatie in een opsporingsonderzoek kan worden vergaard, en in hoeverre opsporing en vervolging tot de mogelijkheden behoort. Maar het is ook niet altijd duidelijk wat de juridische grondslag is voor deze meer informatie vergarende manier van onderzoek doen als opsporing en vervolging minder haalbaar lijkt. Dit vraagt om een bredere discussie over slimme omgang met informatie en over de rol van politie en OM bij criminaliteitsbestrijding. Met name speelt hierbij de vraag of de rol van het OM zich zou moeten beperken tot opsporing en vervolging. Als al bij de start van een onderzoek duidelijk is dat de kans op attributie klein is, maar er wel een groot effect gesorteerd kan worden door opsporingsmiddelen in te zetten ten behoeve van tegenhoudmaatregelen en men is het erover eens dat dit de beste manier is om een dader of fenomeen aan te pakken, dan vraagt dat misschien om aangepaste wetgeving. Tot slot roepen de bevindingen in dit rapport de vraag op of de huidige wet- en regelgeving rondom informatiedeling toereikend is voor de aanpak van cybercriminaliteit. Er lijkt behoefte te zijn aan duidelijkere kaders op basis waarvan informatie kan worden gedeeld, zodat als er urgentie is belangrijke informatie ook snel kan worden gedeeld.

De beantwoording van dit soort vragen strekt verder dan de reikwijdte van dit rapport. Uit dit onderzoek blijkt echter wel dat thema's zoals de omgang met informatie en de weging en inzet van bijzondere opsporingsbevoegdheden bij de aanpak van cybercriminaliteit nadere aandacht vanuit de politiek behoeven en mogelijk om aanvullende wet- en regelgeving vragen.

Summary

Investigating, prosecuting and obstructing cybercrime

The Netherlands has a fast, stable and reliable digital infrastructure that is heavily used, both domestically and internationally. This gateway position offers economic opportunities, but also creates obligations. Illegal activities take place on Dutch servers or are knowingly or unknowingly facilitated by web hosting companies based in the Netherlands.
To investigate cybercrime, the Dutch police have set up the specialised National High Tech Crime Unit (NHTCU) (*Team High Tech Crime*, *THTC*) at the national level, as well as specialised cybercrime teams at the regional level. The cybercrime teams work together with the NHTCU in a national structure and support the regional crime squads and local teams in building knowledge to assist with standard criminal investigations into cybercrime.
As investigating and prosecuting perpetrators of cybercrime can be difficult for several reasons, the police and the Public Prosecution Service sometimes opt for alternative interventions outside of the criminal investigation process when tackling cybercrime. Examples of such alternative interventions are disrupting criminal activities by taking servers offline, as well as focusing on prevention through public awareness campaigns, such as the recent Dutch campaign warning against WhatsApp fraud. In addition, public-private partnerships are sought on an ongoing basis and various projects have been launched to help counter various cybercrime offences.

The aim of this study was to gain more insight into the approach by the police and the Public Prosecution Service to complex types of cybercrime. In addition, this study has examined to what extent criminal investigations have helped to improve the information position in relation to suspects (who are often anonymous in the online domain) and their modus operandi, and how this information could be used not only to track down and prosecute suspects, but also to put a stop to illegal online activities.

Research methods

We used various research methods to answer the research questions. By reviewing the relevant literature and conducting desk research, we gathered background knowledge to gain an overview of the approach used to tackle cybercrime.
In addition, we analysed police files of criminal investigations into high-tech cybercrime. For this purpose, we examined eight files of completed police investigations from the period 2014-2018. Seven of those files were made available by the NHTCU, and one was made available by a cybercrime team at the regional level. We also studied three public-private partnership projects.
At the start of the study, a meeting was organised with a number of experts from the police and the Public Prosecution Service. We asked them to compile a list of high-tech criminal investigations. As this study was aimed at gaining more insight into the possibilities and dilemmas the police and the Public Prosecution Service encounter in their approach to cybercrime, we also asked them about criminal

investigations affected by bottlenecks identified in previous research on organised cybercrime. By examining the police files, we determined which methods were used during the criminal investigations, how the investigations proceeded and what results they produced.
Lastly, we conducted forty-two interviews with police officers, public prosecutors specialised in cybercrime and employees of private parties to gain a more complete picture of the approach to cybercrime. Our interviews with public prosecutors and police team leaders who handled the selected cases enabled us not only to ask overarching questions, but also to gain more insight into information and considerations that may not have ended up in a file but did play a role in the choices they made during the investigation. The interviews also provided an insight into the dilemmas and problems the police encounter.

The bulk of the data was collected by the NHTCU, as this team mainly investigates the type of cases that fall within the scope of our study.

Results: criminal investigations into cybercrime

In contrast to the regional cybercrime teams, almost none of the investigations of the NHTCU were started in response to a police report. Although in theory it is possible for the NHTCU to launch an investigation on the basis of a police report, in practice high-tech crime is rarely reported to the police. This state of affairs was also reflected in the files we examined for this study. The only investigation that started in response to a criminal police report was a case at a regional unit. Of the seven NHTCU investigations we examined, six were started following a tip-off from a private party and/or an alert from a foreign police force.
As the number of cases exceeds the investigation capability of law enforcement, choices have to be made about which cases are taken up by the investigation services. Whether a case is taken up depends both on the policy priorities that have been set and on the seriousness of a case.
Although the primary aim of a criminal investigation is to track down and prosecute suspects, an investigation can also be started from a more strategic point of view; for instance, to gain more knowledge about a cybercrime phenomenon or a particular criminal modus operandi, to be better able to investigate and stop this form of cybercrime. Sometimes investigations do not even target cybercrime in the narrowest sense of the word but types of crime related to it, such as a case involving encrypted communication. One reason for taking up that case was the fact that encrypted phones were widely used in organised crime, which was impeding non-cybercrime investigations. However, the technology behind the phones was so complex that the investigation ended up at the NHTCU. Although it was mentioned several times in the interviews that were conducted for the present study, that it is sometimes difficult to explain why the NHTCU also takes up these kinds of cases, it is also widely recognised that these are precisely the kinds of cases that need to be taken up, as they have such a big impact on tackling organised crime.

Goals

Officially, criminal investigations into cybercrime are only to be started if evidence is available that can be used to track down and prosecute possible suspects, as that is a precondition for the use of investigative powers. However, many cybercriminal investigations do not lead to the identification of a suspect. Sometimes this becomes

evident soon after the start of an investigation, and the police then consider whether other goals can be achieved with the gathered information, such as gaining insight into a particular criminal phenomenon, so as to use that knowledge in subsequent criminal investigations or deploy countermeasures.
In practice, the police apply a flexible approach to the investigation goals formulated at the start of an investigation, also because it is not known at the outset what information the investigation will yield and, therefore, which goals it will serve. Goals can sometimes be changed as the police gather additional information during the investigation. For example, when it emerges that no suspect can be identified or that a suspect cannot be prosecuted, the emphasis will shift to the use of counter-measures to stop this form of cybercrime. Conversely, over the course of an investigation it can emerge that more can be done than was thought at the outset.

Investigative tools and methods

The investigative activities in the files we examined, especially in the initial phase of an investigation, mainly consisted of demanding access to and securing server data. A detailed investigation of server data provides insight into the type of data stored on a server and how a server is used. Sometimes this was done by physically securing a server and other times by making a forensic copy or snapshot. Subsequently, digital evidence was examined in more detail. In addition, these criminal investigations made extensive use of internet wiretaps and looked into network traffic. Based on the information thus obtained, the police were able to plan the further direction of the investigations. These data were also examined to ascertain whether the suspect's identity might be revealed somewhere. It should be noted that the use of these tools did not yield the same amount of information in every investigation.
Furthermore, the files we examined also showed that when no suspect could be identified, generally only digital investigation methods were used. When Dutch suspects were identified, the investigation often shifted to a more tactical approach that also involved using more traditional (offline) investigation tools and methods. Thus, in addition to internet wiretaps, telephone taps were used to learn about contacts between suspects and with others, as well as matters that concerned them. This was often combined with financial investigations to map money flows in order to establish criminal activities like money laundering.
In all five files we examined in which Dutch suspects were identified, undercover investigative powers were used. These powers were used both online and offline. This is striking, as these special investigative powers are normally rarely used in non-cybercrime cases. This may reflect the seriousness of the cases we examined, but it may also imply that in tackling these new cybercrime offences, new ideas are emerging about the use and the severity of existing investigative powers.

Possibilities for prosecution

Suspects were identified in five of the eight files we examined. In four cases, the prime suspects were Dutch nationals. Two of these cases resulted in convictions: a ransomware case and a phishing case. In the ransomware case, community service orders and a suspended prison sentence were imposed, and in the phishing case, prison sentences of five years were imposed. This is also the heaviest punishment imposed so far for this particular offence. In the third case, which concerned DDoS attacks, an alternative settlement was imposed due to the young age of the accused

and the police conducted 'knock and talk' interviews to warn off the buyers of the illegal service. The case relating to encrypted communication has yet to come to court. In the dark web case with two foreign main suspects, the largest Dutch providers of the illegal products were prosecuted. The police conducted 'knock and talk' interviews with some of the other providers and buyers of the products.
Although the NHTCU investigations in particular do not always lead to the identification of suspects who can be prosecuted, launching a criminal investigation does have added value for these types of offences, where prosecuting suspects is difficult. Autonomous, independently operating criminal groups can easily replace a criminal infrastructure. Interventions that focus only on disrupting the infrastructure have a short-lived effect, as new infrastructure will be created and activities will be continued elsewhere. It is therefore important to continue to conduct criminal investigations aimed at identifying and prosecuting suspects. Furthermore, in a number of cases the NHCTU investigations into facilitators, while not yielding a main suspect, did yield information on other forms of crime that could subsequently be used in other criminal investigations or to deploy countermeasures.

Countermeasures

Our study shows that criminal investigations and countermeasures to obstruct criminal processes go hand in hand, as that is the most effective way to tackle cybercrime. In the context, we also refer to the approach used to tackle the infiltration of the public sphere by organised crime, which specifically targets the criminal business model. The interplay between criminal investigations and countermeasures is important because knowledge gained from criminal investigations can be used to gain and update knowledge about these criminal processes. If interventions are limited to countermeasures, only a small part of the criminal process is made visible. By contrast, when suspects are arrested or criminal assets are seized, the entire process can be reconstructed and the key players can be identified. Criminal investigations not only build up knowledge but also have a disruptive effect because they deter potential offenders.
From a legal perspective, the implementation of countermeasures in the context of criminal investigations sometimes gives rise to debates. The police have a broader task than the Public Prosecution Service. This raises the question of what mandate the Public Prosecution Service has with regard to countermeasures. Countermeasures sometimes also require the use of special investigative powers that require authorisation by a public prosecutor or examining judge. This can be problematic when it becomes evident soon after the start of an investigation into a cybercrime offence with a major social impact that no suspect can be identified. In that event, deploying an alternative form of intervention would be desirable. However, there is currently no legal basis for the use of investigative powers for the purpose of disrupting criminal activities. The interviews we conducted show that this does not yet lead to problems in practice, but attempts to resolve this issue do sometimes approach a grey area.

Dilemmas in tackling cybercrime

Over the course of this study, it became clear that the wishes of investigative officers are sometimes at odds with the policy and legal frameworks, leading to areas of tension in the approach to cybercrime.

Information position

The tension in the approach to cybercrime relates first and foremost to the information position in the criminal investigation process. For the police to be able to investigate crimes efficiently and make informed choices in the criminal investigation process, it is important to build up a good information position. To build up an information position on the activities of (international) criminal groups, facilitators and other perpetrators, the police would like to monitor those activities on a continuous basis together with other parties, not necessarily in the context of specific investigations. To achieve this, the NHTCU aims for a data-driven way of working. This includes, for example, examining whether links can be established between data from different criminal investigations in terms of similarities in their modus operandi or the malware used. However, the Public Prosecution Service and the police are not allowed to use investigative powers for the sole purpose of improving their information position. In addition, data from different investigations may not be automatically linked. When information is secured, this is done in the context of a specific criminal investigation. However, within the framework of the Police Data Act (*Wet politiegegevens*, Wpg) information may also be used in other investigations, provided this has been authorised. This basic principle that the police may not use investigative powers to improve its information position sometimes creates difficulties. The police want to gain a good overview of what is going on, as it enables them to respond effectively and efficiently.
Getting to the bottom of cybercrime phenomena requires investigations spanning years. Investigations into cybercrime phenomena consume a lot of time and capacity and often (primarily) yield results in terms of stopping and disrupting cybercrime, but less frequently lead to the identification and prosecution of perpetrators. Such less easily measurable alternative interventions are sometimes difficult to reconcile with the policy-based quantitative targets. While the choice between meeting quantitative targets or increasing the knowledge position is not always so black and white, in practice it often presents a dilemma.

Sharing information

The second major finding of our study concerns problems around sharing information. These problems relate first and foremost to the notification of victims. At present, responsibility for this is not clearly assigned to a specific party. With certain offences, such as hacking, the number of victims is often so large that notifying the victims is not a task that can simply be added to the workload of the investigative officers. In addition, the process of notifying victims is complex. Often, abstract data sets such as IP addresses are the starting point. Furthermore, sharing this information can present legal complications. What seems logical and obvious to do in practice is not always legally permitted. This creates a lack of clarity and inefficiency. In one of the criminal investigations we examined, this meant that several Dutch parties were notified later than desirable and by means of a difficult indirect process. As a result, these Dutch parties were exposed to potential danger for an unnecessarily long time.
In addition, the difficulties also relate to public-private partnerships. Public-private partnerships are an essential component of the integrated approach to cybercrime. Partnerships with private parties enable incorporating other expertise in the approach to cybercrime and enable both the police and the private party to gather additional information.

However, there are also practical objections to such partnerships. Public and private parties have different, and possibly conflicting, interests. The parties should remain aware of this throughout the term of their partnership. Furthermore, the laws and regulations concerning the sharing of information can make such types of cooperation difficult. This includes not only the Police Data Act (Wpg), but also the General Data Protection Regulation (which has replaced the Persona Data Protection Act (*Wet bescherming persoonsgegevens*, Wbp)), the Network and Information Systems Security Act (*Wet beveiliging netwerk- en informatiesystemen*, Wbni) and, where applicable, duties of confidentiality. While it is advisable to exercise a degree of restraint in sharing information, a lack of clarity among parties about the legislation can lead to excessive reluctance to share information.

International cooperation

In tackling cybercrime, the police in many cases depend on international cooperation. Even smaller cases often have an international component. International cooperation is therefore an important part of the criminal investigation process. The NHTCU cooperates frequently and well with various European criminal investigation services, such as services in the UK and Germany, as well as the FBI in the United States. This cooperation includes sharing investigative information, the coordinated search and arrest of suspects and the coordinated deployment of crime disruption activities.
Although good international cooperation can bring success, the officers interviewed in our study stated that the long processing time of international legal assistance requests is one of the biggest bottlenecks. The length of time that teams have to wait for the results of such a request varies greatly. While the interviewed investigative officers are positive about Europol's role, they also noted that success is very dependent on the capacity and priorities in cooperating countries. Each country has limited capacity for handling legal assistance requests. That also applies to the Netherlands. The reality is that by the time a response is received, sometimes the requested information has long since vanished. What has improved in international cooperation compared to a few years ago is that the services in various countries have more knowledge, and contacts with many countries are also improving.

In conclusion

This study has highlighted a number of points that raise the question of how the frameworks that apply in tackling traditional crime relate to the approach used to tackle (complex) cybercrime. Therefore, it could be beneficial to conduct a critical review as to whether the current laws and regulations are adequate to facilitate the collection, processing and analysis of information for the purposes of tackling cybercrime. In addition, the parties involved need to draw up clear frameworks within which information can be shared. This will ensure that when information is urgently needed and parties are willing to share it, they are able to share such important information

Literatuur

Beerthuizen, M.G.C.J., Sipma, T., Laan, A.M, van der (2020). *Aard en omvang van dader-en slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland*. Den Haag: WODC. Cahier 2020-15.

Boeije, H., & Bleijenbergh, I. (2019). *Analyseren in kwalitatief onderzoek: Denken en doen (derde druk*). Amsterdam: Boom.

Boes, S., & Leukfeldt, E.R. (2017). Fighting cybercrime: A joint effort. In *Cyber-physical security* (pp. 185-203). Springer, Cham.

Boerman, F., Grapendaal, M., Nieuwenhuis, F., & Stoffers, E. (2017). *Nationaal dreigingsbeeld 2017: Georganiseerde criminaliteit*. Driebergen: Dienst Landelijke Informatieorgansiatie.

Bokhorst, R.J., Steeg, M. van der, & Poot, C.J., de (2011). *Rechercheprocessen bij de bestrijding van georganiseerde criminaliteit*. Den Haag: WODC. Cahier 2011-11.

Boonstra, J.J. (2007). Ondernemen in allianties en netwerken: een multidisciplinair perspectief. *Tijdschrift voor Management en Organisatie, 61*(3/4), 5-35.

Borwell, J., & Bos-Riepma, K. (2018) *Tech Support Scam: Verdiepende analyse.* [Intern document].

Boutellier, J.C.J. (2007). *Nodale orde: Veiligheid en burgerschap in een Netwerksamenleving* [Oratie].

Brennenraedts, R., Bekkers, R., Kats, J., Hanswijk, M., Bakhyshov, R., Sahebali, W., & Jansen, R. (2020). *Informatie-uitwisseling landelijk dekkend stelsel cybersecurity*. Utrecht: Dialogic Innovatie en Interactie.

Bryson, J.M., Crosby, B.C., & Bloomberg, L. (2014). Public value governance: Moving beyond traditional public administration and the new public management. *Public administration review*, *74*(4), 445-456.

Bulanova-Hristova, G., et al. (2016). Cyber-OC – Scope and manifestations in selected EU member states.

Calster, P. van, & Schuilenburg, M.B. (2009). Burgernet vanuit een nodal governance-perspectief. *Justitiële verkenningen*, *35*(1), 93.

Chromik, J.J., Santanna, J.J., Sperotto, A., & Pras, A. (2015). Booter websites characterization: Towards a list of threats. In *Brazilian Symposium on Computer Networks and Distributed Systems (SBRC)*.

Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Commissie-Koops) (2018). *Regulering van opsporingsbevoegdheden in een digitale omgeving*. Geraadpleegd op 25 november 2020 via: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/06/26/rapport-commissie-koops---regulering-van-opsporingsbevoegdheden-in-een-digitale-omgeving/Rapport+Commissie+Koops+juni+2018.pdf.

Covey, S.M., Merrill, R.R., & Link, G. (2012). *Smart trust: Creating prosperity, energy, and joy in a low-trust world*. Simon and Schuster.

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

Custers, B.H.M., Oerlemans, J.J., & Pool, R.L.D. (2016). *Ransomware*, cryptoware en het witwassen van losgeld in bitcoins. *Strafblad*, *14*(9), 87-95.

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

ENISA (2010). *Cyber Europe 2010. Evaluation Report*.European Network and Information Security Agency. (2010). *Incentives and Challenges for Information Sharing in the Context of Network and Information Security.*
Erkel, J.J. van, Pool, R.L.D., Harbers, M., Oerlemans, J.J., Bargh, M.S., & Braak, S.W. van den (2017). *(Verkeerd) verbonden in een slimme samenleving: Het Internet of Things: kansen, bedreigingen en maatregelen*. Den Haag: WODC.
Europol (2016). *No More Ransom: Law enforcement and IT security companies join forces to fight ransomware.* Geraadpleegd op 10 februari 2020 via: https://www.europol.europa.eu/newsroom/news/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-to-fight-*ransomware*
Europol (2019). *Internet Organised Crime Threat Assessment (IOCTA) 2019.*
Faber, W., Mostert, S., Faber, J., & Vrolijk, N. (2010). *Phishing, kinderporno en advance-fee Internet fraud*: *hypothesen van cybercrime en haar daders.* Oss: Faber organisatievernieuwing.
Feng, K., Wang, S., Li, N., Wu, C., & Xiong, W. (2018). Balancing public and private interests through optimization of concession agreement design for user-pay PPP projects. *Journal of Civil Engineering and Management*, *24*(2), 116-129.
Flier, P.J. van der (2006). De Wet Computercriminaliteit-II en het Cybercrime Verdrag. *Ars Aqui, 55(*12), 914-922.
Fox-IT (2020). *Spoedondersteuning Project Fontana*.
Garsse, S. van, & Verhoest, K. (2008). Succes- en faalfactoren voor PPS-projecten. Leuven: SBOV.
Gerritsma-Breur, C.M. & Verveld-Suijkerbuijk, M.A.M. (2013). 1+1=3: Samen tegen cybercrime. *Tijdschrift Onderneming & Strafrecht in de praktijk*, *1*(1), 16-22.
Gregoire, C. (2017). *The fight against tech support scams.* Geraadpleegd op 25 augustus 2020 via: https://blogs.microsoft.com/on-the-issues/2017/05/18/fight-tech-support-scams/
Gregoire, C. (2018). *New breakthroughs in combatting tech support scams.* Geraadpleegd op 25 augustus 2020 via: https://blogs.microsoft.com/on-the-issues/2018/11/29/new-breakthroughs-in-combatting-tech-support-scams/
Gruening, G. (2001). Origin and theoretical basis of New Public Management. *International Public Management Journal*, *4*(1), 1-25.
Hagenaars, P., & Bonnes, J. (2020). De kracht van privaat-publieke allianties. *Cahier politiestudies*, (56), 63-90.
Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: An empirical analysis. *Police Practice and Research*, *19*(6), 519-536.
Heck, W., & Wassens, R. (2020). *Universiteit Maastricht betaalde bijna 200.000 € losgeld na ransomware-aanval*. Geraadpleegd op 26 augustus 2020 via: https://www.nrc.nl/nieuws/2020/02/05/universiteit-maastricht-betaalde-bijna-200-000-€-losgeld-na-*ransomware*-aanval-a3989357
Heldeweg, M.A., & Sanders, M. (2011). Botsende publieke waarden bij publiek-private samenwerking. Dimensies en dilemmas van juridisch-bestuurskundige legitimiteit in het bijzonder bij openbaar gezag. *Bestuurskunde*, *20*(2), 33-43.
Hengst, M. den, Brink, T. ten, & Mors, J. ter (2017). *Informatiegestuurd politiewerk in de praktijk*. Politie: Politieacademie.
Henseler, H., & Poot, C.J. de (2020). De betekenis van digitale sporen voor bewijs op activiteitniveau. *Expertise en Recht, 2,* 50-59.
Hoepman, J. H., Koops, B. J., & Lueks, W. (2014). *Anoniem misdaad melden via Internet: technische en juridische risico's*. Geraadpleegd op 26 januari 2021 via: https://repository.ubn.ru.nl/bitstream/handle/2066/135039/135039.pdf
Holt, T.J. & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35,* 20-40.

Hudson, B., Hardy, B., Henwood, M., & Wistow, G. (1999). In pursuit of inter-agency collaboration in the public sector: What is the contribution of theory and research?. *Public Management an International Journal of Research and Theory*, *1*(2), 235-260.
Huisman, S., Princen, M., Klerks, P., & Kop, N. (2016) *Handelen naar waarheid: Sterkte- en zwakteanalyse van de opsporing*. Apeldoorn: Politieacademie.
Hutchings, A., & Holt, T. J. (2017). The online stolen data market: disruption and intervention approaches. *Global Crime*, *18*(1), 11-30.
Jacobs, B. (2013). De DDoS paradox: Ontsluiten door afsluiten. *Nederlands Juristenblad, 88*(32), 2191-2195.
Kaspersky (2019). *Advanced threat predictions for 2020*. Geraadpleegd op 20 november 2020, via: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2019/11/20151759/KSB2019_APT-predictions-2020_web.pdf.
Klijn, E.H., & Twist, M.J.W., van (2007). Publiek-private samenwerking in Nederland: Overzicht van theorie en praktijk. *Tijdschrift voor Organisatiekunde en Sociaal Beleid, 3*(4), 156-170.
Kokkeler, B. (2017). *Smart public safety*: *Leiderschap voor nieuwe verbindingen in de digi-sociale wereld*. Breda: Avans Hogeschool.
Koops, E.J. (2010). The internet and its opportunities for cybercrime. *Transnational Criminology Manual* (pp. 735-754). Nijmegen: Wolf Legal Publishers.
Koops, E.J. (2012). De dynamiek van cybercrimewetgeving in Europa en Nederland. *Justitiële verkenningen, 38*(1), 924.
Koops. E.J. (2012b). Politieonderzoek in open bronnen op internet: Strafvorderlijke aspecten. *Tijdschrift Voor Veiligheid, 11(2),* 30-46.
Koops, E.J., & Oerlemans, J.J. (2019). Strafrecht en ICT. SDU.
Kop, N. (2012). *Van opsporing naar criminaliteitsbeheersing: vijf strategische implicaties*. Boom Lemma Uitgevers.
Kop, N. (2017). Leren van publiek-private samenwerking in een afpersingszaak. *Tijdschrift voor de Politie, 79*(7), 12-15.
Kruisbergen, E.W., & Jong, D. de, Kouwenberg, R.F. (contrib.) (2010). *Opsporen onder dekmantel: Regulering, uitvoering en resultaten van undercovertrajecten*. Den Haag: Boom Juridische uitgevers. Onderzoek en beleid 282.
Kruisbergen E.W., Leukfeldt, E.R., Kleemans, E.R., & Roks, R.A. (2018). *Georganiseerde criminaliteit en ICT: Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit*. Den Haag: WODC. Cahier 2018-8.
Laan, A.M. van der, Beerthuizen, M.G.C.J., & Weijters, G. (2016). Jeugdige daders van online-criminaliteit, *Cahier Politiestudies,* (41)*,* 145-168.
Ladegaard, I. (2019). Crime displacement in digital drug markets. *International Journal of Drug Policy.*
Langius, M.B., & Mol Lous, L.P. (2018). De wet computercriminaliteit III. *Ars Aequi,* 830-838.
Lassche, H. (2019). *Digitalisering en de opsporingspraktijk: Juridische aspecten*. Politieacademie.
Leukfeldt, R. (red.) (2017). *The human factor in cybercrime and cybersecurity*. Den Haag: Eleven International Publishing.
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.* Den Haag: Boom uitgevers.
Mansfield-Devine, S. (2016). *Ransomware*: taking businesses hostage. *Network Security*, *2016*(10), 8-17.
Ministerie van Justitie en Veiligheid (2018). *Integrale aanpak cybercrime.* Geraadpleegd op 29 augustus 2020, via: https://www.rijksoverheid.nl/documenten/kamerstukken/2018/04/20/tk-integrale-aanpak-cybercrime.

Montfort, C.J. van, Brink, G.J M. van den, Schulz, J.M., & Maalsté, N.J.M. (2012). *Publiek-private samenwerking in maatschappelijke veiligheid: Naar een improvisatiemodel.* Tilburg: TSPB.
Munnichs, G. Kouw, M. & Kool, L. (2017) *Een nooit gelopen race: over cyberdreigingen en versterking van weerbaarheid*. Den Haag: Rathenau-instituut.
Nationaal Cyber Security Centrum (2012). *Cybercrime: van herkenning tot aangifte*. Den Haag: NCSC.
Nationaal Cyber Security Centrum. (2018). *Nederlandse Cybersecurity Agenda*. Geraadpleegd op 24 augustus 2020 via: https://www.ncsc.nl/onderwerpen/nederlandse-cyber-security-agenda/documenten/publicaties/2019/mei/01/nederlandse-cybersecurity-agenda
NCSC (2018). Cybersecuritybeeld Nederland. Den Haag:NCSC.
NCSC (2020). Cybersecuritybeeld Nederland. Den Haag:NCSC.
No More DDoS (z.d.). *FAQ.* Geraadpleegd op 24 augustus 2020, via: https://www.nomoreddos.org/faq/.
Odinot, G., Poot, C.J. de, & Verhoeven, M. (2018). De aard en aanpak van georganiseerde cybercrime: Bevindingen uit een internationale empirische studie. *Justitiële verkenningen, 44*(5), 9-22.
Odinot, G., Verhoeven, M.A., Pool, R.L.D., & Poot, C.J. de (2017). *Organised cybercrime in the Netherlands: Emperical findings and implications for law enforcement*. Den Haag: WODC. Cahier 2017-1.
Oerlemans, J.J. (2017). *Investigating cybercrime* (Dissertatie). Leiden: Universiteit Leiden.
Oerlemans, J.J. (2018). Facebookvrienden worden met de verdachte: Over undercoverbevoegdheden op internet. *Justitiële verkenningen, 44*(5), 83-99.
OM.nl (2020). Schade helpdeskfraude gehalveerd. Geraadpleegd op 26 augustus 2020, via: https://www.om.nl/actueel/nieuws/2020/01/28/schade-helpdesk-fraude-gehalveerd.
Paulus, A.J.M. (2020). *Verstoring van cybercriminaliteit: De mogelijkheden van verstoring binnen het kader van een opsporingsonderzoek, de toetsing daarvan en het toezicht daarop.* (Masterscriptie, Universiteit Leiden.)
Politie.nl (2020) *No More Ransom: Al 4 miljoen slachtoffers van ransomware gingen de strijd tegen hackers aan*. Geraadpleegd op 11 augustus 2020, via: https://www.politie.nl/nieuws/2020/juli/27/11-no-more-ransom.-hoe-al-4-miljoen-slachtoffers-van-*ransomware*-de-strijd-tegen-de-hackers-zijn-aangegaan.html
Politie.nl (z.d.a). Helpdeskfraude. Geraadpleegd op 25 augustus 2020 via: https://www.politie.nl/themas/helpdeskfraude.html.
Politie.nl (z.d.b). DDoS-aanval is strafbaar. Geraadpleegd op 24 augustus 2020, via: https://www.politie.nl/themas/ddos.html.
Poot, C.J. de, Bokhorst, R.J., Koppen, P.J. van, & Muller, E.R. (2004). Rechercheportret. Over dilemma's in de opsporing. Alphen aan den Rijn: Kluwer.
Poot, H. de, & McKim, M. (2020). Security by design in de vitale sector. Security by design in de vitale sector | iBestuur. Geraadpleegd op 28 maart 2021.
Provan, K.G., & Kenis, P. (2008). Modes of network governance: Structure, management, and effectiveness. *Journal of Public Administration Research and Theory, 18(2),* 229-252.
Raad van Hoofdcommissarissen. (2005). *Visie op Publiek-Private Samenwerking.* Z.pl.:Z.uitg.
Sanders, M. (2017). Publiek-Private Samenwerking: Krachten bundelen of met het publieke belang aan de haal. *Publiek-Private Samenwerking: Kunst van het evenwicht*, 9-16.

Sandt, E. van de, Bunningen, A. van, Lenthe, J. van, & Fokker, J. (2021). *Towards data scientific investigations: A comprehensive data science framework and case study for investigating organized crime and serving the public interest*. Z.pl.: Rephrain.
Sanders, M., & Heldeweg, M. (2014). To PPS or not to PPS? (Publiek-)private samenwerking rond groen gas. *Bestuurswetenschappen*, *68*(1), 41-57.
Sandt, E.H.A. van de (2019). *Deviant Security: The Technical Computer Security Practices of Cyber Criminals*. (Doctoral thesis.)
Schedler, K., & Proeller, I. (2000). *New public management*. Stuttgart/Wenen: Z.uitg..
Schuilenburg, M. (2012). *Orde in veiligheid: Een dynamisch perspectief.* Den Haag: Boom Lemma Uitgevers.
Sipma, T., & Leijsen, E.M.C. (2019). *Slachtofferschap van online criminaliteit: Prevalentie, risicofactoren en gevolgen.* Den Haag: WODC. Cahier 2019-18.
Sophos (2020). *The state of ransomware.* Geraadpleegd op 26 augustus 2020, via: https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-*ransomware*-2020-wp.pdf.
Staats, W., Meerts, C., Kleemans, E.W., & Huisman, W. (2021). *Nieuwe manieren van samenwerken: Een systematische literatuurreview naar (de effectiviteit van) publiek private samenwerkingsverbanden op het gebied van financieel economische criminaliteit en cybercrime*. Amsterdam: Vrije Universiteit Amsterdam, Faculteit der Rechtsgeleerdheid, Afdeling Strafrecht en Criminologie.
Stol, W. (2020). Digitalisering en de maatschappelijke rol van de politie. In J. Nap & G. Meershoek (red.), *In naam der wat? Reflecties op de maatschappelijke politiefunctie*. Apeldoorn: Politieacademie.
Stol, W., & Strikwerda, L. (2017). *Strafrechtspleging in een digitale samenleving*. Den Haag: Boom Juridisch.
Tjong Tjin Tai, E., & Koops, B.J. (2015). Zorgplichten tegen cybercrime. *Nederlands Juristenblad, 90*(16), 1065-1072.
Vries, I. de (2017). Big data. In M. den Hengst, T. ten Brink & J., ter Mors (red), *Informatiegestuurd politiewerk in de praktijk*. Politie: Politieacademie.
Waard, J. de, & Scheepmaker, M. (2012). Voorwoord. *Justitiële verkenningen*, *38*(8), 5.
Wagen, W.van der, Zand-Kurtovic, E.G. van 't, & Matthijsse, S.R. (2019). *Cyberdaders: Uniek profiel, unieke aanpak? Een onderzoek naar kenmerken van en passende interventies voor daders van cybercriminaliteit in enge zin*. Rotterdam: Erasmus Universiteit Rotterdam, School of Law.
Weijer, S.G.A. van de, Leukfeldt, E.R., & Zee, S. van der (2020). *Een onderzoek naar aangiftebereidheid onder burgers en ondernemers*. Den Haag: Politie & wetenschap.
Wall, D.S. (2007), *Cybercrime: The transformation of crime in the information age.* Cambridge, MA: Polity.
Wall, D.S. (2014). *High risk cybercrime is really a mixed bag of threats*. Retrieved November 2020 from: http://theconversation.com/high-sisk-cyber-crime-is-really-a-mixed-bag-of-threats-34091.
WRR (2000). *Het borgen van publiek belang*. Den Haag: Sdu Uitgevers.
Yar, M. (2016). Online crime: Oxford Research Encyclopedia of Criminology. *Criminology and Criminal Justice,* 1-2.

Bijlage 1 Samenstelling begeleidingscommissie

Voorzitter

Prof. dr. W. (Wouter) Stol	Lector cybersafety NHL Stenden Hogeschool en bijzonder hoogleraar politiestudies Open Universiteit

Leden

Mr. M. (Martijn) Egberts	Landelijk Officier van Justitie Cybercrime, Landelijk Parket, Openbaar Ministerie
L. (Laura) de Korte	Beleidsadviseur DGRR, Ministerie van Justitie en Veiligheid
S. (Sander) van der Maden	Adviseur Team High Tech Crime, Nationale Politie
Dr. G. (Geralda) Odinot	Zelfstandig wetenschappelijk onderzoeker

Bijlage 2 Veelvoorkomende cyberdelicten

In deze bijlage worden verschillende soorten cyberdelicten die voor dit onderzoek relevant zijn, uiteengezet.

DDoS-aanval
Een DDoS-aanval is een poging om een website of server onbereikbaar te maken door deze te overspoelen met dataverkeer. Hiervoor wordt vaak gebruikgemaakt van botnets om een server massaal te bezoeken waardoor deze het dataverkeer niet meer aankan en uiteindelijk voor legitieme klanten onbereikbaar wordt (Politie.nl, z.d.b; No More DDoS, z.d.). De besturing vindt meestal plaats vanuit een Command & Control-server. Dit kan zowel een legale server zijn die onder valse voorwendselen wordt gebruikt, als een server waarop is ingebroken (NCSC, 2012).
De gevolgen en schade van een DDoS-aanval kunnen aanzienlijk zijn. Dit is afhankelijk van de dienst die als gevolg van de aanval (tijdelijk) niet beschikbaar is (NCSC, 2012). Een voorbeeld hiervan was de DDoS-aanval die er in 2018 voor zorgde dat internetbankeren bij verschillende banken een paar uur onmogelijk was. DDoS-aanvallen worden regelmatig aangeboden via een dienst die ook wel cybercrime-as-a-service wordt genoemd. Er wordt dan online een kant-en-klaarpakket aangeboden om een cybercrimedelict, in dit geval een DDoS-aanval, mee te plegen. Een dader hoeft voor het uitvoeren van een aanval dus niet per se technische kennis te hebben.

Malware
Onder *malware* vallen alle vormen van software met kwaadaardige bedoelingen zoals computervirussen, *spyware* en ook *ransomware*. Het onderscheid tussen deze verschillende vormen van *malware* vervaagt. Vaak worden verschillende vormen van *malware* tegelijkertijd of gecombineerd ingezet (NCSC, 2012). *Malware* wordt grotendeels verspreid door middel van virussen en/of wormen. Een virus kan gezien worden als een kwaadaardig programma dat zichzelf toevoegt aan bestaande bestanden. Dit wordt ook wel infecteren genoemd (NCSC, 2012). Een worm verspreidt zich via een netwerk of e-mailverbinding van PC naar PC in plaats van via bestanden (Faber et al., 2010). De worm kopieert zichzelf door gebruik te maken van kwetsbaarheden in computer- en netwerksystemen. Kwetsbaarheden zijn zwakke plekken in de algemene beveiliging van een computer of netwerk (NCSC, 2012).

Ransomware, ook wel 'gijzelsoftware' genoemd, is een vorm van *malware*. Dit is kwaadaardige software die de toegang tot een computer en de bestanden daarop versleutelt en daarmee ontoegankelijk maakt (Custers, Oerlemans & Pool, 2016). Vaak komt *ransomware* op een computer doordat op een bestand is geklikt wat er betrouwbaar uit ziet, maar wat in werkelijkheid besmet is. Zo werden bijvoorbeeld reclamefoto's op bekende website gebruikt om de bezoekers van deze website te besmetten met *ransomware* (Odinot et al., 2018). Pas wanneer het slachtoffer een bepaald bedrag betaalt wordt de computer weer vrijgegeven en kan men weer bij deze bestanden. Als men weigert te betalen, wordt gedreigd de bestanden te wissen of te delen met derden. Criminelen voeren steeds vaker een uitgebreide voorverkenning uit om op deze wijze in te schatten wat een reëel geldbedrag is om te eisen en welke onderdelen van een bedrijf vitaal zijn voor de continuïteit van een bedrijf. Ook blijkt er een toename te zijn van het vooraf kopiëren van de versleutelde data. Door (het dreigen om) deze data te publiceren wordt extra druk uitgeoefend op het

bedrijf om tot een betaling over te gaan (NCSC, 2020). Dit is bijvoorbeeld gebeurd toen een Amerikaanse stad in 2019 het slachtoffer werd van *ransomware* en 2 van de 32 Gigabyte is gepubliceerd om de stad te bewegen tot een betaling van een miljoen dollar.

Een bekend voorbeeld van een *ransomware* aanval in Nederland is die op de Universiteit Maastricht in december 2019. In een rapport van Fox-IT (2020) is te lezen dat de daders door middel van *phishing* e-mails het netwerk binnen wisten te komen om vervolgens cruciale systemen voor de bedrijfsvoering van de universiteit te versleutelen. De periode tussen de besmetting via *phishing* e-mails en de daadwerkelijke uitrol van de versleuteling bedroeg meer dan twee maanden. In deze periode wisten de daders het netwerk te verkennen en *malware* te plaatsen op een server waardoor administratierechten op de server werden verkregen. Hiermee hadden de aanvallers de beschikking tot zowel het systeem met de hoogste rechten als de gebruiker met de hoogste rechten, wat hen ook de mogelijkheid gaf om back-ups te verwijderen of te versleutelen. Bij de uiteindelijke uitrol van de *ransomware* werd data van een grote hoeveelheid servers versleuteld. Dit zorgde er onder andere voor dat studenten en onderzoekers niet meer bij hun opgeslagen data konden komen. Volgens Fox-IT (2020) gaat het om een professionele dadergroepering die in elk geval sinds 2014 actief is. In 2019 maakten zij op soortgelijke wijze meer dan 150 slachtoffers. Zes dagen na de infectie is door de Universiteit Maastricht dertig bitcoin ter waarde van 197.000 € betaald voor de ontsleuteling van de servers. De universiteit sprak over een 'duivels dilemma'. Het maatschappelijk belang van het niet betalen aan criminelen woog hierin niet zwaar genoeg tegenover de schade die teweeg zou worden gebracht. Onderzoek en onderwijs konden namelijk geen doorgang meer vinden, systemen moesten opnieuw opgebouwd worden en ook salarisbetalingen van personeel kwamen in gevaar wanneer niet over zou zijn gegaan tot betaling (Heck & Wassens, 2020).

Phishing

Een laatste cyberdelict dat nader wordt toegelicht is *phishing*. *Phishing* is een vorm van internetfraude waarbij meestal gebruik wordt gemaakt van nagemaakte websites om mensen te verleiden om op deze website privégegevens in te voeren (NCSC, 2012). Zo kan een aanvaller zich bijvoorbeeld voordoen als een bank(medewerker) om daarmee gevoelige en/of persoonlijke informatie van het slachtoffer te verkrijgen. Er wordt als het ware 'gevist' naar inloggegevens en persoonsgegevens van gebruikers. Met deze gegevens kan de cybercrimineel vervolgens inloggen op de site van de echte bank en zo geld opnemen (Faber et al., 2010). *Phishing* valt officieel niet binnen de categorie High Tech Crime. Het kan namelijk gezien worden als traditionele oplichting, die plaatsvindt op het internet. Toch is het een probleem waar vooral banken veel mee te maken hebben en hierbij de hulp van cybercrimeteams inschakelen.

In de bovenstaande paragrafen worden de verschillende cyberdelicten los van elkaar omschreven. In de praktijk komen deze vormen van criminaliteit ook samen voor. Zo kan het verspreiden van *malware* als middel ingezet worden om een ander doel te bereiken, zoals een botnet opbouwen om vervolgens via dit botnet geld te stelen van bankrekeningen van slachtoffers (NCSC, 2012).

Bijlage 3 Afkortingen- en begrippenlijst

Bitcoin	Een crypotovaluta
Book of Crime	De book of crime methodiek houdt in dat de modus operandi van een delictsvorm zo volledig en nauwkeurig mogelijk in kaart wordt gebracht om zodoende tot passende interventies of barrières te komen.
Booter	Een booter is een andere benaming voor een website waar DDoS-aanvallen worden aangeboden.
Botnet	Een verzameling van besmette systemen die door actoren centraal bestuurd kan worden. Botnets vormen de infrastructuur voor veel vormen van internetcriminaliteit.
Bug	Een fout in een computerprogramma of website.
Bullet proof hoster	Een bedrijf dat de mogelijkheid biedt volledig anoniem gebruik te maken van serverruimte en er daarmee van verdacht wordt bewust criminaliteit te faciliteren.
CEO-fraude	Oplichtingsmethode waarbij criminelen zich voordoen als CEO (of andere hoge functie) van een bedrijf om werknemers ertoe te bewegen om betalingen te doen. Ook wel BEC-fraude genoemd.
Command and control	Vanuit een command and control server kunnen andere geïnfecteerde systemen worden aangestuurd.
Computer-focused crime	Misdrijven die niet kunnen bestaan zonder ICT. ICT is hierbij het doelwit en het middel van de aanvallen. Bijvoorbeeld DDoS-aanvallen, of hacking.
Computer-assisted crime	Criminaliteit die voorheen analoog, maar nu hoofdzakelijk digital wordt gepleegd. Bijvoorbeeld marktplaatsfraude en CEO-fraude.
Computer-enabled crime	Betreft alle vormen van traditionele criminaliteit die worden gepleegd met behulp van ICT, maar die niet gericht zijn tegen ICT. ICT kan wel een hulpmiddel zijn bij de modus operandi van het delict. Zo kan een liquidatie niet digitaal worden uitgevoerd, maar versleutelde communicatie kan wel bijdrage aan de uitvoering ervan. Datzelfde geldt voor drugshandel via online marktplaatsen. In toenemende mate zijn zo alle vormen van criminaliteit in zekere zin computer-enabled door te toename van ICT-gebruik bij traditionele criminaliteit.

Cryptotelefoons	Speciaal geprepareerde toestellen waar anoniem en versleuteld mee kan worden gecommuniceerd.
Cyber	Iets wat te maken heeft met digitale informatie en systemen die verbonden zijn met het internet.
Cyberaanval	Moedwillige activiteit van een cyberactor die is gericht op het met digitale middelen aantasten van de beschikbaarheid, integriteit of vertrouwelijkheid van informatie- en procesbesturingssystemen, daardoor verwerkte en opgeslagen informatie en daarvan afhankelijke diensten en processen.
Cybercrime-as-a-service	Betreft een omvangrijke online cybercriminele dienstverlening waarbij vrijwel elke stap voor het plegen en het beschermen van cybercrime verhandeld wordt.
Cybersecurity	Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan. Die schade kan bestaan uit de aantasting van de beschikbaarheid, integriteit of vertrouwelijkheid van informatiesystemen en informatiediensten en de daarin opgeslagen informatie.
Darkweb	Deel van het internet wat niet via zoekmachines gevonden kan worden en enkel via speciale browsers (zoals TOR) bezocht kan worden.
DDoS	Distributed Denial of Service. Een vorm van DoS waarbij een bepaalde dienst (bijvoorbeeld een website) niet beschikbaar wordt gemaakt door deze te bestoken met veel netwerkverkeer vanuit een groot aantal bronnen.
Databreach	Lek van beveiligde informatie naar een onbevoegd publiek.
Defacement	Defacing is het zonder toestemming veranderen, vervangen of vernielen van een website. Het wordt ook wel gezien als elektronische graffiti, oftewel het bekladden van de startpagina van een site door hackers.
Facilitator	Actoren die het plegen van bepaalde delictsvormen mogelijk of makkelijker maken.
Grooming	Grooming is een proces waarbij een dader het vertrouwen wint van een ander met het doel deze persoon seksueel te misbruiken.
Hacken	Met kwaadaardige bedoelingen probeert in te breken in ICT-systemen.

Hack_Right	Hack_Right is een alternatief aanvullend straftraject voor jongeren die een cybercriminaliteitsdelict hebben gepleegd. Met dit traject wordt jongeren geleerd hoe zij hun cybervaardigheden op legale manieren kunnen inzetten.
Hightech	Hightech kan zowel verwijzen naar een technisch geavanceerde opsporingsinspanning door de politie, bijvoorbeeld door middel van een technisch complex onderzoek, als naar technisch complexe modus operandi door bijvoorbeeld het toepassen van nieuwe criminele werkwijzen.
Hoster	Een hoster is een bedrijf dat de mogelijkheid biedt om serverruimte af te nemen.
IP	Het internetprotocol zorgt voor de adressering van internetverkeer zodat het bij het beoogde doel aankomt.
IoT	Het Internet-of-Things is een netwerk van slimme apparaten, sensoren en andere objecten die (vaak verbonden met het internet) gegevens verzamelen over hun omgeving, deze kunnen uitwisselen en op basis daarvan (semi-) autonome beslissingen of acties nemen die van invloed zijn op hun omgeving.
ISP	Internet Service Provider.
Keylogger	Een keylogger registreert toetsaanslagen en/of muisbewegingen van een computer.
Knock and talk	Bij 'knock and talk' gesprekken worden personen thuis bezocht door de politie om in gesprek te gaan over de delicten en bewustwording te creëren.
Kwetsbaarheid	Een kwetsbaarheid is een eigenschap die een aanvaller de mogelijkheid biedt een cyberaanval uit te voeren of een eigenschap die kan leiden tot uitval. Dit kan zich voordoen in een digitale dienst, proces of systeem, maar ook in de samenleving als geheel of in een specifieke organisatie.
Malware	Samentrekking van malicious software. Malware is de term die als generieke aanduiding wordt gebruikt voor onder andere virussen, wormen en trojans.
Modus operandi	Een werkwijze die een pleger gebruikt of kan gebruiken voor het plegen van een delict. Denk aan voorbeelden zoals het combineren van middelen voor een aanval, het ongericht inzetten van het middel (schot hagel) of juist heel gericht inzetten van specifieke software.
NCSC	Nationaal Cyber Security Centrum.

Notice and Take-Down	Opsporingsbevoegdheid waarbij communicatiedienst-aanbieders verplicht worden strafbaar materiaal te verwijderen.
PGP	Pretty Good Privacy. Een manier van versleuteling van digitale berichten.
Phishing	Verzamelnaam voor digitale activiteiten die tot doel hebben informatie aan mensen te ontfutselen. Deze informatie kan worden misbruikt voor bijvoorbeeld toegang tot systemen.
Ransomware	Gijzelsoftware. Type malware dat systemen of informatie daarop blokkeert en alleen tegen betaling van losgeld weer toegankelijk maakt.
Remote Access Tool	Een Remote Access Tool (RAT) geeft een persoon de mogelijkheid om een computer op afstand te beheren.
Sextortion	Manier van afpersen waarbij gedreigd wordt met het openbaren van seksueel getint materiaal.
Social Engineering	Social Engineering is het misbruiken van menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen, hebzucht, angst of onwetendheid. Door op deze wijze op mensen in te spelen, worden zij verleid tot het afgeven van vertrouwelijke informatie waar vervolgens misbruik van kan worden gemaakt.
Spear phishing	Spear phishing is een variant van phishing die zich richt op één persoon of beperkte groep mensen, die specifiek wordt uitgekozen op basis van hun toegangspositie, om een zo groot mogelijk effect te sorteren zonder al te veel op te vallen.
Statelijke actor	Staten voeren digitale aanvallen uit op andere landen, organisaties of individuen uit primair geopolitieke motieven. Zij hebben als doel de verwerving van strategische informatie (spionage), beïnvloeding van de publieke opinie of democratische processen (beïnvloeding) of verstoring van vitale systemen (verstoring) of zelfs de vernietiging daarvan (sabotage).
Stealth SMS	Een SMS-bericht dat niet zichtbaar is voor de gebruiker van de telefoon, maar die wel een signaal genereert voor de aanbieder van de communicatiedienst.
Take-Down	Het offline halen van een internetpagina of netwerk.
THTC	Team High Tech Crime.
TOR	Een speciale browser waarmee pagina's op het darkweb bezocht kunnen worden.

Tech Support Scam	Oplichtingsmethode waarbij een crimineel zich voordoet als helpdeskmedewerker van een bedrijf.
Versleuteling	Ook wel encryptie genoemd. Manier van beveiligen van digitale bestanden.
Wraakporno	Het zonder toestemming maken, bezitten en/of verspreiden van seksueel getint materiaal van een ander.