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.