Bureau
Boekhoorn
Sociaal-wetenschappelijk
Onderzoek

De aanpak van cybercrime door regionale eenheden van de politie

- *van intake van cybercrime naar opsporing en vervolging*

Nijmegen, oktober 2019

Voorwoord

Cybercriminaliteit is een belangrijk fenomeen geworden in onze gedigitaliseerde wereld, met een grote impact op de maatschappelijke veiligheid. In de bestrijding van 'cybercrime' is de politie, naast andere partijen, een van de belangrijke actoren en zij heeft in de aanpak van cybercrime in de afgelopen jaren extra geïnvesteerd.
Om een beeld te krijgen van de initiatieven die de politie neemt om het cybercriminelen moeilijker te maken, is door BBSO in opdracht van het programmabureau Politie en Wetenschap een verkennend onderzoek uitgevoerd naar de organisatorische en inhoudelijke aanpak van cybercrime door drie politie-eenheden van de Nationale Politie. Daarbij is de focus gericht op de aanpak van de politie in het gehele proces van aangifte tot en met de opsporing van cybercrime, met bijzondere aandacht voor cyberteams.

Wij willen graag alle geïnterviewden bij de politie, in het bijzonder de leden van de cybercrimeteams van de politie-eenheden Noord-Holland, Rotterdam en Oost Nederland, en het Openbaar Ministerie in deze regio's bedanken voor de gesprekken en de ontvangen informatie tijdens de totstandkoming van dit rapport. Hun medewerking hebben wij zeer gewaardeerd.

Ook is een woord van dank op zijn plaats voor de leden van de leescommissie die het conceptrapport van commentaar hebben voorzien: Wouter Stol (Politieacademie en NHL Hogeschool), Rutger Leukfeldt (NSCR en Haagse Hogeschool), Emma Ratia (politie-eenheid Oost Nederland), Lourens Witteveen (politie-eenheid Noord-Holland) en Annemieke Venderbosch en Kees Loef van het programmabureau Politie en Wetenschap.

Paul Boekhoorn
BBSO

Nijmegen, oktober 2019

Inhoud

1 Inleiding

1.1 Cybercrime: criminaliteit via digitale wegen

Cybercrime heeft in de afgelopen jaren steeds meer aandacht gekregen in het maatschappelijk en wetenschappelijk debat. Ook in de onderzoeksprogramma's van Politie en Wetenschap en in de Veiligheidsagenda 2015-2018[1] van het toenmalige ministerie van Veiligheid en Justitie nam en neemt de bestrijding van cybercrime een prominente positie in. De toenemende digitalisering van de samenleving biedt criminelen de mogelijkheid om op nieuwe manieren slachtoffers te maken. Bovendien zijn ook computer- en informatiesystemen vaker het doelwit van criminaliteit. Vanwege deze ontwikkelingen is het beeld ontstaan dat traditionele delicten minder vaak worden gepleegd en dat cybercrime juist toeneemt in de afgelopen jaren. In dit kader zou mogelijk een verschuiving plaatsvinden van offline criminaliteit naar online criminaliteit (de Cuyper en Weijters, 2016). Cybercrime kan voor criminelen aantrekkelijk zijn vanwege de lage investeringskosten -zeker afgezet tegen de verwachte opbrengst- en de lage pakkans in vergelijking tot die van 'offline' criminaliteit.

In het Cybersecuritybeeld Nederland 2019 (CSBN 2019)[2] wordt een zorgelijke beschrijving gegeven van de veiligheidssituatie in het digitale domein. Zo zijn er dreigingen die betrekking hebben op grootschalige diefstal van middelen en van informatie, maar ook op het verstoren of saboteren van diensten en processen waar overheden en samenleving van afhankelijk zijn voor hun functioneren. In CSBN 2019 wordt, net als in CSBN 2018, aangegeven dat de grootste dreiging uitgaat van beroepscriminelen en statelijke actoren. Beroepscriminelen richten zich in toenemende mate op grote bedrijven voor financieel gewin. Statelijke actoren intensiveren hun ondermijnende digitale activiteiten. Concrete voorbeelden van deze dreigingen zijn onder andere de computeraanvallen met malware, cryptoware en 'ransomware'[3] (bijvoorbeeld de WannaCry-ransomware) en zogenaamde 'advanced persistent threats'. Daarnaast zijn er ook dreigingen door individuen die de kennis en mogelijkheden hebben om in geautomatiseerde systemen van organisaties in te breken. Zo zijn er op online-marktplaatsen complete pakketten te koop waarmee men kunt hacken of een Ddos-aanval kunt uitvoeren. Cybervandalen en 'scriptkiddies' kunnen daarmee ook de 'arena' betreden.

[1] Ministerie van Veiligheid en Justitie (2014). Veiligheidsagenda 2015-2018; Bijlage bij Tweede Kamerstukken, Vergaderjaar 2014-2015, 28684 nr. 412.
[2] Nationaal Coördinator Terrorismebestrijding en Veiligheid, Cybersecuritybeeld Nederland CSBN 2019, Ministerie van Justitie en Veiligheid, 2019.
[3] Een wereldwijde ransomware aanval trof in 2017 de Rotterdamse haven en pakketvervoerder TNT.

Cybercrime en gedigitaliseerde criminaliteit

Er wordt in de literatuur en in de aanpak van cybercrime onderscheid gemaakt naar *cybercrime in brede zin* en *cybercrime in enge zin* (Domenie, Leukfeldt, Van Wilsem, Jansen & Stol, 2013; Zebel, De Vries, Giebels, Kuttschreuter & Stol, 2014; Van der Hulst & Neve, 2008). De twee vormen onderscheiden zich van elkaar door de rol die ICT speelt bij de criminele handeling. Zo omvat cybercrime in enge zin delicten waarbij ICT zowel het instrument als het doelwit is van de criminaliteit. In dit geval gaat het bijvoorbeeld om iemand die met behulp van een computer inbreekt op een andere computer en vervolgens (vertrouwelijke) informatie kopieert of verwijdert ('hacken'). Een ander voorbeeld is het platleggen van een website door het versturen van grote hoeveelheden aanvragen (zogenaamde 'Ddos-aanvallen'). Cybercrime in enge zin wordt ook aangeduid als 'cybercriminaliteit'.
Cybercrime kent technieken en middelen enerzijds en verschijningsvormen anderzijds. Bij technieken en middelen gaat het om hacken, malware, botnets, Ddos-aanvallen en social engineering. Bij verschijningsvormen gaat het om het doel waarmee de technieken en middelen worden ingezet, zoals verstoring van de ICT, diefstal van datasets met persoonsgegevens en fraude met betaalmiddelen.

Het landelijk Team High Tech Crime van de politie omschrijft cybercrime 'in brede zin' als 'elke strafbare gedraging waarbij voor de uitvoering het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is' (Bernaards, Monsma & Zin, 2012). Deze definitie wordt ook gebruikt door het Nationaal Cyber Security Centrum (NCSC) en door het Openbaar Ministerie (OM). Uit deze definitie kan worden opgemaakt dat het zowel gaat om delicten die met behulp van ICT worden gepleegd als om misdrijven waarbij ICT het doelwit is. In principe gaat het om ongeautoriseerde toegang tot geautomatiseerde systemen. Verder gaat het bij geautomatiseerd werk meer dan alleen om computers, maar omvat het ook informatiesystemen en telecommunicatiemiddelen.

Naast cybercrime in enge zin is sprake van *gedigitaliseerde criminaliteit*. Dit is 'traditionele' criminaliteit die een nieuwe impuls heeft gekregen door de opkomst van computertechnologie. Het gaat hier onder meer om internetoplichting (fraude op online handelsplaatsen, zoals Marktplaats), bedreiging of het witwassen van geld via digitale betaalmethoden. Veel vormen van gedigitaliseerde criminaliteit worden met eenzelfde technologie gepleegd als cybercrime. Bij gedigitaliseerde criminaliteit is ICT aldus een middel om traditionele vormen van criminaliteit te plegen maar is de verstoring van de ICT zelf niet het doel (hetgeen bij cybercrime wel het doel is).
Verschillende vormen van ICT kunnen een rol spelen in elk van de fasen van het criminele proces, bij zowel de voorbereiding, de uitvoering als de afronding. Zo kunnen de sociale media dienen als ontmoetingsplaats, het 'darkweb' als handelsplaats en witwassen kan plaatsvinden met behulp van bitcoins. Digitale technologie vergroot de reikwijdte van criminelen en biedt goede mogelijkheden om criminele activiteiten af te schermen voor opsporing en justitie.

In de praktijk is het onderscheid tussen cybercrime en gedigitaliseerde criminaliteit minder strikt als hier omschreven. Er is sprake van een steeds sterkere verweving tussen cybercrime, gedigitaliseerde criminaliteit en traditionele vormen van criminaliteit (Boerman et al, 2017).

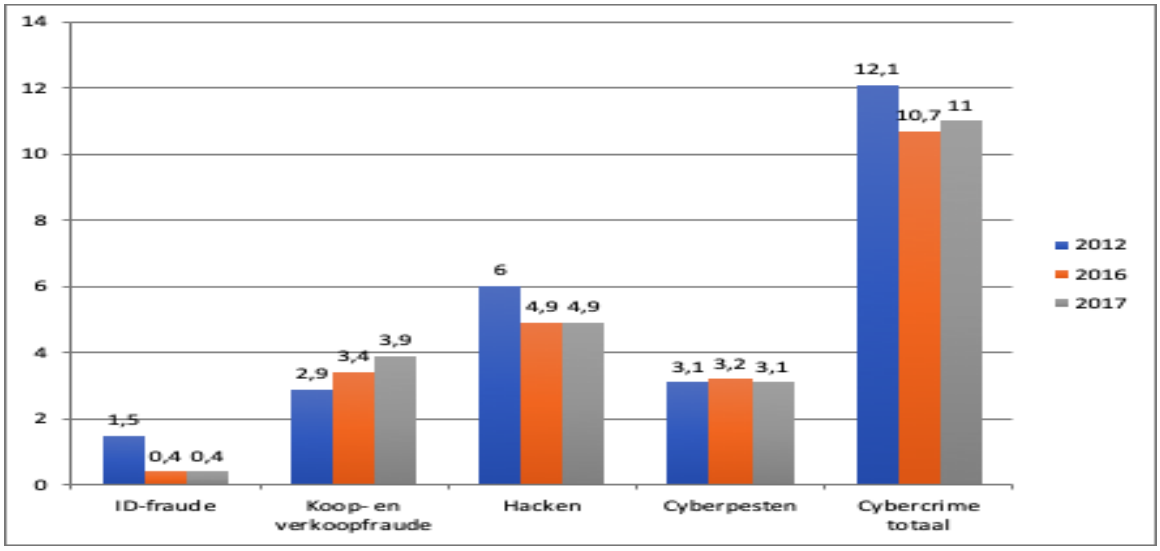
In een poging helderheid te verkrijgen in (onder meer) de definiëring en het bepalen van de omvang van cybercriminaliteit en gedigitaliseerde criminaliteit is in een recent rapport een vergelijkbaar onderscheid gemaakt naar '*cyber-enabled crime*' en '*cyber-dependent crime*' (Smit, et al, 2018). Onder cyber-enabled criminaliteit worden vormen van criminaliteit verstaan die computersystemen gebruiken om een traditioneel misdrijf op een grotere schaal te plegen (ook wel hiervoor gedigitaliseerde criminaliteit genoemd). Onder cyber-dependent criminaliteit vallen vormen van criminaliteit die zonder computersystemen niet mogelijk zouden zijn, en zich expliciet richten op computernetwerken en -systemen (ook wel cybercrime in enge zin).
Bij het bepalen van de omvang van cyberdelicten (cyber-dependent crime) houdt de Politiestatistiek alleen het delict computervredebreuk apart bij. Het ging hier in 2017 om 2.300 delicten. De Veiligheidsmonitor 2017 onder slachtoffers rapporteert 1.050.000 delicten, het gaat hier dan met name om 'hacken'. Ook de Monitor Zelfgerapporteerde Jeugdcriminaliteit rapporteert specifiek over cyberdelicten; het aantal daders onder jongeren van 10 tot 22 jaar bedraagt in totaal 453.000 (Smit, et al, 2018).
Ten aanzien van gedigitaliseerde criminaliteit (cyber-enabled crime) worden deze delicten in de Politiestatistiek wel bijgehouden, maar de gedigitaliseerde delicten zijn niet te onderscheiden van de 'gewone' delicten. Alleen in de Veiligheidsmonitor zijn fenomenen als identiteitsfraude, koop- en verkoopfraude en cyberpesten wel in hun gedigitaliseerde vorm te onderscheiden. Het gaat hier dan om in totaal 1.559.000 delicten (2017).

Slachtofferschap en aangifte van cybercrime

Ook uit slachtofferenquêtes, waaronder de Veiligheidsmonitor, blijkt dat cybercriminaliteit een relevant fenomeen is geworden. Van de Nederlandse bevolking is in 2016 11% slachtoffer geworden van een of meerder vormen van cybercrime; het gaat hier dan onder meer om identiteitsfraude, koop- en verkoopfraude, hacken en cyberpesten (VM, 2017)[4]. Van de delicten waarvan slachtoffers melding maken in de VM, scoort cybercrime met 11% het hoogst.
Van de cybercrimedelicten komt hacken in 2017 het meest voor (5%). Dit wordt gevolgd door koop- of verkoopfraude (4%), pesten via het internet (3%) en identiteitsfraude (minder dan 0,5%).

[4] De cijfers van de Veiligheidsmonitor (uitgevoerd door het CBS) zijn gebaseerd op een grootschalige enquête onder de Nederlandse bevolking van 15 jaar en ouder.

Figuur 1 Slachtofferschap cybercrime, 2012-2017 (in %)



Bron: CBS

Een veelvoorkomend fenomeen is hacken maar ook andere vormen van cybercriminaliteit zoals infecties met malware en allerlei vormen van internetfraude en identiteitsfraude kunnen derhalve als veelvoorkomende cybercriminaliteit worden beschouwd.

Het CBS heeft, in samenwerking met de politie, aanvullend op bestaande onderzoeken een pilotonderzoek 'Digitale Veiligheid & Criminaliteit 2018' uitgevoerd waarin data zijn opgenomen over slachtofferschap van digitale criminaliteit onder internetgebruikers en cybersecurity. Uit dit onderzoek komt naar voren dat In 2018 bijna 1 op de 12 internetgebruikers (8,5 procent) slachtoffer is geweest van digitale criminaliteit. Dit betreft 1,2 miljoen inwoners van 12 jaar of ouder. Jonge internetgebruikers van 12 tot 25 jaar waren met 12 procent het vaakst slachtoffer van digitale criminaliteit; van de 65-plussers was nog geen 4 procent slachtoffer.
Uit de pilotstudie komt onder meer naar voren dat melding en aangifte van hacken nauwelijks plaatsvindt: 5 procent van de slachtoffers meldde dit ergens; minder dan 3 procent deed aangifte bij de politie. Belangrijkste redenen voor het slachtoffer om niet te melden en geen aangifte te doen, waren dat zij van mening waren dat het niet helpt, het niet belangrijk genoeg was, of dat het niet mogelijk was[5].

Ook bedrijven zijn vaak slachtoffer van cybercrime: uit CBS-onderzoek blijkt dat ruim 20 procent van de bedrijven met minstens tien werkzame personen in 2016 te maken heeft gehad met de gevolgen van cyberaanvallen. Vooral bedrijven in de financiële sector en de energiesector hadden hier last van. Bij de helft van de getroffen bedrijven leidden deze aanvallen ook tot hoge kosten[6].

[5] Door het karakter van dit pilotonderzoek zijn er geen vergelijkbare cijfers over eerdere jaren beschikbaar.
[6] CBS, Bedrijven met ICT-incidenten, november 2017.

Van deze delicten wordt echter zelden bij de politie melding gemaakt of aangifte gedaan (van de Weijer en Bernasco, 2016). Van hacks wordt bijvoorbeeld in minder dan 10% van de gevallen door slachtoffers aangifte gedaan. Ook in andere onderzoeken wordt gewezen op lage aangiftepercentages bij zowel individuele slachtoffers (13%; Domenie et al., 2013) als bij organisaties (13%; Veenstra et al., 2015). Bij het MKB doet maar 3,6% een aangifte bij de politie (Veenstra et, 2015). Uit de meest recente Veiligheidsmonitor komt naar voren dat in 2017 8% van de slachtoffers van cybercrime hiervan bij de politie aangifte deed, dit is vergelijkbaar met voorgaande jaren (VM, 2017)[7].

Dergelijke cijfers zeggen niet veel over de feitelijke omvang van cybercriminaliteit, want er wordt een aanzienlijke hoeveelheid niet-geregistreerde cybercriminaliteit vermoed (Leukfeldt, et al, 2010). Het belang van een aangifte is echter groot: het is het startpunt voor een opsporingsproces en het vergroot de kennis over het aantal en de aard van de delicten die worden gepleegd.

1.2 Doel, vraagstelling en aanpak van het onderzoek

Doel van het onderzoek

Cybercrime is inmiddels een centraal thema in verscheidene onderzoeken geworden (Stol, Leukfeldt en Klap, 2012; Stol en Jansen, 2013; Stol, 2014; Leukfeldt en Yar, 2016; Oerlemans, 2017; Stol en Strikwerda, 2017), maar de rol van de Nederlandse politie bij de bestrijding van deze vorm van criminaliteit heeft nog relatief weinig wetenschappelijke aandacht gekregen. Doel van deze verkennende studie is inzicht te krijgen in de organisatorische en inhoudelijke aanpak van cybercrime door drie politie-eenheden van de Nationale Politie. Daarbij is de focus gericht op de aanpak van de politie in het gehele proces van aangifte tot en met de opsporing van cybercrime, met bijzondere aandacht voor cyberteams.

Een van de onderzoeken die in voorgaande jaren naar dit thema is gedaan, komt voort uit het programma van Politie en Wetenschap van 2012. Dit onderzoek toonde aan dat er verschillende knelpunten binnen de politieorganisatie zijn waarop bij de aanpak van cybercrime geïnvesteerd moet worden. Zo zou er geen eenduidige aansturing zijn en er zouden nauwelijks opsporingsonderzoeken worden gestart door een te lage prioriteit bij de teamleiding van de eenheden (Struiksma, et al, 2012). Een studie die de (strafrechtelijke) afhandeling van cybercrime behandelt en de verschillende knelpunten in de rol van de politie daarin is uit 2012 van Leukfeldt, et al. Een onderzoeksnotitie die ingaat op de netwerkpraktijk van de politie bij (onder meer) cybercrime is van Helsloot en Groenendaal (2014). In deze 'working paper' concluderen

[7] Van alle gewelds- vermogens- en vandalismedelicten samen werd in 2017 34 procent bij de politie gemeld. Dit is vergelijkbaar met 2016, maar minder dan in 2012 (38 procent). In 24 procent van de ondervonden delicten werd daadwerkelijk aangifte gedaan; dit is eveneens vergelijkbaar met 2016 en minder dan in 2012 (29 procent). Bron: Veiligheidsmonitor 2017.

zij onder meer dat de politie een zwakke informatiepositie heeft bij de bestrijding van cybercrime en sterk afhankelijk is van de informatie en expertise van andere partijen.

De politie heeft inmiddels op strategisch niveau in de aanpak van cybercrime geïnvesteerd. In onderhavig verkennend onderzoek is nagegaan op welke wijze de politie de bestrijding van cybercrime op eenheidsniveau organisatorisch en inhoudelijk vormgeeft. Mede vanwege de door de politie gekozen 'greenfieldsbenadering' bij de start van de cyberteams, is een selectie gemaakt van drie politie-eenheden om na te gaan hoe zij de aanpak van cybercrime organisatorisch hebben vormgegeven, op welke wijze en in welke mate zij geformuleerde doelen nastreven en invullen en tot welke inzichten dit leidt.

Onderzoeksvragen

De algemene vraagstelling naar de organisatorische en inhoudelijke aanpak van cybercrime door de regionale politie-eenheden is in de volgende deelvragen uiteengelegd:

- op welke wijze is de aanpak van cybercrime bij de politie-eenheden georganiseerd en welke rol hebben cybercrimeteams hierin?
- hoe verlopen de intake en screening van cybercrime bij de politie?
- welke rol heeft een cybercrimeteam bij de opbouw en overdracht van deskundigheid inzake cybercrime binnen de politie-eenheid?
- welke rol speelt informatie en analyse voor het cybercrimeteam bij de aanpak van cybercrime?
- welke opbrengsten behalen de cyberteams naar aantal cybergerelateerde zaken en naar inhoudelijke aanpak/methodiek?
- is er samenwerking bij deze aanpak met andere eenheden, landelijke eenheid (Team High Tech Crime) en externe partijen?

Aanpak van het onderzoek

Voorafgaand aan de start van het onderzoek is geconstateerd dat de politie binnen het brede thema van Digitalisering en gedigitaliseerde criminaliteit 'onderweg' is, maar op verschillende vlakken nog in een ontwikkelingsfase zit. Vanuit deze context heeft onderhavig onderzoek een verkennend karakter, waarbij gekozen is voor een selectie van drie politie-eenheden die deels op verschillende wijzen hun organisatie hebben ingericht om cybercrime te bestrijden. Deze overwegingen hebben geleid tot de opname van de eenheden Noord-Holland, Rotterdam en Oost Nederland in het onderzoek.

Bij de uitvoering van het onderzoek is een aantal methoden toegepast:

- een brede inventarisatie van relevante literatuur en documentatie van landelijke en regionale ontwikkelingen en plannen en van wetenschappelijke bronnen;

- interviews met betrokkenen bij de politie in drie politie-eenheden
  er zijn binnen de drie politie-eenheden interviews op strategisch, tactisch en operationeel niveau afgenomen met een bijzondere aandacht voor de cyberteams. Deze interviews geven een beeld van de wijze waarop de benoemde processtappen bij aanpak cybercrime op eenheidsniveau worden ingevuld. Ook bieden ze zicht op de operationele voorwaarden waaronder men werkt (beschikbaarheid capaciteit, ICT, middelen, e.d.) en van de kennis en kunde rondom cybercrime.
  Er zijn interviews afgenomen met strategisch projectleiders Cybercrime politie, tactisch teamleiders cyberteams, leden cyberteams met een onderscheid naar tactisch rechercheurs, digitaal specialisten en medewerkers uit de informatieorganisatie (informatieanalisten DRIO), leidinggevenden Intake & Service bij blauwe teams en casescreeners;

- interviews met betrokkenen bij de politie op landelijk niveau
  voor het verkrijgen van een landelijk beeld van de doelen en inzichten over de aanpak van cybercrime door de politie zijn interviews afgenomen met de landelijk programmamanager Digitalisering en cybercrime van de politie, met leden van de landelijke projectgroep PIAC en met een senior coördinerend adviseur van de staf van de korpsleiding, directie Operatiën. Daarnaast is een gesprek gevoerd met twee informatieanalisten van de Dienst Landelijke Informatieorganisatie (DLIO) van de politie over de aanpak van cybercrime door de regionale politie-eenheden en over het opstellen van een Nationaal Cyberbeeld;

- interviews met het Openbaar Ministerie
  voor het zicht op de beoordeling van cyberzaken zijn ook interviews afgenomen met beleidsofficieren van justitie bij het OM (‘cyberofficieren’) en parketsecretarissen in de betreffende arrondissementen van de onderzochte politie-eenheden. Ook is een interview afgenomen met een officier van justitie die namens het parket in Den Haag de ‘coördinatie’ voert voor het OM inzake de aanpak van cybercrime. Zij hebben toelichting gegeven op de opsporing van cyberzaken op landelijk en eenheidsniveau in het licht van de gemaakte afspraken in de Veiligheidsagenda 2015-2018;

- interviews met samenwerkingspartners
  Samenwerking met interne en externe partners is door de politie als een belangrijk element aangegeven voor een verbreding van de aanpak van cybercrime. We hebben hiertoe gesprekken gevoerd met deelnemers van het PIAC, met het Team High Tech Crime en een strategisch adviseur van de korpsleiding.

  In bijlage 5 is een overzicht opgenomen van de geïnterviewde sleutelpersonen in het onderzoek.

2 Cybercrime: urgent thema voor de politie

2.1 Cybercrime op de 'agenda' van de politie

De aanpak van cybercrime is voor de Nederlandse politie al verscheidene jaren een reden van aandacht en ook van zorg. Al 15 jaar geleden stelde Wouter Stol In het themanummer 'Cybercrime' van Justitiële Verkenningen het volgende: "Het primaire probleem bij de bestrijding van cybercrime is gebrek aan kennis bij politie en justitie (...)" (Stol, 2004). Deze conclusie had hij ook al eerder getrokken in het onderzoek 'Criminaliteit in cyberspace' (Stol et al, 1999).
Een aantal jaren later wordt deze constatering door andere auteurs herhaald: "Vaststaat dat de digitalisering een serieus criminaliteitsprobleem met zich mee heeft gebracht en dat politie en justitie nog niet goed weten hoe daarmee om te gaan (gebrek aan kennis en digitale vaardigheden). Misschien is het meest basale probleem nog wel dat mensen in cyberspace niet zo eenvoudig zijn te identificeren en te lokaliseren: niet voor andere burgers, maar ook niet voor de overheid" (van Erp et al, 2010). De conclusie van meerdere onderzoekers was dat politie en justitie, zeker in het geval van grensoverschrijdende criminaliteit, nogal wat moeite hebben met misdaadbestrijding in cyberspace (van Erp et al, 2010, Stol et al. 2013; Veenstra et al, 2013).
In de loop van een kleine tiental jaren was wel voortgang te melden: "Het totaalbeeld dat oprijst anno 2012 is dat van een politie die nog flink wat heeft in te halen op de samenleving die haar omringt, niet zozeer omdat er geen actie wordt ondernomen, maar wel omdat de acties nog pril zijn en te veel het karakter hebben van pionierswerk van enkelen (…). 'Digitaal' is ten onrechte nog geen normaal en integraal onderdeel van de politieorganisatie in de volle breedte" (Stol, Leukfeldt & Klap, 2012).

De politie heeft ruim 10 jaar geleden wel de eerste stappen gezet om cybercrime te bestrijden en strafrechtelijk aan te pakken (Domenie et al., 2013). Een concreet voorbeeld is de oprichting van het Team High Tech Crime (THTC) bij de Landelijke Eenheid van de politie in 2007, als vervolg op de groep Digitaal Rechercheren. Het THTC wordt in het rapport 'Handelen naar waarheid' als een succesvol voorbeeld genoemd van vernieuwing binnen de politie (Huisman et al, 2016)[8]. Het team is ook stapsgewijs uitgebreid van 30 naar 120 cyberrechercheurs en is daarmee sinds 2014 op volle sterkte. Het THTC werkt vooral aan landelijke en internationale cyberzaken, heeft inmiddels een zeer gewaardeerde internationale reputatie opgebouwd en is onder meer bekend geworden van een zaak waarbij een illegale online-marktplaats zelf in beheer is genomen (de online-marktplaats 'Hansa' waar illegale zaken werden aangeboden op het 'dark web'[9]).

[8] Huisman, S., Princen, M., Klerks, P. & Kop, N. (2016). *Handelen naar waarheid*. Sterkte- en zwakteanalyse van de opsporing. Amsterdam.
[9] Naast het bekende 'world wide web' bestaat het Darkweb, een online omgeving waarin internetverkeer in sterke mate wordt geanonimiseerd; de sites zijn bijvoorbeeld niet met reguliere zoekmachines te vinden en men kan er browsen zonder traceerbaar te zijn. Een dergelijke anonieme omgeving biedt gelegenheid voor illegale activiteiten, zoals uitwisseling van verboden content (zoals kinderporno), communicatie voor de planning van cyberaanvallen en verkoop van drugs.

Daarnaast is in 2008 het Programma Aanpak Cybercrime (PAC) ingesteld door de Raad van Hoofdcommissarissen en in datzelfde jaar is ook het OM met een programma Cybercrime gestart. Een van de projecten onder de paraplu van het PAC is het Landelijk Meldpunt Internetoplichting (LMIO) dat in 2010 als proeftuin is gestart. Aanleiding voor de start van het LMIO was de toenemende (private) handel via het internet en bijkomende vormen van fraude. Omdat dit type criminaliteit niet plaats- of regio gebonden is, werd voor een effectieve aanpak van deze vorm van criminaliteit landelijke coördinatie op aangiften noodzakelijk geacht.

Naast de (inter)nationale aanpak van cybercrime is men vanaf 2015 ook gestart met een aanpak op het niveau van de regionale politie-eenheden. Daartoe zijn in enkele eenheden 'cybercrimeteams' geformeerd. Deze hebben een 'aanjaagfunctie' voor de bestrijding van cybercrime en dienen tevens een katalysator te zijn voor de digitale ontwikkeling binnen een politie-eenheid. In deze studie zoomen we nader in op de rol van deze cybercrimeteams.

Uit een inventarisatie van het handelen van de politie en het OM bij, onder meer, het bestrijden van cybercrime, bleek dat deze organisaties op meerdere fronten een achterstand hebben in de aanpak van deze vorm van criminaliteit. Zo werd onder andere de afhandeling van cybercrime en (internet)fraude in de basisteams van de politie als ontoereikend beoordeeld. In het rapport 'Handelen naar waarheid' (Huisman, et al, 2016) constateert men dat veel slachtoffers niet worden geholpen en dat de aangiftebereidheid afneemt. Er is, ook volgens deze inventarisatie, vooral nog onvoldoende kennis over cybercrime binnen de politie en het OM.
Er zijn weliswaar specialistische teams opgericht die cybercrime kunnen aanpakken, maar zij worden niet goed ingezet. Digitale criminaliteit krijgt door een gebrek aan mankracht vaak geen voorrang, en bedrijven doen volgens het rapport steeds minder vaak aangifte omdat dit zelden enig effect heeft. In het rapport werd geconstateerd dat in de regionale politie-eenheden geen inzicht is in de instroom van cyberzaken, onvoldoende sturing is op de intake en screening en onvoldoende overleg tussen OM en politie over de afhandeling. Zaken worden niet of te laat opgepakt en er is onvoldoende capaciteit door prioritering van andere zaken (Huisman, et al, 2016).

2.2 Intensivering aanpak cybercrime politie

De conclusies uit voorgaande onderzoeken gaven alle reden om de bestrijding van cybercrime meer aandacht te laten geven door de politie. Het PAC heeft bij de politie mede op basis van de Veiligheidsagenda 2015-2018[10] een vervolg gekregen in de vorm van het Programma Intensivering Aanpak Cybercriminaliteit (PIAC)[11]. Daar waar het PAC meer gericht was op agendasetting, is het PIAC meer gericht op de uitvoering (van der Laan et al, 2016)[12].

[10] Ministerie van Veiligheid en Justitie, Veiligheidsagenda 2015-2018, september 2014.
[11] Nationale Politie, Plan van aanpak intensivering aanpak cybercrime (PIAC), oktober 2016.
[12] Zie ook: A.M. van der Laan, M.G.C.J. Beerthuizen & G. Weijters (2016). Jeugdige daders van online-criminaliteit. Cahier Politiestudies 2016-4, nr. 41, pp. 145-168.

Ook in het PIAC is geconstateerd dat de politie haar positie van achterstand in de aanpak van cybercrime dient te verbeteren: zo wijst men op de beperkte capaciteit voor de aanpak van cybercrime binnen de eenheden, op een ontoereikende informatiepositie van de politie op dit vlak en het niet behalen van resultaatsdoelstellingen. Als zichtbare tekortkoming is bovendien geconstateerd dat de intake van cybercrime niet op orde is waardoor slachtoffers geen gehoor vinden bij de politie. Deze constateringen betekenen volgens het PIAC dat de politie zich op korte en lange termijn sterker moet richten op een effectieve aanpak van gedigitaliseerde criminaliteit en cybercrime (PIAC, 2016).

Speerpunten aanpak cybercrime

Het plan van het PIAC vormt naast het opgestelde strategiedocument[13] de basis voor de huidige aanpak van de politie van cybercrime door de regionale eenheden. In PIAC zijn voor de periode 2017-2020 de volgende zes speerpunten voor de politie benoemd:

- vergroting bewustwording van problematiek van cybercrime bij politie en publiek
- verbetering van intake en screening bij de politie
- opbouwen van informatie- en intelligencepositie binnen de DLIO en DRIO's
- vrijmaken van (tactische) capaciteit binnen eenheden voor samenstelling cyberteams
- verspreiding kennis en kunde binnen politie-eenheden
- samenwerking met publieke en private partners

De speerpunten hangen met elkaar samen; zo is voor het opbouwen van een intelligencepositie een goede intake heel belangrijk, en het speerpunt kennis en kunde is weer een voorwaarde voor het verbeteren van intake en screening. Op basis van genoemde speerpunten streeft de politie aldus naar een verdere op- en uitbouw van 'Cyberintelligence'.

Samenwerking

Om deze cyberintelligence te versterken geeft men in het PIAC aan dat er ook met een aantal externe partijen zal worden samengewerkt. Volgens de notities is er een vorm van samenwerking met het Nationaal Cyber Security Centrum (NCSC), het bedrijfsleven en de non-profitsector om cybercrime tegen te gaan. Zo zijn speciale teams opgericht op landelijk niveau tegen bankenfraude (ECTF: Electronic Crimes Taskforce), kinderporno (TBKK: Team ter Bestrijding van Kinderpornografie en Kindersekstoerisme) en 'high tech crime' (door het THTC). Aangezien cybercrime ook vaak een internationaal karakter heeft, werkt het THTC in de opsporing samen met onder meer Europol, Interpol en de FBI.

[13] Nationale Politie, Cybercrime strategie 2020, Voor een veiliger Nederland, ook in het digitale domein, oktober 2016.

Gelaagdheid in organisatie en aansturing van aanpak cybercrime

Naast de aanpak van cybercrime met een internationaal karakter door het THTC, is er bij de politie derhalve ook een aanpak van cybercrime op eenheidsniveau. Volgens het PIAC is er daarmee een 'gelaagdheid' in de aanpak van cybercrime en vindt verbreding plaats door het werk van het THTC aan te vullen met een regionale aanpak. Cybercrimezaken worden op basis van het Toewijzingskader en beschikbare expertise toegewezen aan de Dienst Landelijke Recherche (DLR), Dienst Regionale Recherche (DRR), districtsrecherche of basisteams.

In het plan van aanpak van PIAC (2016) geeft men aan dat de organisatie en aanpak van cybercrime bij de politie-eenheden in zogeheten 'greenfields' vorm kan worden gegeven, hetgeen betekent dat er ruimte is voor een 'bottom up' benadering vanuit de organisatie. Het model van het THTC wordt daarmee niet naar de eenheden gekopieerd, maar er wordt op basis van een aantal randvoorwaarden in principe rekening gehouden met de 'vertreksituatie' en lokale omstandigheden van de regionale eenheid. In het plan wordt wel gewezen op de randvoorwaarden voor het vrijmaken van voldoende tactische capaciteit voor de samenstelling van cyberteams (zie verder bij cybercrimeteams politie).

De uitwerking van het plan PIAC wordt gevolgd door een werkgroep 'PIAC' waaraan in eerste instantie vertegenwoordigers van eenheden met verschillende functies deelnamen. Het betrof onder meer teamleiders cyberteams, beleidsondersteuners bij de politie, leden van de KMAR, medewerkers verantwoordelijk voor communicatie en leden van het samenwerkingsverband politie en banken. De samenstelling van het PIAC is inmiddels gewijzigd en anders ingedeeld, waarbij in het najaar van 2018 twee platforms zijn ontstaan: een PIAC voor het beleidsgerelateerd overleg van projectleiders cybercrime van de eenheden en een Landelijk Operationeel CyberOverleg (LOCO) van teamleiders van de cyberteams, cyberofficieren van het Openbaar Ministerie en leden van DLIO/Intel.

3 Aanpak cybercrime door de politie

3.1 Doelen van de aanpak cybercrime binnen regionale politie-eenheden

In 2015 zijn in enkele regionale eenheden van de politie, met name in Noord-Holland en Midden-Nederland, cybercrimeteams van start gegaan. Deze cyberteams zijn op dat moment als pilots gestart. Daaropvolgend heeft ook de eenheid Amsterdam een cybercrimeteam geformeerd. De cybercrimeteams in Amsterdam, Midden-Nederland en Noord-Holland zijn ondergebracht bij de Dienst Regionale Recherche; in Noord-Holland en Midden-Nederland als specialistisch team binnen de generieke recherche en in Amsterdam binnen de thematische recherche. In de teams wordt gestreefd naar een samenwerking tussen tactiek en techniek binnen de recherche. De pilots hebben een vervolg en uitbreiding gekregen: inmiddels hebben acht van de tien regionale politie-eenheden de beschikking over een 'cybercrimeteam'; in de eenheid Den Haag is een cyberteam in opbouw (men spreekt van een Expertisecentrum) en in de eenheid Oost Nederland heeft men (in eerste instantie) een andere organisatorische invulling aan de aanpak van cybercrime gegeven dan in de vorm van één centraal 'cyberteam'.

De cyberteams van de politie hebben de volgende hoofddoelen:

- het opsporen en aanhouden van verdachten van cybercrime en het overdragen van de dossiers hiervan aan het OM (het leveren van een vastgesteld aantal cybercrimezaken conform de genoemde afspraken in de Veiligheidsagenda);
- het opbouwen van kennis en ervaring met de aanpak van cybercrime en deze overdragen aan andere teams binnen de eenheid;
- het geven van aandacht aan preventie en het 'weerbaar' maken van organisaties en het publiek voor cybercrime; aspecten die hierin genoemd worden zijn preventie, verstoren, signaleren en adviseren.

Kwantitatieve doelstelling cybercrime politie

In de Veiligheidsagenda 2015-2018 is specifieke aandacht gevraagd voor cybercrime: "De complexiteit van deze vorm van criminaliteit is hoog en daarnaast is de wijze waarop cybercriminelen opereren aan constante verandering onderhevig. Van de politie vraagt dit specifieke expertise en werkwijze. Tevens is preventie van belang bij het voorkomen van cybercrime"[14]. De aanpak van cybercrime heeft daarmee een landelijke prioriteit gekregen voor de politie.

Daarbij zijn twee doelstellingen geformuleerd:

[14] Ministerie van Veiligheid en Justitie, Veiligheidsagenda 2015-2018 (z.d.)

- het terugdringen van cybercrime, door onder andere het vergroten van de weerbaarheid en het treffen van preventieve maatregelen;
- een intensivering van de strafrechtelijke aanpak van cybercrime door het aanpakken van meer zaken.

Om de aanpak van cybercrime te intensiveren en te monitoren zijn door het toenmalige ministerie van Veiligheid en Justitie mede in het kader van de Veiligheidsagenda 2015-2018 ook gekwantificeerde beleidsdoelstellingen voor de politie opgesteld. In de Veiligheidsagenda is aangegeven dat het THTC van de Landelijke Eenheid de specifieke High Tech Crime zaken oppakt conform het toewijzingskader HTC en overeenkomstig de taakstelling van de Dienst Landelijke Recherche. Het gaat hier om complexe zaken zoals een hack van een grote instelling (ziekenhuis) of van vitale infrastructuur, de besmetting door een virus van geautomatiseerde systemen die een essentiële maatschappelijke functie hebben, dan wel de inzet van 'botnets' voor verschillende vormen van vervolgcriminaliteit. De overige (meer of minder complexe) zaken worden in principe bij regionale eenheden belegd.

Bij de algemene landelijke beleidsdoelstelling voor de politie van intensivering van de aanpak van cybercrime met complexe en reguliere zaken[15], streeft men naar:
- een toename van het aantal opsporingsonderzoeken cybercrime naar 360 onderzoeken in 2018 (in 2014 lag deze doelstelling op in totaal 200 reguliere en complexe zaken);
- een toename van het aantal complexe zaken dat wordt opgepakt, conform het toewijzingskader, waaronder minstens 20 zaken door het Team High Tech Crime zaken.

In de volgende tabel is de kwantitatieve doelstelling gepresenteerd met een onderscheid naar reguliere en complexe cyberzaken:

Tabel 1 Kwantitatieve doelen aanpak cybercrime politie (aantal onderzoeken)

Jaar	2014	2015	2016	2017	2018
complexe cyberzaken	20	25	30	40	50
reguliere cyberzaken	180	175	190	230	310
Totaal	**200**	**200**	**220**	**270**	**360**

Bij bestrijding cybercrime wordt aldus enerzijds ingezoomd op het aantal tactisch afgeronde projectmatige onderzoeken door het Team High Tech Crime (THTC), dat conform het opgestelde toewijzingskader opsporing als 'complex' worden beschouwd. Naast het THTC kunnen ook complexe onderzoeken door de politie-eenheden in de regio's worden uitgevoerd; op jaarbasis betreft dat circa 15-20 onderzoeken of grote rechtshulpverzoeken.

[15] In de Veiligheidsagenda wordt onderscheid gemaakt tussen complexe en reguliere cybercrime zaken. Het Toewijzingskader Opsporing is mede bedoeld om handvaten te bieden om het onderscheid in praktijk te kunnen maken en zaken toe te kunnen wijzen. In bijlage 2 zijn ter illustratie voorbeelden van reguliere en complexe cyberzaken besproken.

Daarnaast wordt, met name vanaf 2015, gefocust op de aanpak van reguliere cybercrimezaken. Conform afspraak vindt zowel een telling op basis van OM-gegevens als op politiegegevens plaats, waarbij normstelling op basis van OM-gegevens plaatsvindt.

De taakstelling voor de reguliere cyberzaken voor de politie als geheel heeft ook geleid tot een regionale toedeling van de taakstelling voor de politie-eenheden. Dit betekent dat een politie-eenheid, afhankelijk van de grootte van de eenheid, twintig tot dertig (of meer) zaken, met een jaarlijkse verhoging, dient aan te dragen[16].
Bij deze overdracht van zaken aan het Openbaar Ministerie gaat men voor de telling ten behoeve Veiligheidsagenda uit van de OM-registratie vanuit BOSZ in GPS/Compas van zaken op basis van wetsartikelen die betrekking hebben op cybercrime. Het gaat in dit geval om cybercrime met een aantal specifieke delicten die met de implementatie van de Wet Computercriminaliteit I (1993) en de Wet Computercriminaliteit II (2006) in het Wetboek van Strafrecht zijn opgenomen en/of gewijzigd. Het betreft hier veelal een samenstel van specifieke delicten, waaronder computervredebreuk, malware, websiteaanvallen, botnets, (D)Dos-aanvallen en phishing met gebruik van malware[17].

Het wetsvoorstel Computercriminaliteit III is in juni 2018 door de Eerste Kamer aangenomen. De wet is gericht op de versterking van de opsporing en vervolging van computercriminaliteit. Op basis van deze nieuwe wetgeving, die vervolgens 1 maart 2019 in werking is getreden, mogen politie en justitie heimelijk en op afstand (online) onderzoek doen in computers (pc, mobiele telefoon of server) en cybercriminelen ook zogenaamd 'terughacken'[18]. De politie en het Openbaar Ministerie hebben daarbij tevens de mogelijkheid websites en servers ontoegankelijk te maken als die gebruikt worden voor het plegen van strafbare feiten.

Naast de genoemde kwantitatieve doelen voor cybercrime (in enge zin) is in de Veiligheidsagenda 2015-2018 ook gewezen op een kwalitatieve verbetering van de aanpak mede in het licht van de gedigitaliseerde criminaliteit. In deze gevallen gaat het bijvoorbeeld om online handelsfraude, drugshandel, cyberbedreiging en witwassen van geld met gebruik van internet. Aangezien ook bij de traditionele vormen van criminaliteit steeds vaker sprake is van een digitale component, streeft de politie naar een toename van de digitale expertise binnen de reguliere opsporing. Deze inzet komt bovenop de opbouw van capaciteit en expertise (digitale expertise maar ook tactische recherchecapaciteit) in de eenheden ten behoeve van de aanpak van cybercrime in enge zin.

3.2 Omvang van de geregistreerde cybercrime bij de politie

[16] In bijlage 3 is deze verdeling naar politie-eenheden en jaarschijven weergegeven.
[17] In bijlage 2 zijn deze 10 wetsartikelen benoemd.
[18] De politie mag niet ongelimiteerd 'terughacken': het moet gaan om zware feiten waarvoor 8 jaar of meer gevangenisstraf kan worden opgelegd.

In het voorgaande zijn weliswaar de kwantitatieve doelstellingen van de Veiligheidsagenda besproken, maar is nog geen beeld gegeven van de omvang van de 'cybercrime' waar de politie in ieder geval via haar registraties zicht op heeft. Uit cijfers betreffende de geregistreerde cybercrime bij de politie in Nederland komt over de aangiften, de opgehelderde zaken en het aantal verdachten het volgende beeld naar voren:

Tabel 2 Geregistreerde cybercrime bij de Nationale Politie[19]

jaar	aangiften	opgehelderde zaken	aantal verdachten
2015	2225	165	195
2016	1875	160	210
2017	2300	105	220
2018	2885	240	400

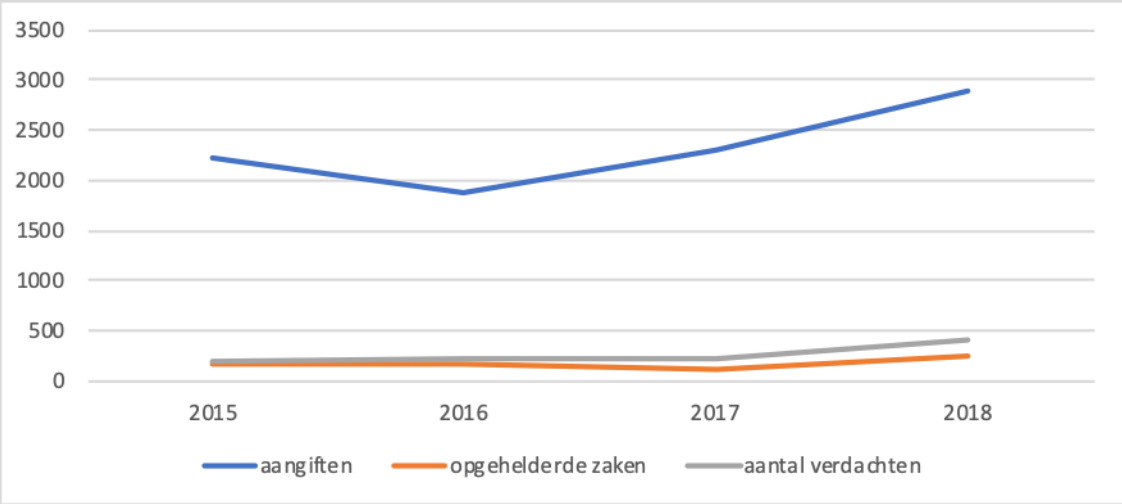
Globaal gesteld zijn tot 2017 op jaarbasis circa 2.000-2.300 aangiften voor cybercrime door de politie opgenomen (in 2016 was sprake van een opvallende dip). Het ophelderingspercentage van deze aangiften lag gemiddeld op 5% - 8% en het aantal verdachten dat jaarlijks door de politie wordt overgedragen aan het Openbaar Ministerie lag tot 2018 op 200-220 personen.

Het aantal door de politie opgehelderde cybercrime-delicten in 2017 is met 4,6% veel lager dan het gemiddelde aantal opgeloste misdrijven door de politie (namelijk 23%). De pakkans van cybercrime is derhalve erg laag. Het aantal geregistreerde aangiften van cybercrime is bovendien slechts een deel van het ondervonden slachtofferschap; uit de VM komt naar voren dat in 27% van de cybercrimegevallen aangifte is gedaan, van bijna driekwart van de cyberdelicten wordt derhalve geen melding gedaan.[20]
Deze gegevens impliceren dat de politie geen accuraat beeld heeft van de aard en omvang van cybercrime en dientengevolge ook nog geen adequaat antwoord heeft op de 'digitalisering van de misdaad'. Stol (2018) wijst erop dat door het lage meldingspercentage de digitalisering van criminaliteit de politie dus nog slechts in beperkte mate raakt; "zo valt niet op dat de politie nog niet goed raad weet met het delict dat tegenwoordig het meeste voorkomt!".

[19] Bron: CBS, op basis van politieregistraties.
[20] Op dit moment is 'computervredebreuk' in de Standaardclassificatie Misdrijven van het CBS de enige categorie die valt onder cybercrime. Internetoplichting en online zedendelicten bijvoorbeeld vallen in deze classificatie onder de categorieën oplichting en seksuele misdrijven. Zowel de politie, die de bron is van de beschrijving van de geregistreerde criminaliteit in Nederland, als het CBS zijn bezig om de registratie en classificatie van cybercrime te verbeteren. Zo heeft de politie nieuwe feitcodes geïntroduceerd voor het classificeren van misdrijven waaronder de feitcode F636 Fraude met onlinehandel. Deze feitcodes vormen de basis van de indeling van misdrijven in de Standaardclassificatie Misdrijven. Vanaf juni 2015 zijn de meldingen van internetoplichting gedaan bij het Landelijk meldpunt Internetoplichting (LMIO) opgenomen in de bij de politie geregistreerde misdrijven. Deze meldingen vallen grotendeels samen met de feitcode Fraude met onlinehandel en komen in de Standaardclassificatie Misdrijven terecht in de categorie Oplichting. In 2016 kwamen er 42.169 meldingen van het LMIO; in 2017 37.329.

De gegevens van de politieregistratie van de aangiften en het aantal zaken van cybercrime over het jaar 2018, geven aan dat het aantal aangiften van cybercrime bij de politie is toegenomen en dat verhoudingsgewijs meer zaken door de politie worden aangepakt en opgelost (met een ophelderingspercentage van 8,3%). Het aantal aangehouden verdachten van cybercrime stijgt van 220 in 2017 naar 400 in 2018.

Figuur 2 *Aantal aangiften, opgehelderde zaken en aantal verdachten cybercrime bij de politie, 2015-2018*



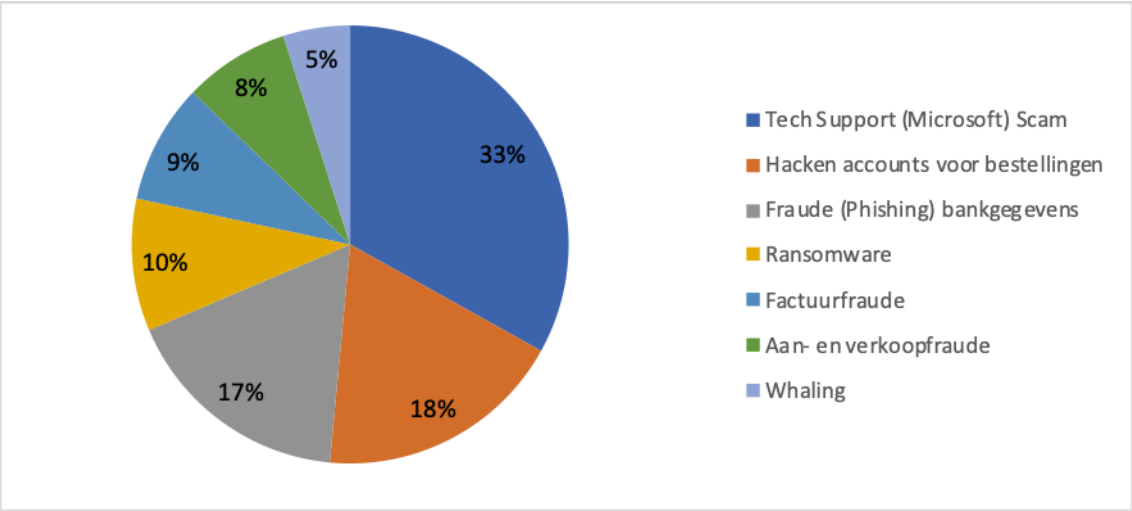
Cybercrime wordt lang niet altijd gemeld, niet bij de politie, maar ook niet bij een andere instantie. Als het wel wordt gemeld, is dit niet altijd (ook) bij de politie maar soms zelfs vaker bij een andere instantie. Zo wordt identiteitsfraude het vaakst gemeld bij de bank of financiële instelling en beduidend minder vaak (ook) bij de politie (CBS, 2018). Identiteitsfraude wordt het vaakst gemeld (86%) onder andere omdat het vaak gepaard gaat met verlies van geld en de bank geïnformeerd wordt om bijvoorbeeld de rekening te blokkeren. Bij de andere onderscheiden vormen van cybercrime ligt dit percentage aanzienlijk lager. Ook is er een aantal procentpunten verschil tussen slachtoffers die een cybercrimedelict melden bij de politie (13,1% van de slachtoffers wil dat de politie er weet van heeft in 2017) en de slachtoffers die dit ook feitelijk laten vastleggen in een proces-verbaal van aangifte (8% van de slachtoffers)[21].

[21] CBS, Cybersecuritymonitor 2018. In het onderzoek van het CBS is naar een gelimiteerd aantal typen cybercrimedelicten gevraagd, namelijk identiteitsfraude, hacken, koop- en verkoopfraude en cyberpesten.

Aard van de cybercrime

Op basis van informatie verkregen van DLIO is een beeld te geven van de aangiften bij de politie naar de aard van de cybercrime[22]. In de periode 2016-2018 is de Tech Support (Microsoft) Scam de meest voorkomende vorm van cybercrime in de politieregistraties. Hacken van accounts voor bestellingen ('account take over') en fraude van bankgegevens, i.c. internetbankieren ('phishing') zijn ook twee vormen van cybercrime die veelvuldig worden gepleegd. Daarnaast komen factuurfraude (de CEO-fraude) en aan- en verkoopfraude (waaronder fraude op onlinehandelssites zoals Marktplaats) relatief vaak voor.

Figuur 3 Aangiften bij de politie naar aard van cybercrime, totaal van 2016-2018

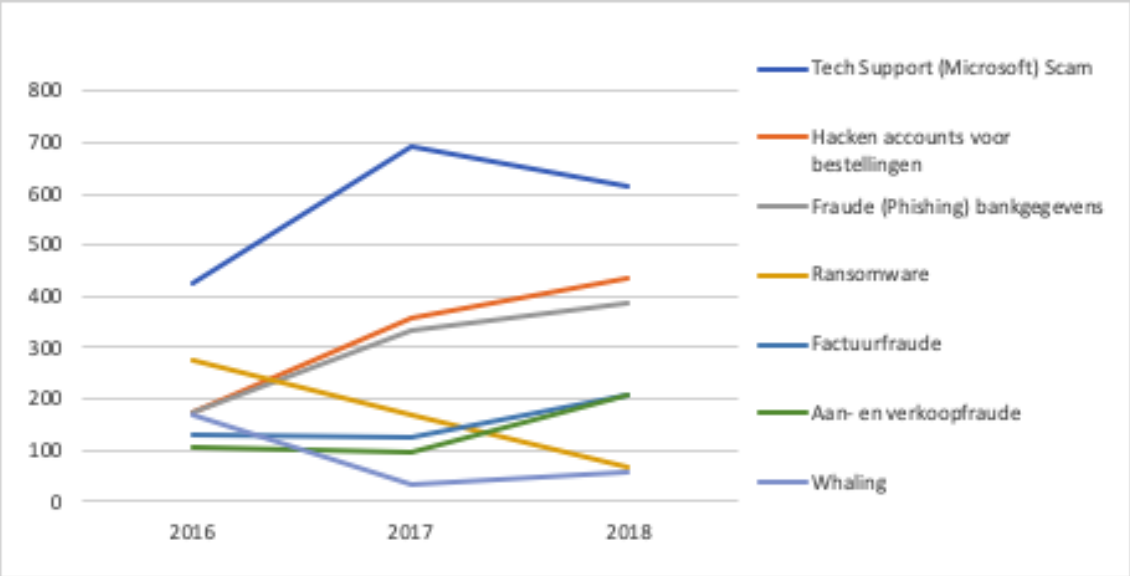


Het hacken van accounts voor bestellingen en 'phishing' zijn twee vormen van cybercrime die sinds 2016 zijn toegenomen. Dit geldt tevens, maar in mindere mate, voor de CEO-fraude en aan- en verkoopfraude. Er is in de politieregistraties sinds 2016 een daling te zien in de aangiften betreffende 'ransomware' en 'whaling'[23] (zie figuur 4).

[22] De weergave van de aard van de aangiften is gebaseerd op door DLIO verzamelde cijfers van steeds de eerste helft van het jaar van respectievelijk 2016, 2017 en 2018 en van zeven politie-eenheden waar alle registraties van beschikbaar waren (van Midden-Nederland, Oost-Brabant en Den Haag waren geen cijfers bekend). Het gaat hier om circa 70 procent van de registraties (op basis van 2016). De cijfers zijn derhalve geen landelijke totalen, maar zijn zo door DLIO gekozen dat ze de landelijke trend zo goed mogelijk weergeven.

[23] Bij 'whaling' krijgt het slachtoffer een 'alarmerend bericht' van iemand uit de vriendenkring of familie. Die zit zogenaamd in het buitenland vast en is zijn geld, telefoon en papieren kwijt. Of een betaling is niet gelukt en hij vraagt of dit kan worden voorgeschoten. De 'kennis' vraagt dringend om financiële hulp via een sociaal netwerk als Facebook, Whatsapp of simpelweg via e-mail. Het bericht kan een dwingende toon hebben. Achteraf blijkt dat het account op het sociale netwerk gekraakt is door een oplichter. Behulpzame vrienden die geld overgemaakt hebben, beseffen pas later dat zij zijn opgelicht.

Figuur 4 Aangiften bij de politie naar aard van cybercrime, trend 2016-2018



Alle politie-eenheden ontvangen met name aangiften van de Tech Support Scam (voorheen Microsoftfraude) en het hacken van accounts voor bestellingen (bij onder andere Vodafone, Marktplaats, Wehkamp en Bol.com). Bij deze cyberdelicten zijn veelal burgers slachtoffer geworden. Dit politie herkent dit vooral bij de 'Microsoft scam': burgers worden gebeld door een Engelssprekend persoon met Indiaas accent die zegt van Microsoft te zijn. Deze persoon laat zien dat de gebelde veel problemen op zijn computer heeft (virussen, et cetera) en vraagt om toegang tot de computer. Wanneer dat eenmaal is gelukt, dan krijgt hij ook vaak de gevraagde toegang tot het internetbankieren en haalt de rekening van de aangever leeg. Bij hacken en misbruik voor bestellingen is een account van de aangever gehackt en dit wordt misbruikt om allerlei producten te bestellen of om producten aan te bieden en niet te leveren (vooral dure mobiele telefoons). Ook ransomware staat in de Top 5 van veelvoorkomende cybercrime, hetgeen vaak voor komt bij kleine bedrijven: zij krijgen een mail met een URL-link en wanneer deze wordt geopend blokkeert malware de computer en kunnen ze alleen nog toegang krijgen door een bedrag (meestal in bitcoins) te betalen. Feitelijk valt dit onder chantage en afpersing. Bij phishing voor bankgegevens krijgen de burgers (i.c. slachtoffers) een mail met een URL-link die afkomstig lijkt van de bank. Wanneer ze de link openen worden ze doorgeleid naar een website die lijkt op die van de bank en daar wordt ze gevraagd om allerlei persoonlijke gegevens (inloggegevens) prijs te geven.
Van deze vormen van cybercrime worden vooral particulieren het slachtoffer. Bij bedrijven is men vooral slachtoffer van ransomware, gevolgd door 'hacken overig', factuurfraude, CEO-fraude en Ddos-aanvallen[24].

[24] Bron: DLIO, 2018.

3.3 Aanpak van cybercrime in drie politie-eenheden

Capaciteit aanpak cybercrime politie

Voor de samenstelling van de cybercrimeteams bij de regionale politie-eenheden is men bij de start van de teams uitgegaan van een minimale bijdrage van 10 fte uit de tactische recherche-capaciteit. De teams zouden daarmee derhalve een 'minimale ondergrens' dienen te hebben van 10 fte. De teams hebben een tactisch teamleider die verantwoordelijk is voor de operationele afstemming met de cyberofficier van het Openbaar Ministerie in de betreffende regio. Ook is deze in principe verantwoordelijk voor overleg en afstemming met cyberteams van andere regionale eenheden en met het landelijk THTC.
In het plan van het PIAC (oktober 2016) is aangegeven dat het gaat om *tijdelijke* cyberteams in elke eenheid; bovendien dienden de afspraken over het vrijmaken van capaciteit in overleg met het lokaal gezag plaats te vinden. De cyberteams krijgen volgens het plan de ruimte om te experimenteren en te leren; de 'greenfieldbenadering' betekent dat deze teams in nauwe samenspraak met andere partijen kunnen zoeken naar de oplossing van het veiligheidsprobleem bij cybercrime.

Bij de cybercrimeteams van de regionale eenheden is tactische capaciteit vrijgemaakt vanuit verschillende afdelingen en teams; zo zijn de leden van de cyberteams afkomstig uit de Dienst Regionale Recherche, de districtsrecherche, de basisteams recherche, maar ook uit het Team Digitale Opsporing (TDO) en de DRIO waar digitaal specialisten en informatieanalisten werkzaam zijn. De ruimte die de teams hebben in de organisatorische aanpak komt ook naar voren in de invulling van functies en ook waar de capaciteit vanuit de eenheid vandaan komt. Zo kan een cyberteam ook blauwe collega's betrekken om de overdracht van kennis en kunde naar de basisteams beter mogelijk te maken, hetgeen een stimulans kan zijn voor de bestrijding van Veel Voorkomende Cyber Crime (waaronder hacken, phishing en e-fraude).

Bij een beoordeling van de samenstelling van cyberteams komt naar voren dat voor de inzet op cybercrime een minimale capaciteit van 10 fte vereist is om deze aanpak "serieus" te laten zijn; als teams te klein blijven, komt de bestrijding cybercrime onvoldoende uit de verf. In de praktijk blijkt dat er verscheidene kleinere cyberteams in de eenheden zijn: het cyberteam in Midden Nederland heeft 8 fte, het team in Zeeland 4 fte en in Oost Brabant heeft men minder dan 10 fte en in de eenheid Den Haag heeft men formeel geen capaciteit voor een cyberteam, evenals in de eenheid Oost Nederland (tot 2019).
Over de cyberteams landelijk heen kijkend is er derhalve een ongelijke verdeling tussen teams, "terwijl (zoals een van de teamleider stelt) we steeds meer last hebben van cybercrime". Door teamleiders van enkele cyberteams wordt aangegeven dat men het "onhandig" vindt dat niet alle eenheden aan de ondergrens van de gewenste capaciteit voldoen of niet een vergelijkbare organisatie hebben. Dit betekent namelijk dat zij onvoldoende mogelijkheden hebben om gezamenlijk landelijke onderzoeken op te pakken ("sommige cyberteams hebben gewoon te weinig capaciteit en dan kunnen we er niet goed mee samenwerken").

De cyberteams hebben ook binnen hun eigen eenheid, formatief beschouwd, een relatief kleine rol. Zo heeft de eenheid Noord-Holland een totale formatie van circa 3800 fte en het cyberteam 25 fte; volgens de teamleider in verhouding met totale eenheid dus “een klein clubje…”.

Cybercrimeteams in Noord-Holland, Rotterdam en Oost Nederland

In het onderzoek naar de bestrijding van cybercrime door de politie zijn drie politie-eenheden als cases geselecteerd. Daarbij is met name gekeken naar de organisatie en inhoudelijke vormgeving en uitvoering van de aanpak van cybercrime. We bespreken eerst kort de organisatie van de aanpak bij de drie politie-eenheden.

Cybercrimeteam Noord-Holland

In de eenheid Noord-Holland is men, als een van de eersten van de politie-eenheden, in september 2015 gestart met het voorbereiden van een operationeel cybercrimeteam. In deze eenheid was er al enige affiniteit en betrokkenheid met een vergelijkbare materie vanwege de gehanteerde aanpak van het LMIO (mede) in deze eenheid in het geval van internetoplichting. Het cyberteam in Noord-Holland is ontstaan uit een behoefte binnen het regionaal recherche-overleg, waarbij ook een ‘portefeuille cybercrime’ is benoemd. Begin 2016 is vervolgens het cyberteam samengesteld; eerst een klein team (met teamleider, een coördinator en twee rechercheurs) en daarna is deze uitgebouwd naar 16 fte. De periode 2016-2017 is eerst als een proefperiode beschouwd voor het cyberteam. In de regio Midden Nederland had men iets eerder een cyberteam (juni 2015), maar dit was en is een klein team met circa 7 leden.
Het cyberteam in Noord-Holland is als operationeel team ‘vanaf de grond opgebouwd’ en zij hebben het landelijke team THTC min of meer als voorbeeld genomen voor de vormgeving van het team (ware het niet dat het THTC een meer internationale oriëntatie heeft). Het cyberteam in Noord-Holland is inmiddels een van de grote teams met een capaciteit van circa 25 fte. Ook de teamleider geeft aan dat ze ‘veel capaciteit’ voorhanden hebben, ook in vergelijking met andere cyberteams. De basis van het team wordt gevormd door leden van de generieke opsporing (10 fte) en leden van vier ‘blauwe’ basisteams vanuit de districten die ieder 3 leden leveren, gezamenlijk derhalve 22 fte. Het team bestaat daarnaast uit twee digitaal specialisten van het TDO (die min of meer ‘vast’ in het team zijn opgenomen), een informatieanalist (gedetacheerd vanuit DRIO) en een rechercheur die vanuit team Finec (financieel economische criminaliteit) een bijdrage levert. In het team wordt een roulatiesysteem toegepast, waarbij iedere 9-12 maanden de leden van de basisrechercheteams weer teruggaan naar hun team en nieuwe leden in het cybercrimeteam worden opgenomen. De formatie die nu beschikbaar is, is op detacheringbasis vanuit de teams; het team is wel een ‘staand team’, in ieder geval tot eind 2019.
Bij de start van het team in 2015 heeft men ook een tijdelijke bijdrage gehad van de vrijwillige politie, waarbij 2-3 ‘techneuten’ met interesse voor IT in het team zijn opgenomen. Inmiddels maken de Landelijke Eenheid (het Darkwebteam) en het cybercrimeteam van de eenheid Rotterdam gebruik van leden van de vrijwillige politie (zie verder).

Cybercrimeteam Rotterdam

Het cybercrimeteam van de politie in de eenheid Rotterdam heeft een langere aanloopfase gehad voordat het tot stand kwam en is als centraal, zelfstandig team feitelijk operationeel sinds januari 2018. Men heeft voor de organisatie van het cyberteams het model van Noord-Holland overgenomen. Dit betekent dat men een 'staand team' heeft opgezet, met een verdeling van de capaciteit naar verschillende specialismen. Het team heeft een personele sterkte van 25 fte, waaraan naast de teamleiding vanuit de Dienst Regionale Recherche (4 fte), 10 tactisch rechercheurs, 7 rechercheurs vanuit de districten (ieder district levert 1 rechercheur), een informatieanalist vanuit DRIO en een Finec-medewerker deelnemen. In het cyberteam is geen personeel van het TDO, dat in Rotterdam zelf over 25 fte beschikt, opgenomen; het TDO geeft met circa 4 personen wel 'op afroep' ondersteuning aan het cyberteam bij de briefing en bij specifieke cyberzaken.
Het cyberteam heeft "als lerend team" in Rotterdam een projectstatus voor de duur van twee jaar en kent derhalve geen vaste borging in de politieorganisatie. Het cyberteam heeft wel als een centraal opererend team ook een 'vliegwielfunctie' voor de opbouw van cyberkennis in de hele politie-eenheid.

Het samenstellen van het cyberteam met de gewenste deskundigheid bleek op basis van de beschikbare en nieuwe instroom van recherchecapaciteit binnen de politieorganisatie niet eenvoudig te zijn. Bovendien kampt men met een uitstroom vanuit de bestaande formatie. Bij de voorbereiding van het cyberteam diende in eerste instantie ook de mogelijke waarde van het cyberteam bij de eenheidsleiding te worden benadrukt, hetgeen voortkomt uit de onbekendheid met het onderwerp en de materie ("een volstrekt onbekend terrein").

In de Rotterdamse situatie is er bovendien een groot belang van een goede bescherming van organisaties en bedrijven in de zeehaven tegen cyberaanvallen op computersystemen. De gemeente en bedrijven in de zeehaven van Rotterdam richten zich daarbij met name op een versterking van de 'cybersecurity' met veel aandacht voor 'cyberresilience' (een verzameling maatregelen die ervoor zorgt dat organisaties weten hoe zij moeten handelen tijdens een cyberaanval). Globaal gesteld betreft dit het 'digitaal weerbaar maken' van de Rotterdamse haven. Vanuit de politie neemt de Zeehavenpolitie hierin het voortouw en richt zich daarmee op andere aspecten van cybercrime dan het cyberteam van de (reguliere) Rotterdamse politie. Zo is het fenomeen van 'storage spoofing'[25] een delict dat voornamelijk door de Zeehavenpolitie wordt opgepakt en niet door het cyberteam. Het cyberteam en de Zeehavenpolitie hebben mede vanwege de verschillende aandachtsvelden binnen de 'cybersecurity' en cybercrime geen expliciete (intensieve) samenwerkingsrelatie.

[25] Storage Spoofing is een verzamelterm voor verkoop van niet-bestaande opslagcapaciteiten en voorraden van grondstoffen en materialen in terminals in het Rotterdamse havengebied. De doelgroep zijn in de eerste plaats de (inter)nationale ondernemers en potentiële kopers die producten aangeboden worden die niet blijken te bestaan. Daarnaast zijn bedrijven die zelf opslagterminals in het havengebied hebben potentieel slachtoffer van deze vorm van fraude, omdat hun naam en netwerk door cybercriminelen misbruikt kan worden.

Organisatie aanpak cybercrime Oost Nederland

In de politie-eenheid Oost Nederland is formeel geen sprake van 'één cyberteam', maar is de aanpak van cybercrime vormgegeven door een bundeling van verschillende teams met digitale kennis op vier centrale locaties in de eenheid (de locaties Apeldoorn, Elst, Enschede en Zwolle). Deze opbouw is mede een gevolg van de keuze van de eenheid Oost Nederland om de aanpak van criminaliteit en de opbouw van kennis, ook wat betreft cybercrime, 'horizontaal', vanuit een 'breedte-benadering', te organiseren en niet te bundelen in vaste centrale teams[26]. In de aanpak wordt door Oost Nederland een brede invalshoek gekozen waarbij zowel sprake is van cybercrime, van gedigitaliseerde criminaliteit als van zaken die andere delicten of onderwerpen raken waarbij een 'digitale component' is te onderscheiden (zoals bijvoorbeeld ook bij milieuzaken). Vanuit deze brede invalshoek beschouwd heeft men circa 1600-1800 meldingen van incidenten die deels een link hebben naar 'cybercrime'. Bij een beoordeling van deze zaken blijkt dat naar schatting circa 15% een digitale component heeft. De inzet van capaciteit vanuit de eenheid gaat daarbij met name naar onderzoeken met een digitale component.

De uitvoering van de aanpak is verspreid over operationeel specialisten A en tactisch rechercheurs (met een 'digitale labeling') in de vier locaties. Voor deze uitvoering zijn in principe 15 rechercheurs vanuit de Dienst Regionale Recherche, 7 rechercheurs vanuit thematische teams en 13 fte vanuit de districtsrecherche van de gehele eenheid beschikbaar (verdeeld over de regio's Gelderland Midden en -Zuid, Noord Oost Gelderland, Twente en IJsselland). Deze capaciteit is beschikbaar voor de aanpak van 'gedigitaliseerde criminaliteit' in brede zin.
De betreffende rechercheurs kunnen in geval van 'cyberzaken' inhoudelijke en operationele ondersteuning aanvragen bij digitaal specialisten van het TDO (die een capaciteit van 16 fte heeft).

De verdeling van de inzet over vier locaties vloeit mede voort uit de wens van het lokale gezag om ook lokaal/regionaal aandacht te besteden aan onder meer cybercrime. Bij de vier locaties is de inzet voor cybercrime in de afgelopen jaren sterk uitgebreid, waarbij ook zij-instromers zijn opgenomen met meer digitale expertise. Vanuit de DRIO worden gegevens verzameld en geanalyseerd door informatieanalisten en aan het TDO ter beschikking gesteld met een verrijking van de informatie voor een opsporingsindicatie. De DRIO van de eenheid Oost Nederland is derhalve niet opgenomen in een 'cyberteam', maar stelt 5 fte beschikbaar voor de informatie- en analysefunctie bij de aanpak van cybercrime.

Uitbreiding capaciteit aanpak cybercrime bij de politie

De toegenomen beleidsaandacht voor de aanpak van cybercrime door de politie heeft medio 2018 geleid tot plannen voor de uitbreiding van de politiesterkte voor deze aanpak vanaf 2019 (tot 2023) met in totaal 143 fte. Van deze uitbreiding wordt 48 fte toegekend aan de Landelijke

[26] In de politie-eenheid Oost Nederland is inmiddels besloten in 2019 een 'cybercrimeteam' op te gaan richten dat een capaciteit zal krijgen van 16 fte.

Eenheid en voor de regionale politie-eenheden komt in totaal 95 fte uitbreiding. In de praktijk betekent dit dat de cyberteams in de eenheden met 9,5 fte worden uitgebreid, waardoor zij, in principe, een basisformatie zouden kunnen krijgen van 19,5 fte per team. De uitbreiding is aangekondigd in de Kamerbrief van de minister van J&V van juni 2018[27] en nader ingevuld in de Begroting en Beheerplan Politie 2019-2013[28]. De uitbreiding is volgens dit plan "voor de benodigde versterking van de eenheden en de al bestaande cybercrimeteams voor de aanpak van cybercrime. Daarbij zal de nadruk liggen op intelligence & analyse, preventie, verstoring en publiek private samenwerking".

3.4 Meldingen en aangiften van cybercrime bij Intake en Service

Van cybercrime kunnen burgers en bedrijven via het centrale telefoonnummer van de politie of op een politiebureau aangifte doen. De politie geeft op haar landelijke website aan dat van een aantal vormen van cybercriminaliteit ook online aangifte gedaan kan worden, maar dit geldt vooralsnog alleen voor internetoplichting (dat in strikte zin beschouwd geen cybercrime is, maar een vorm van gedigitaliseerde criminaliteit).
De aangiftebereidheid van cybercrime is, zoals we al hebben laten zien, laag (uit CBS-cijfers blijkt dat een kwart van de gevallen van slachtofferschap van cybercrime wordt gemeld) en een belangrijk deel van de meldingen van cybercrime komt niet bij de politie terecht maar bij andere instanties. Uit cijfers over slachtofferschap van cybercrime blijkt dat 74% van de meldingen van slachtofferschap bij banken of andere financiële instanties wordt gedaan en in 10% bij andere instanties; 20% van de meldingen van slachtofferschap van cybercrime wordt (ook) bij de politie gedaan (CBS, 2017). Bij een vergelijking van de delicten binnen cybercrime blijkt dat met name online-oplichting (bij koop- en verkoopfraude) vaker ook bij de politie wordt gemeld (in gemiddeld 25% van de gevallen).

Bij een melding van cybercrime of een vorm van gedigitaliseerde criminaliteit komt de burger, het bedrijf of de organisatie als eerste in contact met een medewerker Intake & Service. Uit eerder verricht onderzoek bij de politie (Toutenhoofd-Visser et al, 2009) kwam naar voren dat sprake was van een fragmentarische kennis onder intakers van de zes onderzochte eenheden. In de praktijk betekent dit dat volgens de auteur dat "de ene intaker iets van een bepaalde vorm van cybercrime weet en een andere intaker wat van een andere vorm van cybercrime". De kennis van intakers inzake cybercrime is volgens dit onderzoek vooral gebaseerd op min of meer toevallige praktijkervaringen en niet op een daartoe ontwikkelde deskundigheid of specialisme (Toutenhoofd-Visser, et al, 2009). Uit dit onderzoek bleek tevens dat opmerkelijk weinig aangiftes van cybercrime of gedigitaliseerde criminaliteit werden opgenomen. Het ontbreken van kennis met betrekking tot cybercrime en gedigitaliseerde criminaliteit bij de medewerkers van het Regionaal Service Centrum (RSC) speelde hierin een rol. Het resulteert volgens de on-

[27] TK, Brief van de minister Middelen regeerakkoord politie en flexibiliseringsagenda, 15 juni 2018, kenmerk 2281115.
[28] Nationale Politie, Begroting en Beheerplan Politie 2019-2013, z.d.

derzoekers in situaties waarbij slachtoffers bellen voor een afspraak om een aangifte op te laten nemen en dat de RSC-medewerker al tegen de mensen zegt dat de politie niets kan doen in dat specifieke geval. Hierdoor worden in sommige gevallen slachtoffers ten onrechte de mogelijkheid ontzegd om aangifte te doen (Toutenhoofd-Visser, et al, 2009; Bout, 2017). Ook uit andere onderzoeken komt naar voren dat medewerkers bij Intake & Service onvoldoende kennis hebben om de melding op de juiste waarde in te schatten en af te handelen (Leukfeldt, Veenstra, Domenie, & Stol, 2012).
Een deel van de problematiek heeft te maken met de rol van het RSC in het proces van de totstandkoming van een aangifte (Bout, 2017). Zij hebben de taak om burgers die het algemene nummer van de politie bellen, goed te informeren over wat zij kunnen verwachten en wat zij mee moeten nemen voor een eventuele intake. Daarnaast maakt het RSC een eerste screening aan de hand van de melding van de burger, op basis waarvan zij bepalen of er wordt overgegaan tot een intake (Boekhoorn & Tolsma, 2015).

Een belangrijk knelpunt bij de bepaling van de aard en omvang en mogelijke aanpak van cybercriminaliteit bij de politie, is de relatieve onbekendheid met cyberdelicten van medewerkers bij Intake & Service en bij het RSC. Deze onbekendheid met de materie heeft onder meer tot gevolg dat bij de melding ervan mogelijke cyberzaken niet als zodanig worden herkend en daardoor ook onder een andere incidentcode in het systeem worden geregistreerd (cyberzaken zijn dan 'weggeschreven' onder bijvoorbeeld de classificatie fraude, oplichting, diefstal, et cetera). Ook uit onderzoek van Huisman en anderen (2016) kwam naar voren dat onder meer het opnemen van aangiften van cybercrime en (internet)fraude ondermaats is. Dergelijke aangiften worden vaak -onterecht- afgedaan als civiel geschil. In meerdere voorgaande onderzoeken wordt in dit kader ook gewezen op de ontoereikende kennis van intakers, hetgeen de oorzaak zou zijn van de lage kwaliteit van de aangiftes inzake cybercrime (Liedenbaum & Kruijsen, 2008, Toutenhoofd- Visser et al., 2009, Kouwenhoven et al., 2010 en Leukfeldt, Veenstra, Domenie, & Stol, 2012).
De onbekendheid met cybercrime heeft anderzijds tot gevolg dat medewerkers van Intake & Service ook meldingen van 'traditionele' vormen van criminaliteit (met een 'digitaal tintje') binnen de maatschappelijke klasse van 'computercriminaliteit' plaatsen (de F90 code binnen BVI) terwijl feitelijk geen sprake is van cybercrime. Het gebruik van de F90 code bij de politie geeft daarmee een deel van de werkelijkheid van het slachtofferschap van cybercrime weer.

Aangiften van cybercrime in de drie politie-eenheden

Uit de verzamelde gegevens over meldingen en aangiften van cybercrime bij de drie onderzochte politie-eenheden, blijkt dat deze per jaar en tussen de eenheden fluctueren (onafhankelijk van de grootte van de regio van de politie-eenheden). Ook is er een sterk uiteenlopende rato bij de eenheden tussen het aantal meldingen van cybercrime en de aangiften die daaruit voortvloeien.

In de eenheid Noord-Holland (die 48 gemeenten beslaat en 10 basisteams heeft) zijn in 2017 470 aangiften gedaan van cybercrime (bij een selectie in BVH op de maatschappelijke klasse

F90). In 2018 had de eenheid in Noord-Holland circa 10 tot 15 nieuwe meldingen per week van cybercrime. In 2018 zijn door de politie in Noord-Holland 538 aangiften opgesteld en zijn daarnaast 91 meldingen van cybercrime binnengekomen die niet tot een aangifte hebben geleid (in totaal 629 'incidenten'). In de eenheid Rotterdam (die 32 gemeenten beslaat en 17 basisteams omvat) had men in 2017 225 aangiften, dit is in 2018 toegenomen naar 298 aangiften. In de eenheid Oost Nederland (die 79 gemeenten beslaat en 28 basisteams omvat) heeft men in 2017 in totaal 270 aangiften opgemaakt van 'cybercrime'; in 2018 waren dit er 140 (bij 1776 geregistreerde incidenten).
Opmerkelijk zijn onder meer de verschillen in de verhouding tussen meldingen en aangiften: in Noord-Holland leiden de meldingen in veel gevallen ook tot een feitelijke aangifte; dit geldt in mindere mate voor Rotterdam en in Oost Nederland is deze verhouding geheel anders.
De scheve verhouding tussen het hoge aantal meldingen en het relatief lage aantal aangiften in Oost Nederland in 2018 geeft een indicatie dat relatief veel meldingen en mogelijke cyberzaken niet in behandeling worden genomen. Ook het absoluut aantal aangiften is in dat jaar laag. Wijzigingen in de registraties van 'cybercrime' en 'gedigitaliseerde criminaliteit' spelen hierin mogelijk mede een rol.

Tabel 3 *Geregistreerde aangiften (en incidenten) computercriminaliteit bij de drie onderzochte politie-eenheden*[29]

aangiften	Noord-Holland	Rotterdam	Oost Nederland
2015	220	210	385
2016	290	150	215
2017	470	225	270
2018	629 incidenten; 538 aangiften	801 incidenten; 298 aangiften	1776 incidenten; 140 aangiften

De fluctuatie van het aantal aangiften van cybercrime over de jaren en van het aandeel aangiften op het aantal meldingen (incidenten) geeft mede een indruk van de verschillen in onbekendheid en in interpretatie van het delict 'cybercrime' bij de afdelingen Intake & Service en bij de cyberteams van de eenheden. In het Cyberbeeld van Oost Nederland wordt deze problematiek als volgt geformuleerd: "De kwaliteit van de politie-informatie is divers te noemen. Zo bestaat de ene mutatie in de BVH uit één zin met de melding dat de aangever is gehackt terwijl een andere mutatie meerdere pagina's van gedetailleerde informatie bevat. Deze verschillen in de kwaliteit zijn eigen aan alle BVH-mutaties maar als het om cybercrime gaat, speelt nog de kennis en houding van de verbalisant mee. Sommige collega's zijn in mindere of meerdere mate bekend met het thema en kunnen makkelijk doorvragen naar relevante gegevens terwijl weer andere collega's het verhaal van een aangever over cybercrime duidelijk niet begrijpen".

[29] Incidenten zijn alle meldingen, aangiftes en andere mutaties in de Basisvoorziening Handhaving (BVH) bij elkaar. Een betrekkelijk groot deel van de informatie over cybercrime komt in de politiesystemen in de vorm van een melding en niet als een aangifte.

De politieregistratie en de omgang met de meldingen van 'cybercrime', respectievelijk het opstellen van een aangifte, zijn met andere woorden niet eenduidig en weerspiegelen slechts een deel van de 'cybercriminaliteit'.

Landelijke query cybercrime

Om de omissies en misinterpretaties in de meldingen die mogelijk cybercrime-gerelateerd zijn te verminderen, heeft de politie besloten aanvullend een landelijke query binnen Cognos te ontwikkelen. Er is hiertoe in eerste instantie een aparte screening gedaan van F90-zaken door het cyberteam van Midden-Nederland, "om te kijken wat daar feitelijk tussen zit".

DLIO heeft in een vervolgfase registratiecijfers over een periode van anderhalf jaar verzameld en per eenheid verstrekt (met behulp van de door de DLIO verbeterde landelijke cyberquery). De query haalt registraties uit heel BVH en niet alleen om F90 en het gaat niet alleen om aangiften maar ook om meldingen. Voor de analyse is een instructie gemaakt zodat alle eenheden op dezelfde wijze registraties labelen.
Uit diverse analyses blijkt dat het onderscheid tussen cybercrime en gedigitaliseerde criminaliteit lastig te hanteren is, aangezien diverse vormen van cybercrime verweven zijn met allerlei vormen van gedigitaliseerde criminaliteit. Dit komt ook in een aanvullende analyse van DLIO naar voren. Bijna de helft van de registraties waarin een cybercomponent door DLIO is gevonden gaat over gedigitaliseerde criminaliteit, maar in veel gevallen kan er discussie zijn over de vorm die het betreft. Microsoftfraude, om een voorbeeld te noemen, kan zowel gedigitaliseerde criminaliteit als cybercrime in enge zin zijn afhankelijk van de modus operandi die is toegepast[30].

In aansluiting hierop wordt door leden van de regionale cyberteams op basis van bepaalde teksten en woordcombinaties door het hele aangiftesysteem gekeken of het om cybercrime of gedigitaliseerde criminaliteit gaat. Een deel van de cyberzaken staat namelijk niet onder F90 (maatschappelijke klasse 'computercriminaliteit') weggeschreven, maar onder andere maatschappelijke classificaties (fraude, oplichting, diefstal, stalking, belediging, et cetera)[31]. Een van de voorbeelden van cybercrime die men bij de cyberteams noemt is de "exen-hack" die bij de aangifte door de Frontoffice in BVH onder de incidentcode 'echtelijke twist' wordt geplaatst. Op basis van een nieuwe 'brutolijst' van delicten die door deze 'search' ontstaat, wordt vervolgens een nadere analyse gemaakt om de 'echte' cyberzaken eruit te halen. De query wordt aldus door de cyberteams toegepast om de meldingen van cybercrime beter boven tafel te krijgen en deze vervolgens te kunnen beoordelen voor mogelijke vervolgstappen in de screening.

[30] Bloem, B. en A. Harteveld, Aantal gedupeerden bij cybercrime, notitie DLIO, 2018. Een recent onderzoek dat ook zicht geeft op mogelijkheden tot classificatie, betreft predictieve textmining in politieregistraties, cyber- en gedigitaliseerde criminaliteit (Tollenaar, et al, 2019).
[31] In voorgaande jaren is in een pilotfase in enkele politieregio's een query gebruikt met behulp van het programma BRAINS. Daarbij werd gezocht naar relevante zaken in de totale verzameling aangiften, aan de hand van zowel de maatschappelijke klassencode F90 als een aantal termen die gerelateerd zijn aan computercriminaliteit. Het programma BRAINS is echter niet meer operationeel bij de politie.

Uit de interviews komt naar voren dat de cyberteams hiermee meer en andersoortige cyberzaken beter in beeld krijgen. Het overgrote deel van de meldingen die men eerst ziet betreffen met name cyberdelicten die met 'hacken' hebben te maken; het hacken van Facebook-accounts, het hacken van accounts van webwinkels, van voormalige echtelieden en het cyberpesten.

Ondersteuning Intake & Service

Een methode om, naast de query, een vollediger en adequater zicht te krijgen op de meldingen en aangiften is in eerste instantie een ondersteuning en versterking van de deskundigheid van medewerkers bij Intake & Service. Zo is ten behoeve van de nadere bepaling van de melding door een burger of bedrijf een 'Handreiking cybercrime en gedigitaliseerde criminaliteit' voor medewerkers van I&S opgesteld bij de opname van aangiften. Er zijn instructies beschikbaar en via intranet te raadplegen. Bovendien wordt een module e-learning cybercrime aan alle I&S-medewerkers aangeboden. Ondanks deze inzet is het algemene oordeel van betrokkenen bij de cyberteams dat deze niet tot een grote verbetering heeft geleid.
Vervolgens is ook een web-app ontwikkeld waarbij voor intakemedewerkers, maar ook anderen, sneller duidelijk moet worden of bij aangifte sprake is van cybercrime[32].
Bij de eenheid Noord-Holland wordt daarnaast door het Cybercenter voorlichting gegeven aan medewerkers van Intake & Service, maar de opbrengsten van deze voorlichting worden laag ingeschat ("is een gebed zonder eind"), "het komt niet of nauwelijks over bij de meeste medewerkers van I&S". "We adviseren ze om gewoon de zeven gouden W's af te lopen; maar daar is nog een hoop te winnen". Als aanvulling op deze aanpak is de afspraak gemaakt dat de Front-office altijd het cyberteam kan bellen over de gewenste afhandeling; vraag is hierbij voornamelijk of de aangifte van het delict in BVH binnen de maatschappelijke klasse F90 moet worden opgenomen of niet.
Ook binnen de eenheden Oost Nederland en Rotterdam worden voorlichtingsbijeenkomsten en trainingen over 'cybercrime' gegeven aan medewerkers van I&S, maar ook zij zien weinig vooruitgang door middel deze vorm van algemene deskundigheidsbevordering bij I&S; "de aangifte van cybercrime is gezien de inhoud altijd lastig en de minst opgeleide zit aan de balie waar juist veel deskundigheid nodig is voor de vraagverheldering". Dit vraagt om een kennisvergroting van cybercrime bij de medewerkers van I&S maar het is wellicht niet reëel om van iedere I&S-medewerker een hoge mate van deskundigheid te verwachten ("krijg je I&S überhaupt voldoende toegerust voor deze taak bij cybercrime? Waarschijnlijk niet…"). Dit betekent onder meer dat binnen I&S eerder ruimte zou moeten zijn voor 'taakaccenthouders cybercrime' die als centrale verwijzers zouden kunnen fungeren binnen I&S ("de uitvraag kan en moet veel beter").
De leidinggevenden van de cyberteams geven naast voorlichting aan medewerkers van I&S, ook voorlichting aan de basisteams recherche (BTR) en -zoals in Noord-Holland- aan de recent

[32] https://webapps.politieacademie.nl/cybercrime. Via intranet kunnen politiemensen ook beschikken over 'Herkennen en veiligstellen van digitale apparatuur' en 'Opsporing in een gedigitaliseerde samenleving.' Ook experts kunnen helpen via digitale platforms. Een digitaal platform bestaat uit mensen met meer dan gemiddelde digitale kennis en vaardigheden en dient binnen de regionale eenheid als extra verbinding tussen TDO en de politiemensen die bij hun zaak technische ondersteuning nodig hebben. Een digitaal platform verleent dus als het ware eerstelijns digitale ondersteuning (Stol & Strikwerda, 2017).

ingestroomde vrijwillige leden van politie in het cyberteam. Bij de voorlichting aan de BTR's bemerkt men dat er belangstelling is voor cybercrime, "maar bloed gaat voor computer, dus hun prioriteit voor dit onderwerp ligt niet altijd hoog" ('blood over bits'). Hierdoor ziet het cyberteam zich genoodzaakt de cyberzaken die aan de basdisteams worden overgedragen nog beter voor te bereiden.

3.5 De screening van cybercrimezaken

Uit voorgaande onderzoeken kwam naar voren dat de lage kwaliteit van de aangifte tot gevolg had dat belangrijke informatie in de aangifte ontbrak, waardoor aangiften al tijdens de casescreening werden opgelegd, i.c. niet in behandeling werden genomen (Leukfeldt, Veenstra, Domenie, & Stol, 2012). Ook het verrijken van de aangiften cybercrime en gedigitaliseerde criminaliteit werd volgens dit onderzoek als lastig ervaren. Het is daarbij niet duidelijk welke informatie betrokkenen moeten verzamelen om een aangifte cybercrime of gedigitaliseerde criminaliteit te verrijken. Daarnaast is men voor het verrijken van informatie veelal afhankelijk van derden voor het verstrekken van IP-adressen, NAW-gegevens en dergelijke. De daarvoor vereiste inspanningen en gebrek aan ervaring met dit soort opsporingswerk werpen veelal een drempel op om cybercrime of gedigitaliseerde criminaliteit delicten op te pakken. Daarbij wijzen de verschillende onderzoeken er op dat de kwaliteit van het casescreenen per district of eenheid kan verschillen door één onverwachte factor, zoals bijvoorbeeld de persoonlijke interesses van een betrokken politiefunctionaris (Bout, 2017).

De behoefte aan een uitgebreide query en nadere analyse van de cyberzaken vanuit de BVH wijzen erop dat ook het belang van een goede screening van cyberzaken groot is, niet alleen vanwege de te kiezen aanpak in de opsporing maar ook voor de vervolging van de cyberzaak. Het gaat hierbij niet alleen om een goede selectie van aangiften van cyberzaken die door I&S zijn opgemaakt en die worden opgepakt maar ook de selectie van cyberzaken vanuit de opgestelde query. De landelijke query is niet dekkend voor de delicten vallend onder 'gedigitaliseerde criminaliteit'.
Bij de bepaling van zaken of zij 'cyberwaardig' zijn, geldt onder meer dat deze vallen binnen de 10 wetsartikelen die door het OM worden gehanteerd voor het vervolgen van 'computercriminaliteit' (zie bijlage 2). Een casescreener bepaalt aldus of een cyberzaak in behandeling wordt genomen en zo ja door welk team. Bij de screening en weging hanteert de casescreener allerlei kaders, zoals richtlijnen van het Openbaar Ministerie.

In de drie onderzochte eenheden zijn en worden verschillende wegen bewandeld om een adequate screening van cyberzaken (beter) mogelijk te maken.
In Noord-Holland is de screening van mogelijke (cyber)zaken in eerste instantie alleen op de (recherche)basisteams vormgegeven. Er is een operationele coördinator (OC) voor screening die de zaken voorbereidt voor BOSZ (de chef van het rechercheteam is hierin verantwoordelijke). In de praktijk bleek echter dat veel cyberaangiften werden opgelegd door de basisteams

recherche en de districtsrecherche waardoor het leek alsof er geen of weinig cyberzaken waren. Sinds voorjaar 2018 wordt door leden van het cyberteam 'meegekeken' voor de screening via het mede daartoe ingerichte 'Cybercenter'. Met dit cybercenter van 6 fte (met een recherche-assistent, een recherchekundige voor de overdracht van zaken, twee rechercheurs en twee digitaal specialisten) worden de basisteams als door een soort 'hulploket' ondersteund, aangezien in de daaraan voorafgaande fase alleen door "blauwe mensen zonder opsporingsidee" naar de aangiften werd gekeken.
Het opgerichte Cyber Center binnen het cyberteam en de aldaar werkzame 'leader intake en screening' zijn nu verantwoordelijk voor de dagelijkse en juiste screening van meldingen en aangiften op 'cyber' via de landelijke query en ook voor de werkvoorbereiding voor de cyberzaken voor de basisteams. Daarnaast is er een wekelijkse duiding van zaken die centraal zijn gescreend. Het cyberteam zelf zorgt daarmee zelf voor de screening, veredeling en vervolgens 'panklaar' neerleggen van de cyberzaken bij de basisteams. Het cybercenter stelt daartoe ook de vorderingen op en veredelt de informatie. Deze aanpak sluit ook beter aan bij de afspraken die met het OM over ZSM-zaken zijn opgesteld. Hiermee wordt ook duidelijker welke zaken de basisteams uitvoeren en kunnen ook door het Cyber Center van het cyberteam mogelijke trends snel(ler) worden onderkend. Wordt de 'zaak te groot' voor een basisteam, dan blijft de aanpak in principe bij het cyberteam.

Het merendeel van de zaken kan echter worden opgelost door het basisteam recherche; het gaat daarbij onder meer om phishing, sextortion, hacking mails (van ex-partners), hacking online en CEO-fraude. Zaken die sinds kort ook voorkomen betreffen 'whaling' hetgeen een variant is van phishing, waarbij naar geld wordt gevraagd via Whatsapp. Het betreft een hack van Whatsapp, via gegevens van Facebook en ofschoon er een digitale component in zit opgenomen is het geen cybercrime (in strikte zin), maar is het een vorm van gedigitaliseerde criminaliteit. Deze zaken worden vervolgens veelal niet opgepakt door het cyberteam maar door de districtsrecherche.

Het cyberteam in Noord-Holland is primair gericht op het aanpakken van cybercrimezaken, maar daarnaast neemt men ook zaken op die als gedigitaliseerde criminaliteit worden omschreven. In het laatste geval zijn dat vaak 'samengestelde' zaken waarbij gekeken wordt naar de haalbaarheid voor de opsporing en het mogelijk leereffect van zaken voor het cyberteam. Mede gezien het grote aantal cyberzaken die men onder de noemer 'veel voorkomende cybercriminaliteit' kan vatten, is er een sterke behoefte bij dit team (en ook bij andere cyberteams) om meer innovatieve aanpakken te ontwikkelen voor meer complexe zaken. Men wil eerder kunnen ingaan op signalen en hiervoor methoden ontwikkelen; "meer aan de voorkant gaan zitten….".

De casescreeners in de eenheid Oost Nederland zijn niet opgenomen bij het 'cyberteam', maar vallen onder het Operationeel Coördinatie Knooppunt (OCP) dat onderdeel is van het basisteam. De casescreeners beoordelen de aangiftes op volledigheid en inhoud, met de volgende vragen: is sprake van een strafbaar feit; zijn alle bestandsdelen die in de wetteksten staan, aanwezig in de aangifte; zit er voldoende opsporingsindicatie in de aangifte? Als aan een van

de drie volledigheidscriteria niet is voldaan, gaat de aangifte inclusief de feedback terug naar degene die de aangifte heeft opgenomen voor aanvulling of verbetering (Bout, 2017). De indruk is dat de aangiften van cybercrime vanwege deze criteria 'sneller uitgescreend' worden. In Oost Nederland is de casescreening daarmee in eerste instantie een verantwoordelijkheid van het OCP bij de basisteams, maar om deze screening van cases te verbeteren is een specifiek project 'screening' gestart waarbij leidinggevenden van het TDO de aangiften op 'cyberkenmerken' screenen. Ook in Oost Nederland wordt een groot belang toegekend aan de rol van de casescreener ("nog belangrijker dan van de I&S-medewerker"), maar ook bij deze functie is verbetering gewenst. Een belangrijke tekortkoming ziet men hierbij in het nagenoeg ontbreken van de opbouw van digitale kennis in de politieopleidingen; "ook aan de nieuwe lichtingen van politiemensen wordt nauwelijks een digitale component in de opleiding aangeboden en ontbreekt het aan basiskennis op het gebied van de aanpak van cybercrime".
Om de screening verder te verbeteren is er een tijdelijke inzet geweest van een parketsecretaris van het Openbaar Ministerie die op het politiebureau steekproefsgewijs aangiften en dossiers controleerde op kwaliteit. Daarnaast heeft de parketsecretaris regelmatig presentaties over onderwerpen gegeven waarvan zij vermoedde dat daaraan een behoefte was onder de medewerkers van het basisrechercheteam. De aanwezigheid van de parketsecretaris werd als zeer positief ervaren, maar door de beperkte aanwezigheid concludeerde men in voorgaand onderzoek dat de kwaliteitsbewaking van de aangiften niet structureel was (Bout, 2017).

De screening van aangiften gebeurt in de politie-eenheid Rotterdam eveneens op de districten bij de basisteams, maar men heeft bemerkt dat op deze wijze relatief weinig opsporingsinformatie wordt gevonden als het om (mogelijke) cyberzaken gaat. Aangezien cyberzaken vaak niet worden herkend, worden de aangevers in Rotterdam vaak een tweede keer benaderd, maar dan door leden van het cyberteam. Om de screening te verbeteren, is (tijdelijk) een aparte casescreener in het cybercrimeteam opgenomen die zich specifiek heeft gericht op het herkennen van cyberzaken op basis van de ontwikkelde (landelijke) query die daarna verder is verfijnd.
De query wordt (inmiddels werd) dagelijks gescand door een medewerker van het cyberteam, waarna de casescreener de mogelijke cyberzaken importeert in een Excel-bestand en deze in eerste instantie beoordeelt op basis van de F90 codering maar op ook mogelijke andere cyberzaken (hacking, phishing, e.d.) die niet als zodanig meteen herkenbaar zijn. De selectie van incidenten is gedaan op basis van de Bluespot Report rapportage 2853 - Landelijke Query Cybercrime. Elke registratie wordt aldus gelezen en vervolgens wordt er duiding aan gegeven welke vorm van cybercrime het is. De casescreener bij het cyberteam geeft vervolgens een opsporingsindicatie aan de zaak (of niet) en maakt samenvattingen van de cyberzaken die mogelijk worden doorgestuurd. Een van de parketsecretarissen van het OM kijkt in een tweewekelijks overleg vervolgens ook naar deze geselecteerde zaken voor een check op basis van de wetsartikelen voor cybercrime en voor een 'inkleuring' van de mogelijke aanpak. Daarna wordt besloten om de zaak te behandelen en over te dragen naar het cyberteam of naar een district, naar gelang capaciteit en gewenste deskundigheid.

De uitgebreide screening van cases biedt ook de mogelijkheid op bepaalde momenten mogelijke trends in de cyberzaken te herkennen, bijvoorbeeld bij een 'hype' aan meldingen van 'hacking' van accounts van webshops (zoals bij Bol.com en Wehkamp).

Een nadere screening van meldingen wordt mede toegepast vanwege de KPI die is vastgelegd in de Veiligheidsagenda 2015-2018. Deze kwantitatieve doelstelling betekent volgens leden van de cyberteams dat "je eerst een wasstraat van ZSM-zaken voor cyber bent om de gestelde aantallen te halen…, maar daar leer je als cyberteam weinig van als het om bepaalde fenomenen gaat in de cybercrime". Voorbeeld van een (reguliere) cyberzaak met een ZSM-karakter is "een winkeldief die een '*jammer*' op zak heeft om te voorkomen dat de signalen van detectiepoortjes afgaan".

Informatieanalyse bij aanpak cybercrime

Voor de verrijking van de cyberinformatie is er, naast de rol van de casescreeners, ook een rol van informatieanalisten van de DRIO in de regionale eenheden. Deze informatieanalisten hebben onder meer tot taak een analyse op patronen van mogelijk bij elkaar horende zaken te maken, waardoor kan worden achterhaald of mogelijk sprake is van het werk van een criminele bende.

In de eenheid Oost Nederland heeft DRIO onder meer een rol in de nadere screening van (cyber)zaken die op basis van de query naar boven komen. Dit geldt niet zozeer voor de F90-cyberzaken (daar wordt de screening met name ondersteund door twee leidinggevenden van het TDO) maar eerder voor de zaken die op basis van een analyse van de vrije tekst in de query opvallen. Dit levert een veelvoud aan zaken op in vergelijking met de reguliere registratie via de F90-code (in het laatste geval betreft het in Oost Nederland 5-6 zaken per week, bij een selectie in het vrije tekstgedeelte circa 40 registraties per week). In de query wordt van een brede benadering uitgegaan waarbij het niet alleen cybercrimezaken betreft maar ook gedigitaliseerde criminaliteit. Deze benadering is ook van belang voor de informatiepositie van DRIO, want het betekent ''opbouw van intelligence in brede zin". De DRIO in Oost Nederland heeft 5 fte beschikbaar voor de informatie- en analysefunctie bij de aanpak van cybercrime.
Ook in de twee andere eenheden is het thema 'Digitaal' in de DRIO opgenomen en is een operationeel specialist werkzaam binnen dit thema. In de eenheid Noord-Holland zijn vier (informatie)analisten werkzaam, die een verdeling kennen naar strategisch analist, zaaksanalist, informatieanalist en een informatiecoördinator (themahouder). Een van de analisten wordt specifiek ingezet voor ondersteuning van het cyberteam. Deze analist houdt zich specifiek bezig met het beoordelen van trends in de meldingen van cybercrime en het analyseren van data voor het verkrijgen van zicht op mogelijke dadergroepen. DRIO Rotterdam beschikt over 5 fte, waaronder 3 'inforechercheurs', 1 OSINT-rechercheur en 1 informatieanalist. De DRIO in Rotterdam is 'zo dicht mogelijk' bij het cybercrimeteam geplaatst, maar heeft ook taken voor andere afdelingen. In het kader van de verbetering van de herkenbaarheid van cyberaangiften, heeft DRIO via Blue Intel een methode ontworpen om aangiften automatisch in te laden en daarvan snel een grafische weergave te presenteren.

Thematische benadering in analyse cybercrime

De DLIO en DRIO's werken samen aan de opbouw van een 'informatie & intelligencepositie' op het gebied van Cybercrime (dit doen ze onder meer door het opstellen van cyberdashboards voor overzicht en het gebruiken van cyberintelligence tools voor duiding van informatie en actiegerichte beslissingen). Daartoe worden eenheidsbeelden gemaakt, waarvan de doelstelling is het in kaart brengen van cybercrime en het duiden van informatie gericht op handelingsperspectieven voor de politie (en zo mogelijk ketenpartners). In een opdracht vanuit de politieleiding is omschreven dat elke DRIO een Eenheid Cyber Beeld (ECB) maakt en de 11 ECB's zouden in principe samen een Nationaal Cyber Beeld (NCB) kunnen vormen. Inhoudelijk fungeert het NCB als verlengstuk van het Nationaal Dreigingsbeeld (NDB).

De DRIO's van de onderzochte (en andere) politie-eenheden hebben, op eigen initiatief en zonder beleidsmatige aansturing, voor een verbetering van de informatiepositie naar samenwerking gezocht en een aantal cyberthema's onderling verdeeld zodat daarop enige specialisatie kan worden opgebouwd.
Daarbij zijn vijf thema's zowel binnen cybercrime als van gedigitaliseerde criminaliteit geselecteerd met de meest voorkomende vormen en met de grootste toegebrachte schade voor burgers. Informatieanalisten van de onderscheiden politie-eenheden richten zich daarbij op:

- phishing (Rotterdam)
- CEO-fraude en koop- en verkoopfraude (Noord-Holland)
- Ddos-aanvallen (Oost Nederland)
- accounthackers van webshops (Den Haag)
- helpdeskfraude, ook wel 'tech-support scams' genoemd (zogenaamd van 'Microsoft', door Intel politie Noord-Nederland)

Enkele DRIO's van politie-eenheden in het zuiden van het land houden zich specifiek bezig met ransomware. De informatieanalisten van de DRIO's hebben hiertoe zelf het initiatief genomen om aanvullende kennis te ontwikkelen, waarbij geen vaste kaders van tevoren zijn vastgesteld. De inzet van de DRIO's is gericht op het ontwikkelen van cyberbeelden bij de verschillende thema's en op het zoeken naar specifieke daders van cybercrime. Voor het onderzoeken van mogelijke trends in de onderscheiden cyberthema's wil men samen met DLIO ook vaker externe partijen betrekken, maar deze samenwerking is nu nog beperkt.

3.6 Voorbeelden van onderzoeken door de cybercrimeteams

De cyberteams richten zich vanuit de afspraken in de Veiligheidsagenda in hun taakstelling op de aanpak van cybercrime (in enge zin) maar krijgen in de praktijk veel meldingen waarbij ook

sprake is van een vorm van gedigitaliseerde criminaliteit. De scheidslijn tussen cybercrime en de aanpak van gedigitaliseerde criminaliteit is daarbij niet altijd scherp te trekken.
Om een beeld te geven van de aanpak, schetsen we een aantal voorbeelden van de inzet van de cyberteams naar verschillende cyberonderwerpen. Het centrale criterium dat teamleiders van de cybercrimeteams aangeven voor de inzet van de politie bij cyberzaken is: *"waar de burger en bedrijven last van hebben bij cybercrime"*.

Phishing

Een van de voorbeelden van de aanpak van cybercrime betreft onderzoek naar 'phishing' (cyberteam Noord-Holland)[33]. Hiertoe is samenwerking gezocht met de media (programma TROS Opgelicht) en met het bankwezen (ECTF). Voor dit onderzoek zag het cyberteam NH zich genoodzaakt nieuwe methoden te ontwikkelen met zowel een digitale inzet (met digitaal specialisten) als een inzet vanuit de recherche. Knelpunt hierbij is dat er digitale, technische kennis aanwezig is bij de personen die vanuit het TDO in het cyberteam worden ingezet, maar dat men minder vaardigheden heeft in de tactische opsporing. Om dit deels op te lossen wordt vaak in 'koppeltjes' gewerkt met een tactisch rechercheur en digitaal specialist; de kennis van beide politiemensen wordt op deze wijze zo veel mogelijk in het team geïntegreerd.

Sextortion

Een ander voorbeeld van aanpak van cybercrime betreft onderzoek naar afpersing via de chat en webcams naar aanleiding van seks georiënteerde filmpjes ('sextortion')[34]. De leider van het cyberteam heeft de indruk dat hiermee veel slachtoffers worden gemaakt, terwijl het aantal aangiften feitelijk laag is.

Tikkiefraude

Een volgend voorbeeld van de aanpak van cybercrime (door cyberteam Noord-Holland, in samenwerking met het cyberteam van Zeeland-West Brabant) betreft een maandenlang onderzoek naar Tikkiefraude, via Markplaats[35]. Daarbij zijn relatief veel slachtoffers gemaakt (er zijn

---

[33] De schade bij banken door phishing is in 2018 bijna verviervoudigd ten opzichte van 2017. Volgens de Betaalvereniging Nederland, de branchevereniging voor het betalingsverkeer, liep de schade door fraude bij internetbankieren op van een miljoen euro in 2017 naar bijna vier miljoen euro vorig jaar. Oplichters worden steeds creatiever en sturen steeds betere phishing-mails, waarin ze slachtoffers verleiden op een malafide link te klikken. Daar maken ze inloggegevens voor internetbankieren afhandig en halen ze de rekening leeg.

[34] Sextortion is afpersing met een seksueel getinte foto of video van het slachtoffer. Dit kan een naaktfoto of video van het slachtoffer zijn, maar het kan ook zijn dat webcambeelden van iemand zo gemonteerd worden dat het lijkt alsof het slachtoffer seks heeft met een minderjarige, zodat ook op deze manier gechanteerd wordt met het online zetten van materiaal. De afperser wil meestal geld of juist meer pikante foto's of video's van het slachtoffer. Vaak zijn de foto's en video's gestolen via social media, e-mails, door het overnemen van webcams of door het stelen van apparatuur.

[35] Slachtoffers die op Marktplaats een advertentie zagen met een mobiel telefoonnummer erbij, namen via WhatsApp contact op met de verkoper. Om vertrouwen te winnen werd voorgesteld om met de Tikkie-app een betaling van € 0,01 te doen. De verdachten beschikten over een phishing-website die identiek was aan de originele website van Tikkie. De kopers op Marktplaats werden naar deze namaaksite gelokt. Vervolgens kreeg de koper tijdens de pogingen om in te loggen en de eurocent over te maken een aantal malen een foutmelding. Gedurende de inlogpogingen werd door de verdachten, met de gephishte inloggegevens van het slachtoffer, toegang tot diens bankrekening verschaft en deze in zeer korte tijd leeggeroofd. Het cybercrimeteam heeft 42 aangiften in behandeling genomen. Eerder in dit onderzoek was door het cybercrimeteam Noord-Holland al een inval bij de verdachten gedaan om computers en telefoons in beslag te nemen. Zij werden daarbij bijgestaan door collega's van de politie-eenheid

40 aangiften gedaan) en het door de daders (jongens van 17 en 18 jaar in Brabant) hiermee verworven geld is vervolgens geïnvesteerd in de aan- en verkoop van drugs op het 'darkweb'.

Hacking

De cyberteams geven aan dat veel tijd en energie wordt besteed aan het natrekken van meldingen van 'hacking' in allerlei vormen. Een voorbeeld (van cyberteam Noord-Holland) is de hack van een account van een bekende YouTube-ster. Daarbij is begin 2018 een dader aangehouden voor 'computervredebreuk' die het niet alleen op de YouTube-ster had gemunt, maar ook tientallen accounts van andere bekende en onbekende Nederlanders hackte. In de visie van de teamleider van het cyberteam was dit een 'grote zaak' met veel slachtoffers, die succesvol is afgesloten met de aanhouding en bekentenis van de dader. De media-aandacht die deze zaak heeft gehad, heeft mogelijk ook tot gevolg dat de bewustwording bij het publiek voor dergelijke delicten toeneemt.

Tech Support Scam

Een veel voorkomende vorm van 'cybercrime' (feitelijk gedigitaliseerde criminaliteit) die men in de politie-eenheden registreert, is de 'Tech Support Scam' (Microsoft fraude). Zo vormt deze vorm van cybercrime een kwart van de meldingen bij het cyberteam in Rotterdam. Op initiatief van de politie-eenheid Rotterdam en het Openbaar Ministerie is in de aanpak voorjaar 2018 een convenant met private partijen ondertekend. Het convenant heeft tot doel tot verstorende maatregelen te komen ten aanzien van de Tech Support Scam (TSS). Een van deze verstorende maatregelen is het blokkeren van telefoonnummers, door de Autoriteit Consument & Markt (ACM), waarmee slachtoffers worden gebeld. In deze periode is tevens veel aandacht in de media besteed aan deze vorm van cybercrime, maar er is slechts een kleine daling zichtbaar in het totaal aantal incidenten van deze vorm van cybercrime en blijft daarmee dus een groot probleem.

Een nieuwe variant hiervan is gebaseerd op het 'inbreken' door criminelen op het zoekgedrag van burgers op het internet. Indien burgers 'googlen' op de helpdesk van gerenommeerde bedrijven zoals Microsoft, Norton, McAfee of Adobe, krijgt men vervolgens een Engelssprekende 'medewerker' aan de lijn die hen op dezelfde wijze oplicht als bij de klassieke Microsoft fraude door gebruik te maken van verschillende nep-websites. Het cybercrimeteam Rotterdam heeft dit fenomeen in samenwerking met Openbaar Ministerie opgepakt en daarin tracht men ook 'verstorend' op te treden.

Hacken van accounts van webshops

Zeeland-West-Brabant in Oosterhout. In de woning van een van de verdachten werd een flinke hoeveelheid soft- en harddrugs aangetroffen welke klaar was gemaakt voor verzending naar diverse buitenlandse bestemmingen. De verdovende middelen werden door politie inbeslaggenomen en er werd tevens een onderzoek ingesteld naar het bezit van en de handel en export in drugs.
Tijdens het onderzoek bleek deze verdachte ook betrokken te zijn bij internetoplichtingen. Bij het Landelijk Meldpunt Internet Oplichting (LMIO) werden diverse aangiftes gedaan waarbij hij betrokken lijkt te zijn.

Een andere vorm van cybercrime waarmee de cyberteams te maken hebben, is het hacken van accounts van bedrijven (webshops) door criminelen. Zij versturen vervolgens vanuit deze accounts berichten naar klanten van de webshops waarin bijvoorbeeld staat dat het rekeningnummer is gewijzigd. Nietsvermoedende klanten betalen hun facturen en maken ongemerkt geld over naar de bankrekening van criminelen, die vaak vanuit het buitenland opereren.
Een variant hierop is "Misbruik voor bestelling": in dit geval wordt de e-mail en/of account van consumenten gehackt om van hieruit te komen bij gerenommeerde webshops (bijvoorbeeld van Bol.com en Wehkamp), om vervolgens goederen te bestellen en deze te laten afleveren op een ander adres dan dat van de gehackte slachtoffers.
Het betreffende cyberteam geeft aan dat bij een specifieke zaak een (snelle) aanpak noodzakelijk was: er was sprake van "een verdachte, 2 misbruikte webshops, 23.000 mogelijke slachtoffers en 400 aangiften. Het stoppen van de verdachte was een belangrijke interventie".

CEO-fraude

Een andere vorm van oplichting met digitale middelen is de 'CEO-fraude'. Deze vorm van fraude is er in verschillende varianten. Vaak ontvangt een medewerker op de financiële administratie van een bedrijf een e-mail van de allerhoogste baas, de CEO of CFO. Deze draagt hem of haar op een fors bedrag over te maken naar een buitenlandse rekening. Ter verificatie van gegevens kan hij een advocatenkantoor bellen. Dit 'advocatenkantoor' zit in het complot.
De criminelen hebben voorafgaand aan hun acties de e-mailadressen van de CEO en van de functionaris op de financiële administratie achterhaald. Meestal werkt de administrateur bij een dochteronderneming of een buitenlands filiaal van een multinational. De bestuursvoorzitter kent hij niet persoonlijk. De afstand tussen beiden is zo groot, dat hij niet durft na te gaan of het wel klopt. Of de persoon die hem benadert zet hem zo onder druk dat er geen tijd voor is. Uit de interviews komt naar voren dat de oplichters in deze situatie een groot 'manipulatief vermogen' hebben om de transactie te laten uitvoeren door de betreffende bedrijfsmedewerker; "er wordt gebruik gemaakt van 'social engineering' om de boodschap zo natuurlijk mogelijk te laten overkomen en te laten aansluiten bij wat gebruikelijk is in het bedrijf".

In een andere variant doen oplichters zich voor als de IT-leverancier met de boodschap dat een geldoverboeking getest moet worden. In werkelijkheid gaat het om een echte overboeking. Ook komt het voor dat brieven worden verstuurd over een nieuwe bankrekening waar betalingen in de toekomst naartoe moeten, hetgeen uiteraard de bankrekening van de oplichter is.
Meldingen van deze vorm van fraude kunnen, naast de politie, ook worden gedaan bij de Fraudehelpdesk die deze (toenemende) vorm van fraude ook registreert.
Bij een van de politie-eenheden (i.c. het 'cyberteam' van Oost Nederland) geeft men aan een preventieve aanpak van de CEO-fraude noodzakelijk is, maar ook veel inzet vraagt: "een belronde door de politie naar de CEO's van 120 bedrijven in de regio heeft voorkomen dat zij slachtoffer werden van deze vorm van oplichting".

Oprollen van netwerk van gekloonde modems

Een aanvullend voorbeeld van een aanpak van cybercrime door een van de onderzochte eenheden (cyberteam Rotterdam) betreft een onderzoek naar de inzet van een kleine groep criminelen die circa 500 gekloonde modems wilden gebruiken bij het opzetten van een 'ondergronds' netwerk. Via het Nationaal Cyber Security Centrum werd informatie uit Canada doorgegeven aan de provider in Rotterdam en het cyberteam. Tijdens het onderzoek, dat het cyberteam Rotterdam in overleg met het THTC heeft uitgevoerd, kwam een 36-jarige Rotterdammer in beeld die, onder andere door gemodificeerde software, modems zo aan kon passen dat zij, uiteraard zonder abonnement, signalen van een grote provider (Ziggo) konden doorgeven. Er kwamen ook twee andere verdachten in het vizier die de modems leverden en konden installeren. Deze twee verdachten waren als (onderaannemer) in dienst bij de provider. Deze drie mensen zijn aangehouden en worden onder andere verdacht van computervredebreuk/hacking, het voorhanden hebben van zogenoemde malware, deelname aan een criminele organisatie, oplichting van een telecommunicatiedienst en witwassen. Bij huiszoekingen zijn circa 500 modems en computerapparatuur in beslag genomen. De verdachten, naast de 36-jarige, Rotterdammers van 30 en 42 jaar oud, kregen hun klanten via mond-tot-mondreclame. De afnemers betaalden enige honderden euro's voor het modem en bijvoorbeeld de aansluiting op internet-televisie. De verdachten leverden zelfs nog enige service als het modem niet meteen werkte. De politie kon de verdachten aanhouden nadat een bestelling in scene was gezet. Op het moment dat het bestelde en gekloonde modem zou worden aangesloten, werden de verdachten aangehouden.

3.7 Tactische inzet in cyberteams en opsporing van cybercrime

De opsporingsfunctie binnen de politie is op drie niveaus ingericht (bij de basisteams, districtsteams en regionale teams) en daarbij wordt het 'speelveldmodel' gehanteerd. Dit betekent in de praktijk dat de benodigde specialismen aan de verschillende onderzoeken worden toegevoegd. De toewijzing van zaken aan de rechercheniveaus gebeurt met behulp van een toewijzingskader dat is gebaseerd op een afweging tussen de criminaliteitssoorten en aanpakwijze.
Cybercrime is tot januari 2016 eveneens via het speelveldmodel aan de rechercheniveaus toegewezen, maar sinds 2016 wordt cybercrime tevens thematisch aangepakt door een cybercrimeteam. Uit een pilotonderzoek komt naar voren dat (traditioneel) opsporingsonderzoek en opsporingsonderzoek voor cybercrime op dezelfde wijze zijn opgebouwd, van instigatie van het onderzoek tot en met het insturen van het dossier aan het Openbaar Ministerie (Valkengoed, 2017). Opsporingsonderzoek gericht op cybercrime behoeft vanuit dit oogpunt dezelfde aanpak, maar is meer gestoeld op het digitale vlak. Tactische rechercheurs dienen zodoende ook vergelijkbare competenties te bezitten.

Voor de samenstelling van de cybercrimeteams is men bij de start van de teams uitgegaan van een minimale bijdrage van 10 fte uit de tactische recherchecapaciteit. Daarnaast is capaciteit vrijgemaakt vanuit verschillende afdelingen en teams; zo zijn leden van de cyberteams afkomstig uit de Dienst Regionale Recherche, de districtsrecherche, de basisteams recherche, maar

ook uit het Team Digitale Opsporing (TDO) en de DRIO. De ruimte die de teams hebben in de organisatorische aanpak komt ook naar voren in de invulling van functies en ook waar de capaciteit vanuit de eenheid vandaan komt. Zo kan een cyberteam ook blauwe collega's betrekken om de overdracht van kennis en kunde naar de basisteams beter mogelijk te maken, hetgeen een stimulans kan zijn voor de bestrijding van Veel Voorkomende Cyber Crime (waaronder hacken, phishing en e-fraude).

Voor de cyberteams in de onderzochte eenheden geldt dat er een grote behoefte was en nog is om de specialistische digitale kennis binnen de generieke opsporing te versterken. Een aantal teamleiders en teamchefs spreekt hierbij van 'diepte-specialisten', bijvoorbeeld bij de bestrijding van Ddos-aanvallen. De gewenste digitale kennis is globaal te onderscheiden naar: basiskennis van websitebeheer en -zoekgedrag; kennis van gedigitaliseerde criminaliteit (waaronder internetoplichting); 'diepte-kennis' van bijvoorbeeld gebruik van IP-adressen, servers, e.d. De dieptekennis op digitaal vlak is met name voorhanden bij de LE (THTC) en bij de teams digitale opsporing. De teams digitale opsporing binnen de regionale eenheden kunnen daarbij ondersteunend zijn aan de cyberteams en aan de reguliere opsporingsteams.
Bij de onderzochte eenheden is de opbouw van de cyberteams met de gewenste tactische en technische kennis een belangrijk aandachtspunt. Bij de tactische recherchedeskundigheid gaat het om vorderingen opstellen, aanvragen, ('uitlezen') en opbouw van inhoudelijke deskundigheid voor de opsporing. Bij de leden die vanuit het 'blauw' in het cyberteam instromen is dit een extra aandachtspunt[36].

Inzet en organisatie cyberaanpak; in de breedte of in de diepte?

In de organisatorische structuur van de 'cyberteams' heeft de eenheid Oost Nederland (evenals Den Haag) ervoor gekozen om de aanpak van cybercrime 'gewoon te maken' binnen het reguliere proces en om op deze wijze, uiteindelijk, ook meer capaciteit vrij te kunnen maken voor deze vorm van criminaliteit door een spreiding van de aanpak over meerdere teams in de eenheid. In de visie van de eenheid Oost Nederland dient de cyberkennis aldus niet voorbehouden te blijven aan 'één cyberteam', maar gespreid te worden over de 'blauwe' (recherche)teams, de rechercheteams van de districten en de regionale recherche.
Daar tegenover staat de keuze van de vorming van een centraal georganiseerd cyberteam (zoals de acht cyberteams) waarbij in eerste instantie een snelle besluitvorming en de opbouw van specialismen centraal staan. Beide structuren kunnen in theorie voordelen bieden, voor enerzijds een bredere en snellere spreiding van kennis van de aanpak van cybercrime binnen de politieorganisatie, i.c. de basisteams recherche, en anderzijds een opbouw van digitale expertise die het (beter/meer) mogelijk maakt om fenomeen-onderzoek te doen, met explicieter aandacht voor de modus operandi van daders en meer mogelijkheden om samen te werken met andere (gespecialiseerde) cyberteams.

[36] Zo is de kennis over het veiligstellen van digitale sporen bij het plaats delict een van de gewenste aandachtpunten (waarvoor ook de handreiking voor 'het betreden van een plaats delict in een gedigitaliseerde omgeving' is opgesteld).

In Oost Nederland heeft men bij de districtsrecherches in totaal 15 fte beschikbaar met digitale expertise. Deze expertise is verdeeld over de vier locaties van waaruit men in deze eenheid opereert. Binnen deze locaties is circa 4 fte gericht op de aanpak van cybercrime; zo is er een operationeel specialist-digitaal, 3 tactische rechercheurs en een specialist die zich specifiek richt op telefoon- en (digitale) sporenonderzoek. In de eenheid is sprake van vijf Operationeel Coördinatie Knooppunten (OCP), maar alleen bij één van deze OCP's is tactisch-digitale expertise voorhanden; binnen de andere districten is deze kennis niet bij de OCP's beschikbaar.
In de aanpak van een 'grotere cyberzaak' kan het voorkomen dat sprake is van een 'wolk van delicten' maar het komt voor dat in de eenheid Oost Nederland te weinig capaciteit voorhanden is om hierop "door te kunnen rechercheren". Het ontbreken van een gespecialiseerd cyberteam biedt in dit kader weinig mogelijkheden om de "grotere cyberzaken" op te pakken. Het zou dan dienen te gaan om een gecombineerde inzet van zowel tactisch rechercheurs als van digitaal specialisten.

Binnen de politie-eenheden wordt mede op basis van het toewijzingskader beoordeeld of de cyberzaak vervolgens naar gelang de capaciteit en deskundigheid naar de districtsrecherche of een basisteamrecherche wordt toebedeeld. Indien er cyberzaken zijn die een expliciete digitale en tactische deskundigheid behoeven neemt een cyberteam het voortouw en behoudt veelal ook de opsporing van de zaak. In de onderzochte eenheden geldt dat met name voor het cyberteam in Noord-Holland en in Rotterdam; in de eenheid Oost Nederland worden deze zaken eerder toebedeeld aan de districtsrecherche of een basisteam. Bij de eenheid in Oost Nederland betekent dit dat na weging van zaken in de stuurploeg dat "zwaardere cyberzaken vaker weg kunnen vallen" vanwege het ontbreken van de formatieve en inhoudelijke capaciteit.

Deskundigheid opsporing cybercrime bij politie

In het licht van de vraag naar de gewenste deskundigheid van de politie bij de aanpak van cybercrime, is in voorgaande jaren ook de vraag gesteld of gedigitaliseerde criminaliteit wel zo complex is, dat het specialistische aandacht behoeft. Deze discussie draaide in de kern om de gedachte van digitale experts dat gedigitaliseerde criminaliteit als normaal beschouwd moet worden in de huidige tijdsgeest en dat elke rechercheur binnen de opsporing over 'basisvaardigheden' dient te beschikken op het gebied van gedigitaliseerde criminaliteit (Struiksma, De Vey Mestdagh, & Winter, 2012; Bout, 2017). Deze vraag vormde mede de achtergrond voor de discussie over het feit of gedigitaliseerde criminaliteit wel het label 'cybercrime' moest dragen (Domenie, Leukfeldt, Wilsem, Jansen, & Stol, 2013).

In een onderzoek naar de beschikbare kennis en competenties bij de recherche van de politie in het geval van cybercrime, is door van Valkengoed in 2016 een voorstudie gedaan naar de kennis van tactisch rechercheurs bij de politie-eenheid Amsterdam inzake opsporing van cybercrime. Uit dit eerste inventariserende onderzoek bleek onder meer dat de competenties van tactisch rechercheurs onvoldoende toereikend zijn om cybercrime effectief op te kunnen sporen. Tactisch rechercheurs hebben wel de juiste attitude, maar missen de noodzakelijke

kennis en vaardigheden om te voldoen aan het vereiste basisniveau. Dit is volgens deze voorstudie op alle rechercheniveaus het geval. De basisteamrecherche scoort significant lager dan de regionale recherche en de score van de districtsteams ligt iets tussen de basisteams en de regionale recherche in. In de studie wordt geconstateerd dat de competentie van tactisch rechercheurs in de betreffende politie-eenheid op basisteamniveau het laagste is, op districtsniveau iets hoger en op regionaal niveau het hoogste is. Gezien het noodzakelijke competentieniveau voor de aanpak van cybercrime scoren de tactisch rechercheurs op alle rechercheniveaus te laag. Tevens is het opvallend is dat vaardigheden voor de opsporing van cybercrime in essentie weinig verschillen van opsporingsvaardigheden die nodig zijn voor andersoortige, 'traditionele' zaken. Desalniettemin zijn rechercheurs handelingsverlegen als het gaat om cybercrime. De resultaten van de studie suggereren dat het gebrek aan kennis daar debet aan is; bijna tweederde van de rechercheurs zou een onvoldoende halen op een kennistoets over cybercrime. Van Valkengoed concludeert in zijn voorstudie (2016) dat cybercrime hierdoor -op dat moment- niet effectief kan worden opgespoord door de tactisch rechercheurs van de onderzochte politie-eenheid.

3.8 Opsporing van cybercrime en doelen Veiligheidsagenda

Een van de doelstellingen in de bestrijding van cybercrime door de politie, zoals opgenomen in de Veiligheidsagenda 2015-2018, is de intensivering van de strafrechtelijke aanpak van cybercrime door het aanpakken van meer zaken. Hiertoe zijn afspraken met de politie en het OM gemaakt, waarbij jaarlijks een (toenemend) aantal cyberzaken op landelijk en eenheidsniveau zijn vastgesteld (zie ook tabel 1).
De intensivering van de aanpak van cybercrime zou hiermee aldus tot een gekwantificeerde toename in het aantal zaken en verdachten dienen te leiden. Bij de beoordeling van de cyberzaken die meetellen in de registratie van het OM hanteert het OM tien wetsartikelen die op 'computercriminaliteit' betrekking hebben (zie bijlage 2). Deze wetsartikelen richten zich op de aanpak van delicten die als 'cybercrime' (in enge zin) zijn omschreven (delicten die in principe ICT zowel als middel als doel hebben).

Realisatie kwantitatieve doelen cybercrime Veiligheidsagenda [37]

Het totaal aantal reguliere cybercrimezaken dat door de Nationale Politie bij het Openbaar Ministerie is aangeleverd, vertoont in de afgelopen jaren een stijgende lijn: van 137 in 2015 naar 184 in 2016 (volgens opgave van het Openbaar Ministerie). Daarmee bleef het aantal aangeleverde zaken van cybercrime in 2015 en 2016 onder de afgesproken norm vanuit de Veiligheidsagenda. In 2017 is het aantal door de politie aan het OM aangeleverde zaken van cybercrime

[37] De politie registreert bij de reguliere cyberzaken het aantal naar het OM ingezonden verdachten in BOSZ en dit wordt door het OM gevalideerd door deze in BOSZ (OM-module BOSZ) te beoordelen. Het OM registreert het aantal ingestroomde verdachten in GPS/Compas. De politie telt het aantal naar het OM ingezonden verdachten. Hierbij worden de onder instroom OM en instroom OM overig in BOSZ geregistreerde verdachten met MK F90 geteld. Voor een specificatie van de onder Cybercrime vallende wetsartikelen, zie bijlage 2. Het OM telt de instroom aan de hand van het aantal verdachten (parketnummers met wetsartikelen bijlage 2) vanuit GPS/Compas.

echter gestegen (naar 231 zaken), gevolgd door een sterke stijging in 2018 naar 311 cyberzaken. De politie heeft daarmee de kwantitatieve doelen binnen de aanpak van cybercrime voor 2017 en 2018 (net) behaald. Volgens de opgave van de politie is ook een groter aantal dossiers van verdachten van cybercrime naar het OM ingezonden dan in voorgaande jaren (400 verdachten in 2018).

Tabel 4 *Doelstelling aanpak politie reguliere cyberzaken en vervolging cybercrime, politiecijfers[38] en OM-cijfers 2015-2018*

jaar	doelstelling aantal reguliere cyberzaken	opgehelderde zaken politie	door politie naar OM ingezonden verdachten	instroom cybercrime Openbaar Ministerie
2015	175	165	195	137
2016	190	160	210	184
2017	230	105	220	231
2018	310	240	400	311

Kwantitatieve doelen bij onderzochte politie-eenheden

De intensivering van de aanpak van cybercrime voor de Nationale Politie als geheel betekent ook voor de drie onderzochte eenheden dat zij meer zaken dienen aan te leveren aan het Openbaar Ministerie. Voordat we deze doelen bespreken, geven we eerst een beeld van de ontwikkeling van de aangiften van cybercrime bij de drie politie-eenheden in de afgelopen jaren en van het aantal verdachten die de politie registreert.

De politie-eenheden registreren over het algemeen een stijging van het aantal aangiften van cybercrime in de periode 2015-2018, maar er zijn ook opmerkelijke fluctuaties te zien, ook in de relatie tussen het aantal meldingen van cybercrime en de aangiften daarvan in 2018 (zie tabel 5). De opmerkelijke verschillen tussen aangiften en meldingen en de ontwikkelingen in de jaren kunnen mogelijk verklaard worden door een feitelijke toename van de cybercrime (en mogelijk toename van de aangiftebereidheid), maar evenzogoed ook door afwijkende en wisselende interpretaties van wat 'cybercrime' is in de politieregistraties.

[38] Bron: CBS.

Tabel 5 *Geregistreerde aangiften (en incidenten) computercriminaliteit en verdachten drie onderzochte politie-eenheden (politiecijfers)*

aangiften en OM-zaken	Noord-Holland		Rotterdam		Oost Nederland	
	aangif-ten	verdachten aan OM	aangiften	verdachten aan OM	aangiften	verdachten aan OM
2015	220	10	210	19	385	8
2016	290	17	150	33	215	13
2017	470	17	225	30	270	34
2018	538	22	298	42	140	50
2018 incidenten	629		801		1776	

Doelen en realisatie cybercrime onderzochte politie-eenheden

In de strafrechtelijke aanpak van cybercrime is voor de politie-eenheid Noord-Holland in 2017 een opdracht gesteld om 17 reguliere cybercrimezaken aan te dragen (zie tabel 6). Uit overzichten van de politie komt naar voren dat men deze norm ruimschoots heeft gehaald met het aanleveren van 28 zaken aan het Openbaar Ministerie; uit overzichten van het Parket-Generaal komt echter naar voren dat men deze norm in 2017 net niet heeft gehaald met het aanleveren van 15 zaken. De doelstelling voor 2018 is gesteld op 23 cyberzaken en er zijn er door de politie 22 feitelijk ingestuurd naar het OM; in 2018 is de norm nagenoeg gehaald.

Voor de politie-eenheid Rotterdam is het doel in 2017 gesteld op het aanleveren van 30 reguliere cybercrimezaken bij het OM. Deze norm heeft men volgens politiecijfers in 2017 gehaald met het aanleveren van 32 zaken; uit cijfers van het PaG komt naar voren dat in 2017 24 zaken zijn aangeleverd. De norm voor 2018 is voor het cyberteam in Rotterdam gesteld op het aanleveren van 40 reguliere zaken. De politie-eenheid Rotterdam heeft volgens politiecijfers deze norm gehaald met het aanleveren van 42 zaken; uit cijfers van het PaG komt naar voren dat in 2018 26 zaken zijn aangeleverd en daarmee is de norm niet gehaald.

De politie-eenheid Oost Nederland heeft in 2017 26 zaken bij het OM betreffende cybercrime ingediend; de gestelde norm van 34 zaken heeft men niet gehaald in dat jaar. In 2018 is de norm voor het aantal ingediende cybercrimezaken verhoogd naar 46 reguliere zaken; uit PaG-cijfers blijkt dat de eenheid niet aan de norm heeft voldaan (met 36 zaken).

Het overzicht met de gestelde doelen en aangeleverde verdachten van cybercrime door de politie bij het Openbaar Ministerie wijst uit dat de politie de gestelde doelen kan halen indien men uitgaat van de door hen aangehouden verdachten; indien men uitgaat van de cijfers van het Openbaar Ministerie voor vervolging blijkt dat de doelen soms lastiger te bereiken zijn omdat het OM de mogelijkheden voor vervolging van deze verdachten veelal lager inschat en cyberzaken seponeert. Uit de tabel komt naar voren dat zich hierin tot veel fluctuaties voordoen:

Tabel 6 *Doelstelling politie aanpak reguliere cyberzaken en vervolging cybercrime, politiecijfers[39] en OM-cijfers bij drie onderzochte politie-eenheden, 2016-2018*

jaar	doelstelling aantal reguliere cyberzaken	opgehelderde zaken politie	door politie naar OM ingezonden verdachten	instroom cyberzaken OM
2016 (tot)	**190**	**160**	**210**	**184**
Noord-Holland	14	25	35	17
Rotterdam	25	10	10	33
Oost Nederland	28	20	25	13
2017 (totaal)	**230**	**105**	**220**	**231**
Noord-Holland	17	20	25	15
Rotterdam	30	15	30	24
Oost Nederland	34	20	25	41
2018 (totaal)	**310**	**240**	**400**	**311**
Noord-Holland	23	15	25	22
Rotterdam	40	100	130	26
Oost Nederland	46	20	45	36

Complexiteit van en richting in de opsporing van cybercrime

De opsporing en het vervolgen van daders van cybercrime blijkt in de praktijk een complexe aangelegenheid te zijn waarbij de kans op succes gering is: de mogelijkheden voor criminelen om in grote mate anoniem via het internet te opereren zijn groot en het deels internationale karakter van cybercrime (bijvoorbeeld via het darkweb of via de Microsoft scam) zorgt ervoor dat de pakkans van cybercrime klein is. De politie wordt daarbij in een deel van de cybercrimezaken geconfronteerd met een of meerdere vanuit het buitenland opererende criminelen.
Het beeld over het internationale karakter van cybercrime is echter niet eenduidig als slachtofferschapenquêtes in beschouwing worden genomen. Zo kwam uit onderzoek van Veenstra et

[39] Bron: CBS.

al. (2015) naar voren dat bedrijven weliswaar ook slachtoffer worden van internationaal opererende verdachten, maar het overgrote deel van de e-fraudes en hackzaken (80%) zou vanuit Nederland worden gepleegd. Maatregelen voor cybercrimebestrijding, zoals bijvoorbeeld het bijeen brengen van aangiften, zouden volgens dit onderzoek dan ook om te beginnen nationaal georiënteerd dienen te zijn.
Het ophelderingspercentage van 8% van cybercrime-aangiften bij de politie geeft aan dat er veelal geen succesvolle opsporing (op de veel voorkomende cybercrime) plaats vindt. Bij de initiatieven om de mogelijkheden voor de opsporing van cybercrime te vergroten, zoekt men ook de juridische grenzen op aangezien de digitale mogelijkheden van daders ook groot zijn om hun sporen te maskeren.
Zo hebben het cyberteam Noord-Holland en het Openbaar Ministerie in Haarlem begin 2019 een rechtszaak aangespannen in het kader van de aanhouding van een verdachte van bankpasfraude en de ontgrendeling van een smartphone om voor de politie relevante gegevens te verkrijgen. Deze 'cyber007-zaak' draait om een phishingbende die bankpassen en pincodes stal en daarmee duizenden euro's buitmaakte. In februari 2016 besloot het Alkmaarse cybercrimeteam bij wijze van test de iPhone 6 van een van de verdachten op 'simpele' wijze te kraken. De verdachte werd geboeid en een rechercheur drukte de duim van de verdachte op de 'identity sensor' van de smartphone. Deze smartphone op een andere wijze ontgrendelen, was op dat moment nog geen optie en de verdachte wilde niet meewerken. De rechtbank oordeelde dat het drukken van de duim op de identity sensor 'slechts een beperkte inbreuk op de lichamelijke integriteit' omvat. Daarnaast stellen de rechters dat een in beslag genomen telefoon onderzocht mag worden en dat de politie materiaal dat onafhankelijk van de wil bestaat, zoals een vingerafdruk, onder dwang mag afnemen. De juridische mogelijkheden binnen de opsporing van cybercrime zijn daarmee verruimd[40].

Ofschoon het behalen van de kwantitatieve doelstellingen, c.q. het aantal cybercrimezaken, als KPI is geformuleerd om de intensivering van de aanpak van cybercrime te stimuleren, geeft deze normering volgens de cyberteams onvoldoende weer welke inzet men vanuit de politie kan en dient te plegen voor het opsporen van cybercrimeverdachten.
In de praktijk blijkt dat de cyberincidenten die de politie registreert voornamelijk 'brengzaken' zijn en dat derhalve alleen een beeld bestaat en ook actie wordt ondernomen op de binnengekomen aangiften. Voor een proactieve aanpak in de vorm van 'haalzaken' is veelal minder formatiecapaciteit voorhanden, of wordt daar niet voor vrijgemaakt. Aandacht voor 'haalzaken' bij cybercrime is van belang mede omdat bij veel vormen van cybercrime slachtoffers vaak niet eens weten slachtoffer te zijn; een server kan bijvoorbeeld misbruikt worden voor allerlei doeleinden zonder dat de eigenaar ervan op de hoogte is. Pas tijdens een lopend onderzoek komt de politie hier achter en gaat eventueel slachtoffers waarschuwen[41]. Om cybercrime aan te pakken betekent dit voor de politie dat zij meer aandacht moet geven aan 'haalzaken'.

[40] https://www.volkskrant.nl/nieuws-achtergrond/de-politie-dwong-bryan-o-om-zijn-smartphone-te-ontgrendelen-mag-dat-wel-~ba84be51/
https://www.volkskrant.nl/nieuws-achtergrond/politie-mag-verdachte-dwingen-zijn-smartphone-te-ontgrendelen~b5fe6c66/
[41] Politie, Eenheid Oost-Nederland (2019). Veranderingen in criminaliteit. Een verkenning van de oorzaken in Oost-Nederland.

De norm geeft de cyberteams vooral weinig ruimte om inzet te plegen voor de aanpak van 'fenomenen' binnen de cybercrime die relatief veel tijd en capaciteit vergen. Zo richt men zich ook op zaken waarbij men door de complexiteit en tijdsbeslag van de zaak ook een periode van maanden bezig kan zijn; dit betekent ook dat het aantal opgeloste zaken mede daardoor wordt bepaald.
In de visie van de cyberteams -en ook van het OM- vraagt dit om een andere benadering van de effectiviteit van de inzet van cyberteams waarbij tevens de inhoudelijke aanpak en aard van de zaak wordt meegewogen. De verwachte inzet van de cyberteams op het aantal aan te leveren verdachten van cybercrime leidt bij de betrokkenen van de politie tot veel discussie over de te behalen kwantitatieve en kwalitatieve doelstellingen. De politie is in de afgelopen jaren 'afgerekend' op het aantal aangeleverde cyberzaken, terwijl er een verder liggend doel is van een 'digitaal weerbare samenleving'. De KPI-cijfers zijn bovendien geen garantie dat cybercrime effectiever wordt aangepakt; een projectleider stelt dat "iedereen die betrokken is bij het vaststellen van onze landelijke cijfers weet dat deze boterzacht zijn, misschien zijn juist kwalitatieve verhalen spijkerhard".

3.9 Vervolging en sanctionering van cybercrime

In de praktijk blijkt dat veel van de door de politie aangedragen cyberzaken bij het Openbaar Ministerie worden afgedaan zonder dat deze een parketnummer krijgen. Bij een beoordeling van de zaken in BOSZ wordt door het Openbaar Ministerie namelijk relatief vaak besloten tot een sepot[42]. Bij het besluit tot seponeren van cyberzaken is relatief vaak sprake van een technisch sepot waarbij men uitgaat van een (bij voorbaat) kansloze vervolging (bijvoorbeeld omdat de dader zich vaak in het buitenland ophoudt en niet kan worden aangehouden).
Op dit moment zijn daarmee bij het OM alleen de aantallen verdachten van cyberzaken herkenbaar die ook feitelijk een parketnummer hebben gekregen. Dit betekent bij een beoordeling van de ingediende zaken van cybercrime afwijkingen kunnen worden geconstateerd tussen de cijfers van de politie en van het Openbaar Ministerie.

Bij de vervolging en sanctionering van verdachten van computervredebreuk komt het voor dat het Openbaar Ministerie zonder tussenkomst van de rechter een strafbeschikking uitdeelt of een transactie aanbiedt. Dit zijn veelal transacties die in het geval van computervredebreuk vaak bestaan uit een werkstraf of een geldboete. Uit CBS-data komt naar voren dat in de periode 2009 - 2016 het totale aantal opgelegde straffen voor computervredebreuk 285 bedroeg. In deze periode was het aandeel van door het Openbaar Ministerie aangeboden transacties en opgelegde strafbeschikkingen 54 procent (CBS, 2018).

[42] Het Openbaar Ministerie geeft aan dat deze werkwijze zal veranderen (in 2019) en dat alle zaken zullen worden geregistreerd in de OM-systemen.

Uit verzamelde cijfers van het Openbaar Ministerie over 2018 komt naar voren dat van de totale instroom van cyberzaken (in totaal 311 zaken), 156 zaken (50,2%) zijn geseponeerd en in 20 gevallen is een OM-transactie aangeboden. Het aandeel OM-afdoeningen is 60%, het aandeel ZM-afdoeningen 40%. In 103 gevallen is sprake van een schuldigverklaring, dat is 34% van de uitstroom bij het OM in eerste aanleg (zie verder bijlage 3).
Naast de rol van het Openbaar Ministerie in de opsporing en vervolging van cybercrime, wordt door hen ook geparticipeerd in verschillende publiek-private initiatieven op het gebied van cyber security en de aanpak van cybercrime. Zo neemt het Openbaar Ministerie deel aan de Cyber Security Raad (CSR), het Nationaal Cyber Security Centrum (NCSC) en de Electronic Crimes Task Force (ECTF). Binnen de verschillende samenwerkingsverbanden worden ook de voor cybercrime onderliggende (legale) structuren in kaart gebracht, waarbij ook wordt gekeken in welke fases van het cybercrimeproces barrières kunnen worden opgezet (zoals het moeilijker maken voor cybercriminelen om voor hun criminele activiteiten diensten af te nemen bij Nederlandse hostingpartijen).

Uit de relatie tussen het Openbaar Ministerie en de politie bij de aanpak van cybercrime komt naar voren dat men in de afgelopen jaren naar nieuwe vormen van afstemming en samenwerking heeft gezocht. De relatieve onbekendheid die beide partijen in eerste instantie hadden met het fenomeen ‘cybercrime’ heeft ook tot een onderlinge ‘zoektocht’ geleid om tot meer adequate gezamenlijke afspraken te komen.
Zo zijn in Rotterdam in eerste instantie in de samenwerking met OM en politie “relatief veel zaken gedraaid” op basis van het ‘arenamodel’. Aangezien het OM echter vervolgens zaken moest gaan bepleiten bij de stuurploeg van de politie is via de verschillende rechercheteams veel kennis verloren gegaan. De aanpak via verschillende lagen binnen de politieorganisatie bleek in de visie van het OM uiteindelijk niet efficiënt te zijn. Door de opzet van een centraal georganiseerd cyberteam acht men de aanpak en samenwerking met het OM sterk verbeterd. De concentratie van aandacht voor cyberzaken in een cyberteam zorgt er in principe voor dat de ‘vluchtigheid’ in de aanpak is verminderd.
Bij het Openbaar Ministerie in Oost Nederland komt naar voren dat men niet alleen bij de eigen organisatie veel aandacht moet vragen voor een verbetering van de cyberdeskundigheid van de officieren van justitie, maar ook voor de deskundigheid van de politie bij cybercrime, bijvoorbeeld voor het opstellen van een “goed technisch proces verbaal”. Het OM ziet daarin dat duidelijke verbeteringen nodig zijn om zaken ‘digiproof’ te maken en specialisme op te bouwen.

In de visie van officieren bij het OM in de drie politie-eenheden is het bestrijden van ‘cybercrime in enge zin’ een te beperkte invalshoek voor de aanpak, maar dient in de focus meer aandacht te zijn voor gedigitaliseerde criminaliteit, of, zoals een officier van justitie het verwoordt “liever nog criminaliteit en digitaliteit”. In deze benadering dient de politie meer te kijken naar de dwarsverbanden van typen criminaliteit en de zwaardere delicten die door toepassing van digitale middelen mogelijk zijn geworden. Voorbeelden hiervan zijn het gebruik van PGP-telefoons door criminelen die daardoor hun crimineel gedrag digitaal konden verbergen en het gebruik van gehackte creditcardgegevens voor drugshandel binnen het ‘darkweb’. De

focus die nu wordt gelegd op cybercrime in enge zin geeft aldus een beperkt beeld van de toepassing van digitale mogelijkheden door criminelen en geeft de politie ook beperkt zicht op cybercrime in brede zin. Een van de OvJ's stelt in dit verband: "de ontwikkeling van cybercrimes gaat op dit moment zo ontzettend rap en de modus operandi bij deze delicten veranderen dagelijks, daar moet de politie ook op kunnen anticiperen".
Het streven naar een intensivering van de aanpak van cybercrime door middel van de KPI die tot meer cyberzaken moet leiden, betekent deels ook dat een keuze wordt gemaakt voor relatief 'simpele zaken' die als 'veelvoorkomende cybercriminaliteit' wordt omschreven, waardoor minder tijd en capaciteit beschikbaar is voor fenomeen-onderzoek dat een groter lerend effect kan opleveren voor de cyberteams. Ook vanuit het Openbaar Ministerie wordt aangegeven dat "meer ambitie is ontstaan om meer werk te maken van fenomeengericht onderzoek". Bovendien speelt mede de overweging bij het Openbaar Ministerie om de strafrechtelijke handhaving 'spaarzaam in te zetten' ("is kostbaar en selectief in te zetten bij vervolging van cyberzaken"). Voor de politie en andere betrokkenen bij de aanpak van cybercrime betekenen deze overwegingen dat ook (meer) aandacht gegeven dient te worden aan 'preventie' en 'verstoring' (waaronder 'notice and take down'[43]).

Strafmaat voor cybercrime

In samenloop met de intensivering van de aanpak van cybercrime is bij het Openbaar Ministerie ook meer het besef ontstaan dat cybercrime 'serieuze criminaliteit' kan zijn en derhalve als ernstige delicten dienen te worden beschouwd indien het gekoppeld wordt aan een criminele organisatie. In de visie van het Openbaar Ministerie is de strafmaat voor cybercrime in voorgaande jaren 'aan de lage kant' geweest.
Mede in dit kader zijn sinds februari 2018 nieuwe richtlijnen ingesteld voor officieren van justitie[44]. Deze moeten het makkelijker maken om een straf te bepalen voor vergrijpen als diefstal via internetbankieren. Ook is onder meer de strafmaat voor zaken als inbreken in een computeraccount met het wachtwoord van een ex-geliefde, of diefstal van gegevens van bedrijven, bijvoorbeeld door een ex-werknemer, duidelijker.

Dadergroepen cybercrime

In de aanpak van cybercrime heeft onder meer de politie te maken met verschillende typen dadergroepen. In CSBN 2019 wordt aangegeven dat de grootste dreiging uitgaat van beroepscriminelen en statelijke actoren. Beroepscriminelen richten zich in toenemende mate op grote bedrijven voor financieel gewin en vormen een doelgroep voor de regionale cyberteams. Bij de aanpak van cybercrime uitgevoerd door statelijke actoren heeft met name het THTC een belangrijke rol. Daarnaast zijn er ook dreigingen door individuen die de kennis en mogelijkheden hebben om in geautomatiseerde systemen van organisaties in te breken. Zo zijn er op online-

[43] De Notice and TakeTown code richt zich op de afhandeling van meldingen ten aanzien van (vermeende) onrechtmatige en/of strafbare inhoud op internet. Daarnaast kan de code ook aangewend worden voor inhoud die door tussenpersonen als ongewenst of schadelijk wordt gezien. De code draagt eraan bij dat private partijen dit soort meldingen zoveel mogelijk zelf afhandelen. Overigens blijft voor partijen altijd de mogelijkheid open staan om naar de rechter te stappen of aangifte te doen.
[44] Richtlijn voor strafvordering cybercrime (2018R001), 1 februari 2018. Staatscourant, 2018, Nr. 3271.

marktplaatsen complete pakketten te koop waarmee men kunt hacken of een Ddos-aanval kunt uitvoeren. Cybervandalen en 'scriptkiddies' hebben daarmee ook de 'arena' betreden.

In de eerste cyberbeelden die door politie-eenheden zijn opgesteld, is relatief weinig informatie opgenomen over mogelijke dadergroepen, maar ligt het accent met name op de beschrijving van kenmerken van slachtoffers die aangifte van cybercrime hebben gedaan. In het cyberbeeld van Oost Nederland wordt wel een beschrijving van mogelijke dadergroepen gegeven, met de algemene opmerking dat daders van cybercrime veelal onbekend zijn en/of in het buitenland vertoeven. In dit cyberbeeld wordt wel aangegeven dat een aanzienlijk deel van het financieel gemotiveerde cybercrime wordt gepleegd door Nederlandse beroepscriminelen die niet alleen in het digitale domein actief zijn. Zij komen in ieder geval bij fraude met bankgegevens (phishing) en misbruik van accounts voor bestellingen in beeld. Dit lijkt, volgens het opgestelde cyberbeeld, geen kwestie van een verschuiving van offline criminaliteit naar online criminaliteit maar eerder een verbreding van het criminele takenpakket.
De rol van beroepscriminelen ligt voor een deel voor de hand, want bij veel cybercrime blijft de cash-out een probleem; op een gegeven moment moet de dader over het ontvreemde geld en goederen kunnen beschikken. Beroepscriminelen hebben onder andere toegang tot netwerken van katvangers en andere personen die bijvoorbeeld bereid zijn om gestolen goederen bij een afhaalpunt op te halen of geld te pinnen met een gestolen pas. In het aangehaalde cyberbeeld wordt naast beroepscriminelen op nog een belangwekkende groep daders gewezen die vanuit Nederland opereert. Deze daders zitten niet achter zaken in de eerder aangegeven 'Top 5' van cybercrime, maar zijn eerder verantwoordelijk voor complexe hacks, botnets en Ddos-aanvallen. Deze daders hebben overal in het land en in het buitenland contacten, ook onderling, bijvoorbeeld via Discord, Skype of Teamspeak (programma's waarmee live gesproken en gechat kan worden). Dit zijn veelal jonge, autochtone mannen rond 20 jaar met interesse in ICT die vaak, maar niet altijd, hoogopgeleid zijn.
De beroepscriminelen die ook digitale delicten plegen, zijn niet allemaal even digitaal onderlegd. Er is een levendige handel in onder andere gekraakte wachtwoorden, phishing tools en nepwebwinkels in groepen op Telegram (een chatapplicatie zoals Whatsapp). Dit is geen diepe cyber underground: in principe kan iedereen toegang krijgen tot deze groepen[45].

In de Monitor Jeugdcriminaliteit 2015 (van der Laan en Goudriaan, 2016) is voor het eerst ook uitgebreid onderzoek gedaan naar de mate waarin jongeren betrokken zijn bij onlinedelicten (cyber- en gedigitaliseerde delicten). Politie- en justitiestatistieken bieden weinig informatie over het aantal jeugdige verdachten en strafrechtelijke daders van onlinecriminaliteit. De informatie die beschikbaar is, geeft geen goed landelijk beeld van het aantal jeugdigen dat onlinedelicten pleegt. Ook in de daaropvolgende Monitor Jeugdcriminaliteit (van der Laan en Beerhuizen, 2018) wordt aangegeven dat het aantal jeugdige veroordeelden voor cyber- en gedigitaliseerde criminaliteit crime gering is en (nog steeds) niet goed in beeld in de landelijke registraties. Het aandeel jeugdigen dat veroordeeld is wegens een cyber- of gedigitaliseerd delict is minder dan 1% van alle jeugdige strafrechtelijke daders. Dit is volgens de monitor een forse

[45] Cyberbeeld politie Oost Nederland 2016-2018.

onderschatting van het aantal jeugdigen dat betrokken is bij cyber- en gedigitaliseerde criminaliteit, omdat deze typen delicten nog niet goed in beeld zijn in de politie en justitie registraties op landelijk niveau (van der Laan en Beerthuizen, 2018).
Op basis van zelfrapportage is er meer informatie over onlinedaderschap. Het percentage jongeren dat zegt onlinedelicten te plegen, is het hoogst onder de minderjarigen en het laagst onder de twaalfminners. Van de minderjarigen in 2015 zegt 31% in het voorafgaande jaar een (of meerdere) onlinedelict(en) te hebben gepleegd, bij de jongvolwassenen is dit 28% en bij de twaalfminners 10%. Minderjarigen zeggen relatief vaker betrokken te zijn bij gedigitaliseerde delicten dan jongvolwassenen (in 2015 rapporteert respectievelijk 22% en 14% betrokken te zijn geweest bij één of meerdere gedigitaliseerde delicten over het voorafgaande jaar); jongvolwassenen zijn relatief vaker betrokken bij cyberdelicten dan minderjarigen (in 2015 rapporteert respectievelijk 22% en 17% betrokkenheid bij cyberdelicten in het voorafgaande jaar).
Bij deze cyberdelicten van jongeren gaat het meestal om inloggen op een computer of netwerk zonder toestemming of om wachtwoorden van iemand anders veranderen waardoor deze niet meer kan inloggen. Van de 12 tot 18-jarigen meldde meer dan een op de vijf zich schuldig te hebben gemaakt aan een gedigitaliseerd delict. Hiertoe behoren onder andere het zich voordoen als iemand anders op internet, iemand online bedreigen of tegen iemands wil seksueel getinte foto's van die persoon rondsturen.

Aan de hand van een aanvullende analyse van onderzoek onder jongeren concluderen Rokven et al. (2017) dat een deel van de jeugdige online daders een nieuwe groep daders is. Jongeren die naar eigen zeggen alleen cyberdelicten plegen, blijken een ander profiel te hebben dan de andere groepen online en offline daders. Voor cyberdelinquenten zijn daarom mogelijk nieuwe interventies nodig om hen ervan te weerhouden om opnieuw (online) delicten te gaan plegen.

Bij de cyberteams geeft men aan dat de daders die zij aanhouden vaak al andere antecedenten hebben opgebouwd met andere delicten. Er wordt een voorbeeld genoemd van ‘jonge overvallers’ die zijn ‘omgeschoold’ naar cybercriminelen. De mogelijkheden om cybercrime te plegen zijn volgens de politie ook vaak relatief groot; met 2 jaar Mbo-opleiding (‘of lager’) en een beetje IT-kennis kunnen ze makkelijk toeslaan, mede op basis van pakketjes (van bijvoorbeeld Ddos-aanvallen) die op internet te koop zijn. De daders lopen relatief weinig risico (in vergelijking met andere vormen van criminaliteit), ze hoeven geen bedreigingen toe te passen en laten geen DNA achter. Ze laten wel (alleen) ‘digitale sporen’ achter, maar deze waren lastig te achterhalen voor de politie om tot opsporing over te gaan.
Door de vorming van een zelfstandig cyberteam zijn er meer mogelijkheden gekomen om als team zich te verdiepen in de modus operandi van onder meer de ‘hackers’. Een van de acties bij het cyberteam in Noord-Holland was hiertoe zelf een ‘hacker’ in te huren.

Aanpak jongere hackers

Uit onderzoek (van Laan et al, 2016; Rokven et al, 2017) blijkt dat ook minderjarige jongeren zich schuldig maken aan gedigitaliseerd delicten. Het gaat hier onder meer om het zich voordoen als iemand anders op internet, iemand online bedreigen of tegen iemands wil seksueel getinte foto's van die persoon rondsturen. Uit politiegegevens komt naar voren dat per jaar

circa 70 jongeren tussen de 12 en 23 jaar worden aangehouden voor cybercrime. Om jongeren die voor een eerste cybercriminaliteitsdelict worden veroordeeld alternatieve of aanvullende straftrajecten aan te bieden, is de politie eind 2017 in samenwerking met het OM en ketenpartners met het project 'Hack_Right' gestart. Deze aanpak dient recidive bij de jongeren te voorkomen en hun ICT-talent te bevorderen (binnen de daartoe gestelde kaders). De interventies worden gepleegd met en uitgevoerd door strafrechtketenpartners, cybersecuritybedrijven en de ethische hackergemeenschap. In 2018 zijn elf jongeren tussen de vijftien en twintig jaar met proeftrajecten gestart (de aanpak zal onderwerp zijn van evaluatie).

3.10 Aanpak cybercrime: inzet op meerdere sporen

Bij de bestrijding van cybercrime onderscheidt de politie een aantal taken: preventie, verstoring, schadebeperking en opsporing. In de discussies over de aanpak worden door de politie ook nieuwe termen geïntroduceerd, die variaties op een thema omvatten (waaronder de termen attributie, notificatie, e.a.).

In de alternatieven en aanvulling op opsporing gaat het vooral om:

- preventie: het betreft het versterken van bewustwording en van de digitale weerbaarheid onder het motto: 'burgers en bedrijven denk aan uw eigen digitale veiligheid'.
  Een voorbeeld van preventie die de politie bij cybercrime heeft ingezet was de campagne 'Wordt u gebeld door Microsoft? Hang op!' in juni 2017. In 2017 deden 1669 mensen aangifte van de Microsoftscam, tegenover elfhonderd in 2016. In totaal raakten de slachtoffers honderdduizenden euro's kwijt. In samenwerking met Microsoft en media legde de politie uit hoe de oplichters te werk gaan en op welke wijze men het beste kan reageren. Uit de aangiftecijfers bleek dat het aantal slachtoffers afnam in de periode direct na de campagne, maar daarna ook weer toenam. Deze constatering heeft tot een vervolg van de voorlichtingscampagne geleid begin 2018;
- verstoring van de cyberdaad en cyberdader: de cyberteams pakken dit aan door bijvoorbeeld een malafide website op zwart te zetten, een foute bankrekening te blokkeren of de naam van een fraudeur op te nemen in het Check Verkoper register;
- signalering en advisering (notificatie): dit betreft het op de hoogte stellen van burgers en bedrijven die slachtoffer geworden zijn of mogelijk gaan worden; 'slachtoffers verander uw wachtwoord';
- schadebeperking en het ondersteunen van burgers en bedrijven als ze slachtoffer geworden zijn van cybercrime; de website www.nomoreransom.org is hiervan een voorbeeld.

De resultaten van de aanpak van cybercrime door de politie leidt tot de vraag welke interventies mogelijk meer of aanvullend succes hebben bij de huidige benadering in de opsporing. De resultaten van de opsporing lijken licht te verbeteren door een toename van het aantal verdachten dat men aanhoudt, maar er is een besef dat de aanpak van cybercrime een meer structureel karakter dient te hebben waarbij 'aan de voorkant' moet worden gewerkt.

Dit kan door zich meer te richten op onderzoek en analyse van fenomenen binnen cybercrime, als ook een versterking van de digitale mogelijkheden van de politieorganisatie zelf als van burgers en bedrijven. Bij de digitale 'kracht' van de politie zelf stelt Stol (2018) dat "de eerder vermelde conclusie uit 2012 dat 'digitaal' nog geen normaal en integraal onderdeel is van de politieorganisatie in de volle breedte, geldt nog steeds. Sindsdien is wel voortgang geboekt, maar de politie moet zich sneller aanpassen aan de digitalisering van de samenleving en ze kan dus niet volstaan met het draaien van meer cybercrimezaken. Zij moet verlangen dat alle medewerkers digitale mogelijkheden benutten bij al hun zaken en andere taken."

3.11 Samenwerking politie bij aanpak cybercrime

In de plannen voor een geïntensiveerde aanpak van cybercrime door de politie (zoals omschreven in de PIAC 2016) wordt onder meer gewezen op de wens en noodzaak van samenwerking binnen de politieorganisatie en met publieke en private partners. Deze samenwerking zou met name gericht dienen te zijn op informatie-uitwisseling en het nemen van maatregelen ten behoeve van preventie en het opwerpen van barrières.

In Nederland zijn inmiddels verscheidene organisaties en instanties bezig met de bestrijding van verschillende vormen van cybercrime. In 2010 is het Landelijk Meldpunt Internet Oplichting (LMIO) gestart. Dit meldpunt richt zich specifiek op het tegengaan van oplichting in de internethandel (bijvoorbeeld op Marktplaats). Via dit meldpunt kunnen consumenten relatief eenvoudig melding doen van internetoplichting. Daarnaast hebben publieke en private organisaties de handen ineengeslagen in een samenwerking onder de naam Electronic Crimes Taskforce (ECTF), het zogenaamde 'bankenteam'. Dit samenwerkingsverband richt zich op het voorkomen en aanpakken van digitale criminaliteit in de financiële sector (zoals financiële malware en phishing- aanvallen).

Samenwerking met Landelijke Eenheid, Team High Tech Crime

In de structuur voor de aanpak van cybercrime door de politie is er een laag op (inter)nationaal niveau (waarop het THTC opereert) en een laag op eenheidsniveau. Het werk van het THTC wordt als het ware verbreed en aangevuld met een regionale aanpak. Cybercrimezaken worden op basis van het Toewijzingskader en beschikbare expertise toegewezen aan de Dienst Landelijke Recherche (DLR), Dienst Regionale Recherche (DRR), districtsrecherche of basisteams. Het THTC heeft inmiddels een sterke internationale reputatie opgebouwd door haar innovatieve aanpak met een groot bereik. Een voorbeeld daarvan is de sluiting van een grote Ddos-website in de 'Operation Power Off' in april 2018.
Het betrof de grootste cybercriminele website Webstresser.org die als een zogenaamde 'booter' of 'stresser' dienst deed: een website waar tegen lage prijzen krachtige Ddos-aanvallen konden worden aangekocht. In deze actie zijn vier beheerders van deze website in onder andere Servië en Kroatië opgespoord. In Canada en het Verenigd Koninkrijk werden ook acties ondernomen op vermoedelijke beheerders. Ook in Nederland werden huiszoekingen gedaan

en werden gebruikers van Webstresser.org aangehouden. Een tweede voorbeeld van de aanpak van de THTC is de actie in het kader van de Hansa Market, waarbij medio 2017 een van de grootste illegale marktplaatsen op internet werd overgenomen en offline gehaald. De val van Hansa Market vormde het sluitstuk van een internationaal afgestemde infiltratie operatie. De Nederlandse politie kreeg daarbij het beheer van de marktplaats in handen. Dat verschafte het THTC en het Darkwebteam van de politie zicht op grote aantallen verkopers en kopers van voornamelijk harddrugs.

In de gelaagdheid van de organisatie is ook een gezamenlijke afspraak gemaakt voor uitwisseling van kennis tussen het THTC en de cyberteams van de regionale eenheden. Zo is een 'adoptie' van eenheden door het THTC voorgesteld waarbij individuele leden van de cyberteams ingezet zouden worden op cyberzaken van het THTC. Uit de interviews komt naar voren dat op incidentele basis sprake is van uitwisseling van medewerkers van de cyberteams en van uitwisseling van informatie. Zo heeft het THTC wel het cyberteam van de eenheid Rotterdam in een cyberzaak (van de gekloonde modems) ondersteund. Er is echter geen intensieve vorm van samenwerking tussen het THTC en de cybercrimeteams van de regionale eenheden ontstaan.

Samenwerking binnen politieorganisatie, eenheid overstijgend

Een belangrijk kenmerk van cybercrime is dat deze niet gebiedsgebonden is; zo beperken de meeste fenomenen van cybercrime en netwerken daarachter zich niet tot één gebied, politie-eenheid of zelfs een land. Uit de interviews komt naar voren dat slechts op incidentele basis sprake is van een operationele samenwerking tussen de cyberteams van enkele politie-eenheden; indien men een cyberzaak start met de aangifte in een bepaalde eenheid zal men veelal ook zelf als cyberteam van deze eenheid (indien mogelijk) de dader aanhouden indien deze in de regio van een andere eenheid woonachtig is of verblijft. Er zijn op projectbasis samenwerkingsvormen geweest tussen de cyberteams van Noord-Holland en Zeeland-West Brabant (bij de oplossing van Tikkiefraude) en bij een project tussen de cyberteams van Amsterdam en Limburg.
Overdracht en samenwerking tussen de cyberteams is tot nu toe echter beperkt en de focus van de inzet van de cyberteams is vooral gericht op hun eigen werkgebied. Bij de inzet van de cyberteams ontbreekt hierdoor een herkenbare focus in welke cyberfenomenen men gezamenlijk, landelijk kan aanpakken en waarop men deskundigheid kan opbouwen.

De eerste aanzetten tot afstemming en samenwerking worden hiertoe sinds eind 2018 gedaan door middel van het Landelijk Operationeel CyberOverleg (LOCO) van teamleiders van de cyberteams, cyberofficieren van het Openbaar Ministerie en leden van DLIO/Intel. Het initiatief om eenheidsoverstijgend, fenomeen- of thematisch gericht te werken binnen de aanpak van cybercrime is hieraan voorafgaand door medewerkers van DLIO en DRIO in verschillende politie-eenheden zelf genomen. Dit doen zij in het kader van het Nationaal Cyberbeeld en de onderliggende eenheidsbeelden. Een eerste stap van het Plan van Aanpak Eenheidsbeelden Cybercrime is door DLIO uitgevoerd. De DRIO's van enkele politie-eenheden hebben voor een verbetering van de informatiepositie naar samenwerking gezocht en vijf-zes cyberthema's onderling verdeeld zodat daarop enige specialisatie kan worden opgebouwd. Vanuit de DRIO's en

DLIO wordt ook expliciet naar samenwerking met externe partijen gezocht om de deskundigheid van de politie op het cybervlak te verbeteren.

Een belangrijk knelpunt in de verbetering van de informatiepositie van de politie bij cybercrime is echter het ontbreken, dan wel 'weghalen' van analysecapaciteit voor zowel een verdiepende analyse als het actueel houden van de analyse van de aangiften. Mede omdat er geen concrete opdracht is geformuleerd richting de eenheden om analysecapaciteit te leveren, is sprake van een ongelijkwaardige inzet van eenheden bij DRIO waarbij de gewenste formatiecapaciteit voor analyse voor andere doeleinden wordt ingezet. De ontwikkeling van Cyberbeelden op eenheidsniveau en vervolgens van een Nationaal Cyberbeeld wordt daardoor belemmerd. Het ontbreken van een (landelijke) aansturing en inkadering op de inzet van de DRIO's en DLIO geeft onduidelijkheid over de mogelijkheden om de informatiepositie bij cyberfenomenen verder te verbeteren. De verbetering van de aanpak van cybercrime binnen de politie is daarmee onder meer ook afhankelijk van de medewerking van leidinggevenden binnen de politieorganisatie die ook het belang van een intensivering van de cyberaanpak zouden moeten onderschrijven en ondersteunen. Het ontbreken van een meer landelijke, beleidsmatige aansturing op dit vlak waarbij bestrijding van cybercrime niet het onderspit delft indien andere prioriteiten zich voordoen, werkt volgens een aantal betrokkenen bij Intel 'enorm verlammend' en is een uiting van 'coördinatie- en sturingsproblemen' bij de intensivering van de aanpak van cybercrime.

Samenwerking met burgers; politievrijwilligers

In het plan van het PIAC is tevens gewezen op de mogelijkheid om politievrijwilligers in te zetten bij de aanpak van cybercrime. Uit een interne inventarisatie in 2017 bleek dat bij de politie ruim tweehonderd vrijwilligers werkten die over relevante ICT-kennis en -expertise beschikken. Er zijn eind 2018 veertien vrijwilligers geselecteerd die hoofdzakelijk bij het Darkwebteam van de Landelijke Eenheid en deels bij het cybercrimeteam van de eenheid Rotterdam aan de slag zijn gegaan.

Samenwerking met partners vanuit een barrièremodel

In de aanpak van cybercrime zijn ook initiatieven genomen waarin externe partners, waaronder ook lokale overheden, expliciet een rol krijgen. Zo werkt men vanuit het 'barrièremodel', een strategie om met verschillende partijen zoveel mogelijk barrières op te werpen en het verdienmodel van criminelen te doorbreken. Dat gebeurt op verschillende manieren, zoals door het goed in de gaten houden van het 'darkweb', het waarschuwen van mensen voor phishingmails en het aangaan van een dialoog met producenten van hardware en software om applicaties veiliger te krijgen. In een artikel wijst Stol (2018) in dit kader op de mogelijke rol van de gemeente die ten onrechte nog nauwelijks een rol speelt in de bestrijding van digitale criminaliteit. Politie en gemeenten kunnen meer samen optrekken. Gemeenten kunnen bijvoorbeeld initiatieven nemen om in hun gemeente de weerbaarheid tegen digitale criminaliteit te vergroten en de samenwerking ter bestrijding van digitale criminaliteit te versterken door partijen bij elkaar te brengen.

In dit 'barrièremodel digitale criminaliteit en cybercrime' zijn onder meer enkele pilots in Oost Nederland gestart, waar men zich richt op bewustwording en 'betekenisvolle' interventies. Bewustwording is van belang vanwege het preventieve effect dat hiervan uitgaat. Daarnaast is het belangrijk dat ketenpartners weten wat ze moeten doen als ze getroffen worden door een cyberaanval (bijvoorbeeld: het voorkomen van datavernietiging door een verkeerde aanpak, wat te doen als een cyberaanval de oorzaak is van een GRIP-situatie, wat zijn dan de 'do's en don'ts' en wat betekent dat voor de crisisorganisatie?).

Voorbeelden van interventies vanuit de barrière-aanpak zijn:

- een digitale authentieke handtekening-app die door politie, OM, enkele gemeenten (waaronder Nijmegen), de Radboud Universiteit samen met grote webshops, brancheorganisaties en postorderbedrijven wordt ontwikkeld. Het betreft de app IRMA ('I reveal my attributes'). Deze aanpak voor een verbeterde digitale identiteit van burgers vloeit voor uit een nieuwe publiek-private samenwerking, waarin de Radboud Universiteit 'technisch' het voortouw heeft genomen en de gemeente Nijmegen als testgemeente optreedt;
- de pilot 'betekenisvol handelen bij aangiften van fraude en onlinehandel'; deze pilot wordt uitgevoerd in IJsselland Zuid. Het gaat hier om de aanpak van verdachte rekeninghouders (katvangers/'moneymules') die hun bankrekening (laten) gebruiken ten behoeve van internetoplichting. Zij worden thuis door de politie bezocht (met een 'stopgesprek') en krijgen de mogelijkheid een schuldbekentenis te ondertekenen en het slachtoffer terug te betalen (vanuit een civiele overeenkomst). Indien men niet mee werkt, kan een strafrechtelijk onderzoek worden gestart. De pilot draagt bij aan genoegdoening, het stoppen van het strafbare feit en het vergt geen extra opsporingscapaciteit van het basisteam.

Samenwerking in netwerken en met externe partijen

De cybercrimeteams hebben op incidentele basis ook samenwerkingsprojecten die gerelateerd zijn aan bepaalde vormen van cybercrime. Zo is in de aanpak tegen 'phishing' door een van de cybercrimeteams samen met de ING een script ontwikkeld in het spamphishing-project bij het ECTF, als een samenwerking tussen de politie en banken. Deze samenwerking vindt plaats op basis van een landelijk convenant waarin afspraken zijn gemaakt over de deling van cyberinfo. Daarnaast is op incidentele en beperkte basis samenwerking tussen de cybercrimeteams en externe partijen. Een van de enkele cases betreft de samenwerking van het cyberteam van Rotterdam met Ziggo voor de aanpak van de zaak rondom gekloonde modems. Er zijn daarnaast nauwelijks contacten met externe, commerciële partijen/bedrijven (zoals Fox-IT of andere IT-bedrijven) voor aanpak cybercrime mede vanwege de problematiek rondom informatiedeling met externe partijen over mogelijk strafbare feiten. Er is bij het cyberteam van Noord-Holland wel sprake van landelijke mediacontacten om de aanpak van cybercrime bij een breder publiek over het voetlicht te krijgen.

4 Samenvatting en conclusies

4.1 Samenvatting

Cybercrime als aandachtspunt voor de politie

Cybercrime en de aanpak daarvan is voor de Nederlandse politie al verscheidene jaren een reden van aandacht en ook van zorg. Een belangrijke reden voor de zorg was onder meer het gebrek aan kennis bij politie en justitie inzake de 'digitalisering van de criminaliteit' waarmee zij niet goed weten om te gaan. De conclusie uit eerdere onderzoeken was dat politie en justitie veel moeite hebben met misdaadbestrijding in cyberspace.

De politie heeft in voorgaande jaren de eerste stappen gezet om cybercrime te bestrijden en strafrechtelijk aan te pakken. Een concreet voorbeeld was de oprichting van het Team High Tech Crime (THTC) bij de Landelijke Eenheid in 2007 dat zich met name richt op landelijke en internationale cyberzaken. Bovendien is in 2008 het Programma Aanpak Cybercrime (PAC) ingesteld door de Raad van Hoofdcommissarissen en in datzelfde jaar is ook het OM met een programma Cybercrime gestart.

Cybercrime als urgent aandachtspunt; intensivering van de aanpak van cybercrime

Ofschoon de politie een aanzet had gemaakt met de aanpak van cybercrime, bleek deze ontoereikend te zijn. In het Plan van Aanpak Intensivering Aanpak Cybercrime (PIAC, 2016) werd opgemerkt dat de politie een achterstand heeft in de aanpak van cybercrime: op regionaal niveau werd in de eenheden nauwelijks capaciteit ingezet, de informatiepositie van de politie op dit thema was zwak en ook de (minimale) resultaatdoelstellingen werden niet gehaald. Mede gezien de geconstateerde populariteit van Nederlandse infrastructuur onder cybercriminelen werd een intensivering van de aanpak noodzakelijk geacht. Een van de zichtbare tekortkomingen was dat de intake van cybercrime niet op orde is, waardoor slachtoffers geen gehoor bij de politie vinden.

Cybercrimeteams als instrument voor intensivering aanpak

De intensivering van de aanpak diende ook op regionaal niveau verder ingevuld te worden, hetgeen tot de oprichting van regionale 'cybercrimeteams' heeft geleid. De eerste opbrengsten van de aanpak werden echter niet hoog ingeschat: de cyberteams werden niet goed ingezet en digitale criminaliteit kreeg door een gebrek aan mankracht vaak toch geen voorrang. De conclusies uit voorgaande onderzoeken gaven alle reden om de bestrijding van cybercrime meer aandacht te laten geven door de politie.
De prioritering van de aanpak van cybercrime bij de politie is terug te vinden in de afspraken van de Veiligheidsagenda 2015-2018. Daarin zijn de volgende kwantitatieve en kwalitatieve doelen voor de politie geformuleerd:

- het opsporen en aanhouden van verdachten van cybercrime en het overdragen van de dossiers hiervan aan het Openbaar Ministerie (op basis van het leveren van een vastgesteld aantal cybercrimezaken);
- het opbouwen van kennis en ervaring met de aanpak van cybercrime en het overdragen hiervan aan andere teams binnen de politie-eenheid;
- het geven van aandacht aan preventie en het 'weerbaar' maken van organisaties en het publiek voor cybercrime; aspecten die hierin genoemd worden zijn preventie, verstoren, signaleren en adviseren.

Om deze doelen te behalen is aan de cybercrimeteams van de politie-eenheden een belangrijke rol toebedacht. In het organisatieproces van intake naar opsporing wordt met name gestreefd naar de invulling van een aantal speerpunten:

- een verbetering van de intake en screening van mogelijke cybercrimezaken;
- het opbouwen van een informatie- en intelligencepositie binnen de DLIO en DRIO's;
- het vrijmaken van tactische capaciteit binnen de politie-eenheden voor de samenstelling van cyberteams;
- de verspreiding van kennis en kunde binnen de verschillende lagen van de politie-eenheden;
- samenwerking met publieke en private partners;
- een vergroting van de bewustwording van de problematiek van cybercrime bij burgers.

Cybercrime en opheldering door politie

De omvang van de bij de politie geregistreerde cybercrime is vooral af te leiden uit de aangiften die zij naar aanleiding van meldingen van slachtoffers van cybercrime (van burgers en van bedrijven) opmaken. In de jaren 2015-2017 varieerde het aantal aangiften van 'computercriminaliteit' tussen 1.900 en 2.300 aangiften, in 2018 is dit aantal gestegen naar 2.900 aangiften. Het aantal geregistreerde aangiften van cybercrime omvat echter maar een beperkt deel van het ondervonden slachtofferschap; uit de Veiligheidsmonitor 2017 komt naar voren dat in bijna driekwart van de cyberdelicten geen aangifte bij de politie wordt gedaan. Ook het opheldering spercentage van cybercrime-delicten (4,6% in 2017) is veel lager dan het gemiddelde aantal opgeloste misdrijven door de politie (namelijk 23%). Deze cijfers over beperkte aangiftebereidheid en geringe opheldering van cyberzaken impliceren dat de politie geen accuraat beeld heeft van de aard en omvang van cybercrime en ook nog geen adequaat antwoord op de 'digitalisering van de misdaad' (Stol, 2018).

Het verkennend onderzoek wijst uit dat het aantal aangiften van cybercrime bij de politie in 2018 is toegenomen en dat absoluut en relatief meer cybercrimezaken door de politie worden aangepakt en opgelost (met een opheldering spercentage van 8,3%). Ook is het aantal aangehouden verdachten van cybercrime toegenomen van 220 in 2017 naar 400 in 2018. De pakkans van cybercrime blijft echter erg laag.

Cybercrimeteams in regionale eenheden

De aanpak van cybercrime door de cyberteams is vanaf najaar 2015 in pilotvorm in enkele eenheden gestart; sinds begin 2018 hebben acht politie-eenheden een cybercrimeteam, de eenheden Den Haag en Oost-Nederland werken met een 'flexibel team'. In de verkenning is nader ingezoomd op de wijze waarop drie politie-eenheden (Noord-Holland, Rotterdam en Oost Nederland) de aanpak van cybercrime organisatorisch en inhoudelijk vorm geven.

Voor de samenstelling van de cybercrimeteams is men bij de start uitgegaan van een 'minimale ondergrens' van 10 fte tactische recherchecapaciteit. In de praktijk blijkt dat er verscheidene grotere en kleinere cyberteams in de eenheden zijn (variërend van 4 fte tot 25 fte) en in de eenheid Den Haag heeft men formeel geen capaciteit voor een cyberteam, evenals in de eenheid Oost Nederland (tot 2019). Bij de onderzochte eenheden is inmiddels sprake van grotere cyberteams, in ieder geval in Noord-Holland (25 fte) en Rotterdam (25 fte). Voor de tactische capaciteit is in verschillende mate ruimte vrijgemaakt vanuit verschillende afdelingen en teams; zo zijn de leden van de cyberteams afkomstig uit de Dienst Regionale Recherche, de districtsrecherche en de basisteams recherche; digitaal specialisten van het Team Digitale Opsporing (TDO) en informatieanalisten van DRIO worden in wisselende mate direct of indirect betrokken bij de inzet van de cyberteams. In een van de regionale teams (eenheid Rotterdam) worden sinds 2018 ook enkele politievrijwilligers 'met digitale vaardigheden' ingezet om het cyberteam te ondersteunen.

Meldingen en aangiften van cybercrime

In de aangiften bij de politie zijn enkele hoofdvormen van cybercrime te herkennen, waarbij met name de Tech Support Scam (de `Microsoft Scam') veel voorkomt. Hacken van accounts voor bestellingen ('account take over') en fraude van bankgegevens, i.c. internetbankieren ('phishing') zijn ook twee vormen van cybercrime die veelvuldig worden gepleegd. Daarnaast komen factuurfraude (de CEO-fraude) en aan- en verkoopfraude (waaronder fraude op online-handelssites zoals Marktplaats) relatief vaak voor.

Burgers en bedrijven kunnen cybercrime melden via het centrale telefoonnummer van de politie of op een politiebureau aangifte doen. Op haar landelijke website geeft de politie aan dat van een aantal vormen van cybercriminaliteit ook online aangifte gedaan kan worden, maar dit geldt vooralsnog alleen voor internetoplichting (dat in strikte zin beschouwd geen cybercrime is, maar een vorm van gedigitaliseerde criminaliteit).
Bij een melding van cybercrime of een vorm van gedigitaliseerde criminaliteit bij de politie komt de burger, het bedrijf of de organisatie als eerste in contact met een medewerker Intake & Service. De relatieve onbekendheid met cyberdelicten bij Intake & Service en bij het RSC wordt, ondanks de voorlichting die leden van cyberteams aan I&S geven en de tools die beschikbaar zijn gekomen om een melding en aangifte adequater te behandelen, als een knelpunt ervaren. Het heeft onder meer tot gevolg dat bij de melding ervan mogelijke cyberzaken niet als zodanig worden herkend en de aangifte niet goed wordt behandeld. De politieregistratie en de omgang met de meldingen van 'cybercrime' zijn in dit kader niet eenduidig en weerspiegelen slechts een deel van de 'cybercriminaliteit'.

Om dit inzicht te verbeteren is door DLIO een landelijke query ontwikkeld en deze wordt door de cyberteams toegepast waardoor zij meer en andersoortige cyberzaken beter in beeld krijgen. Het onderscheid tussen cybercrime en gedigitaliseerde criminaliteit in de aangemelde zaken blijkt echter lastig te hanteren, aangezien diverse vormen van cybercrime verweven zijn met uiteenlopende vormen van gedigitaliseerde criminaliteit.

Screening van cyberzaken

De lage kwaliteit van de aangifte had en heeft tot gevolg dat belangrijke informatie in de aangifte ontbreekt, waardoor aangiften al tijdens de casescreening worden opgelegd, i.c. niet in behandeling worden genomen. In de drie onderzochte eenheden zijn en worden verschillende wegen bewandeld om de screening van cyberzaken te verbeteren. Een van de methoden is het 'Cybercenter' dat het cyberteam van Noord-Holland als een soort 'hulploket' voor basisteams heeft ingericht. Het cyberteam zorgt in dit geval voor de screening, veredeling en vervolgens het 'panklaar' neerleggen van de cyberzaken bij de basisteams. In de twee andere eenheden vindt de screening plaats bij het Operationeel Coördinatie Knooppunt, dat onderdeel is van het basisteam. De verkenning wijst uit dat bij deze screening van aangiften relatief weinig opsporingsinformatie wordt gevonden als het om (mogelijke) cyberzaken gaat. Beide eenheden hebben om dit op te lossen tijdelijke aanvullende inzet gehad van een casescreener of een leidinggevende van een TDO erbij betrokken om de casescreening te verbeteren. De inzet van casescreening is in deze gevallen derhalve niet structureel hetgeen negatieve consequenties kan hebben voor de beoordeling van mogelijke cyberzaken.

Informatieanalyse cybercrime

Voor de verrijking van de cyberinformatie is er, naast de rol van de casescreeners, in de regionale politie-eenheden ook een rol van informatieanalisten van de Dienst Regionale Informatie Organisatie (DRIO). Het gaat hier om een ''opbouw van intelligence in brede zin" als het om cybercrime gaat. Door de DRIO's worden 'cyberdashboards' opgesteld en sinds begin 2019 ook de eerste 'Eenheid Cyber Beelden' (ECB). De regionale eenheidsbeelden zouden in principe samen het eerste 'Nationaal Cyber Beeld' (NCB) kunnen vormen (als verlengstuk van het Nationaal Dreigingsbeeld). Dit Nationaal Cyber Beeld is nog niet gereed.

De DRIO's van de onderzochte (en andere) politie-eenheden hebben, op eigen initiatief en zonder beleidsmatige aansturing en inkadering, voor een verbetering van de informatiepositie naar onderlinge samenwerking gezocht. Zij hebben daarbij een vijftal cyberthema's verdeeld zodat daarop enige specialisatie kan worden opgebouwd. Het gaat om thema's inzake cybercrime en gedigitaliseerde criminaliteit met de meest voorkomende vormen en met de grootste toegebrachte schade voor burgers. Voor het onderzoeken van mogelijke trends in de onderscheiden cyberthema's wil men samen met DLIO ook vaker externe partijen betrekken, maar deze samenwerking is nog niet goed van de grond gekomen.

Voorbeelden van onderzoeken cyberteams

In het licht van de afspraken in de Veiligheidsagenda richten de cyberteams van de regionale eenheden zich op de aanpak van cybercrime (in enge zin), maar in de praktijk krijgen zij veel meldingen waarbij ook sprake is van een vorm van gedigitaliseerde criminaliteit. De scheidslijn tussen cybercrime en gedigitaliseerde criminaliteit is daarbij niet altijd scherp te trekken. De teamleiders van de cyberteams geven aan dat het motto bij de inzet van de politie bij cyberzaken is: *"waar de burger en bedrijven last van hebben bij cybercrime"*.

Daarnaast wordt in de Veiligheidsagenda onderscheid gemaakt tussen complexe en reguliere cybercrime zaken, waarbij het Toewijzingskader Opsporing in principe handvaten geeft om het onderscheid in de praktijk te kunnen maken en zaken toe te kunnen wijzen. De inzet van de regionale cyberteams omvat voor het grootste deel reguliere cybercrimezaken waarbij er sprake is van 'veelvoorkomende cybercrime' (VVCC) waarop men incidentgericht reageert. De inzet van de cyberteams betreft dan ook uiteenlopende activiteiten, waaronder onderzoek naar phishing, sextortion, hacking, Tikkiefraude, CEO-fraude, et cetera.

Incidenteel worden door de cyberteams ook grotere zaken gedraaid, waarbij de aanpak 'meer complex' is en ook meer fenomeenonderzoek wordt uitgevoerd. Voorbeelden daarvan zijn onder meer de aanpak van gekloonde modems door het cyberteam in Rotterdam, onderzoek naar Tikkiefraude via Markplaats en van de hacking van accounts van bekende 'YouTubesterren' door het cyberteam Noord-Holland. Een ander voorbeeld van een 'complex onderzoek' is uitgevoerd door de eenheid Oost-Nederland waarbij chatberichten van criminelen via versleutelde PGP-telefoons ('Ironchat'), waarmee personen in principe ongestoord met elkaar kunnen communiceren, gedurende een bepaalde periode 'live' zijn gevolgd. Hiermee is het cryptoverkeer ontsleuteld en kon de politie meekijken met het criminele communicatieverkeer.

Tactische inzet in cyberteams en opsporing

De cybercrimeteams zijn samengesteld uit rechercheurs uit de Dienst Regionale Recherche, de districtsrecherche, de basisteams recherche, maar ook zijn leden van het Team Digitale Opsporing (TDO) en de DRIO in meer of mindere mate direct betrokken bij de inzet van de cyberteams. Voor de cyberteams in de onderzochte eenheden geldt dat er een grote behoefte is om de specialistische digitale kennis binnen de generieke opsporing te versterken. Bij de tactische recherchedeskundigheid gaat het om vorderingen opstellen, aanvragen, ('uitlezen') en opbouw van inhoudelijke deskundigheid voor de opsporing. Bij de cyberteams waarin 'blauw', zonder specifieke opsporingsdeskundigheid instroomt, vormt dit een extra aandachtspunt aangezien zij de noodzakelijke kennis en vaardigheden missen om aan de vereiste deskundigheid te voldoen.

Opsporing en doelen Veiligheidsagenda

De opsporing van daders van cybercrime blijkt in de praktijk een complexe aangelegenheid te zijn waarbij de kans op succes gering is: de mogelijkheden voor criminelen om in grote mate anoniem en deels ook in het buitenland via het internet te opereren zijn groot. Het opheldersingspercentage van 8% van cybercrime-aangiften bij de politie (in 2018) geeft aan dat er veelal geen succesvolle opsporing op de veel voorkomende cybercrime plaatsvindt.

De kwantitatieve doelen uit de Veiligheidsagenda 2015-2018 zijn bedoeld om de aanpak van cybercrime door de politie te stimuleren en hierin wordt, gezien de toename van het aantal bij het OM ingediende zaken van cybercrime, vooruitgang geboekt. De geformuleerde prestatie-indicatoren geven echter onvoldoende weer welke inzet men vanuit de politie kan en moet plegen voor het opsporen van cybercrimeverdachten.
In de praktijk blijkt dat de cyberincidenten die de politie registreert voornamelijk 'brengzaken' zijn en dat derhalve alleen een beeld bestaat en ook actie wordt ondernomen op de binnengekomen aangiften; voor een proactieve aanpak in de vorm van 'haalzaken' is veelal geen formatiecapaciteit voorhanden, of wordt daar niet voor vrijgemaakt. De opgestelde normen geven de cyberteams vooral weinig ruimte om inzet te plegen voor de aanpak van 'fenomenen' binnen de cybercrime die relatief veel tijd en capaciteit vergen. Door de complexiteit van en tijdsbeslag aan één cyberzaak, waaraan men maanden bezig kan zijn, loopt een cyberteam het risico dat men het aantal afgesproken cyberzaken, niet haalt. De behoefte om meer 'cyberdeskundigheid' op te bouwen met fenomeenonderzoeken 'aan de voorkant' botst derhalve met de noodzaak om de kwantitatieve doelen te behalen.

Vervolging en sanctionering cybercrime

De relatieve onbekendheid die politie en het Openbaar Ministerie in eerste instantie hadden met het fenomeen 'cybercrime' heeft ook tot een onderlinge zoektocht geleid om tot meer adequate gezamenlijke afspraken te komen. Ook voor de organisatie van het Openbaar Ministerie betekende dit het opbouwen van meer 'cyberdeskundigheid', bij officieren van justitie en parketsecretarissen. Bovendien is de focus van de geïnterviewde officieren bij het OM in de drie politie-eenheden niet (meer) gericht op het bestrijden van 'cybercrime in enge zin' maar op gedigitaliseerde criminaliteit of "alles wat samenhangt met criminaliteit en digitaliteit".

Veel van de door de politie aangedragen cyberzaken worden bij het OM afgedaan zonder dat deze een parketnummer krijgen; er wordt relatief vaak besloten tot een (technisch) sepot. Hierbij gaat men uit van een bij voorbaat kansloze vervolging omdat de dader niet kan worden aangehouden. Bij de vervolging en sanctionering van verdachten van computervredebreuk die wel zijn aangehouden, komt het voor dat het Openbaar Ministerie zonder tussenkomst van de rechter een strafbeschikking uitdeelt of een transactie aanbiedt (een werkstraf of geldboete).

Uit de analyse van cijfers van het Openbaar Ministerie over 2018 komt naar voren dat van de totale instroom van cyberzaken 50% is geseponeerd. Bij de cyberzaken waarin wel sprake is van strafvervolging is het aandeel OM-afdoeningen 60% en het aandeel ZM-afdoeningen 40%. Met de intensivering van de aanpak van cybercrime is bij het Openbaar Ministerie ook meer het besef ontstaan dat cybercrime 'serieuze criminaliteit' kan zijn en derhalve als ernstige delicten dienen te worden beschouwd indien het gekoppeld wordt aan een criminele organisatie.

Dadergroepen

Cybercrime wordt door verschillende typen dadergroepen gepleegd. Beroepscriminelen richten zich op bedrijven in het MKB voor financieel gewin en vormen een doelgroep voor de regionale cyberteams. Bij de aanpak van cybercrime uitgevoerd door statelijke actoren hebben de regionale cyberteams geen rol; het voortouw wordt daarin door het THTC genomen. Daarnaast zijn er individuen die de kennis en mogelijkheden hebben om in geautomatiseerde systemen van bedrijven en organisaties in te breken. Zo zijn er op online-marktplaatsen complete pakketten te koop voor 'cybervandalen' die daarmee kunnen hacken of een Ddos-aanval uitvoeren (de aanbieders van malware hebben soms ook een 'helpdesk' voor de personen die deze aanvallen willen uitvoeren; dit fenomeen van ondersteuning staat bekend als 'crime as a service').
In de cyberbeelden die door politie-eenheden zijn opgesteld, is relatief weinig informatie opgenomen over mogelijke dadergroepen. Veelal blijkt dat mogelijke dadergroepen onbekend zijn en/of in het buitenland vertoeven. Een aanzienlijk deel van het financieel gemotiveerde cybercrime wordt naar verwachting wel gepleegd door Nederlandse beroepscriminelen die niet alleen in het digitale domein actief zijn. Daardoor is mogelijk niet zozeer sprake van een verschuiving van offline criminaliteit naar online criminaliteit, maar eerder van een verbreding van het criminele takenpakket binnen bestaande dadergroepen.

Aanpak cybercrime: een inzet op meerdere sporen

Bij de bestrijding van cybercrime onderscheidt de politie een aantal taken: preventie, verstoring, schadebeperking en opsporing. In de discussies over de aanpak worden door de politie ook nieuwe termen geïntroduceerd, die variaties op een thema omvatten (waaronder de termen attributie, notificatie, e.a.). De verkenning wijst uit dat met alleen de opsporing van cybercrime de politie de problematiek slechts deels kan bestrijden en dat aanvullende strategieën noodzakelijk zijn.
Bij preventie gaat het om het versterken van de bewustwording en van de digitale weerbaarheid van burgers en bedrijven. Hiertoe heeft de politie in 2017 en 2018 onder meer voorlichtingscampagnes opgezet waarbij met name wordt gewaarschuwd voor oplichting via de 'Tech Support Scam' ('Microsoftscam'). Ook geeft de politie waarschuwingen en preventietips rondom actuele cybercrime-fenomenen, waaronder nepbetaalverzoeken, phishing, CEO-fraude, oplichting via WhatsApp en de ransomware GandCrab.

Een tweede aanpak van de politie, uitgevoerd in samenwerking met enkele externe partijen, omvat de verstoring van de cyberdaad en cyberdader. De cyberteams pakken dit aan door bijvoorbeeld een malafide website te (laten) blokkeren ("op zwart te zetten"), een foute bankrekening te (laten) blokkeren of de naam van een fraudeur op te nemen in het Check Verkoper register. Een aanvullende aanpak van de politie, i.c. cyberteams, bestaat uit 'signalering en advisering' (notificatie); dit betreft het op de hoogte stellen van burgers en bedrijven die slachtoffer geworden zijn of mogelijk gaan worden van een vorm van cybercrime. De notificatie kan bijvoorbeeld bij bedrijven zijn om wachtwoorden van computersystemen aan te passen zodat de toegang hiervan voor criminelen (alsnog) wordt verhinderd. Een voorbeeld van een dergelijke aanpak is ook de grootschalige benadering van bedrijven in de regio door de politie Oost

Nederland voor het fenomeen van 'CEO-fraude'. Ook de eenheden Noord-Holland, Noord-Nederland en Den Haag hebben zich samen met publiek-private partijen ingezet om CEO-fraude en 'Business E-mail Compromise Fraud' (BEC-fraude) aan te pakken. Een vierde aanpak omvat schadebeperking en het ondersteunen van burgers en bedrijven op het moment dat ze slachtoffer zijn geworden van cybercrime; de website www.nomoreransom.org is hiervan een voorbeeld.

Samenwerkingsvormen cyberteams aanpak cybercrime

In de plannen voor een geïntensiveerde aanpak van cybercrime door de politie is onder meer gewezen op de wens en noodzaak van samenwerking binnen de politieorganisatie en met publieke en private partners. Deze samenwerking zou met name gericht dienen te zijn op informatie-uitwisseling en het nemen van maatregelen ten behoeve van preventie en het opwerpen van barrières.
Inmiddels zijn verscheidene organisaties en instanties bezig met de bestrijding van verschillende vormen van cybercrime. Zo is er het Landelijk Meldpunt Internet Oplichting (LMIO) dat zich specifiek richt op het tegengaan van oplichting in de internethandel (bijvoorbeeld op Marktplaats). Daarnaast is er onder meer de Electronic Crimes Taskforce (ECTF), het zogenaamde 'bankenteam', dat zich richt op het voorkomen en aanpakken van digitale criminaliteit in de financiële sector (zoals financiële malware en phishing- aanvallen). De politie is landelijk vertegenwoordigd in deze ECTF; er is geen directe deelname hieraan van leden van de regionale cyberteams.

Binnen de politieorganisatie is een gezamenlijke afspraak gemaakt voor uitwisseling van kennis tussen het THTC en de cyberteams van de regionale eenheden. Zo is een 'adoptie' van eenheden door het THTC voorgesteld waarbij individuele leden van de cyberteams ingezet zouden worden op cyberzaken van het THTC. In de praktijk blijkt dat op incidentele basis sprake is van uitwisseling van medewerkers van de cyberteams en van uitwisseling van informatie. Er is echter geen intensieve vorm van samenwerking tussen het THTC en de cybercrimeteams van de regionale eenheden ontstaan.

Een belangrijk kenmerk van cybercrime is dat deze niet gebiedsgebonden is; zo beperken de meeste fenomenen van cybercrime en netwerken daarachter zich niet tot één gebied, politie-eenheid of zelfs een land. De verkenning wijst uit dat desalniettemin slechts op incidentele basis sprake is van een operationele samenwerking tussen de cyberteams van politie-eenheden. Overdracht en samenwerking tussen de cyberteams is tot nu toe beperkt en de focus van de inzet van de cyberteams is vooral gericht op hun eigen werkgebied. Bij de inzet van de cyberteams ontbreekt een herkenbare focus in welke cyberfenomenen men gezamenlijk, landelijk kan aanpakken en waarop men deskundigheid kan opbouwen.
De eerste aanzetten tot afstemming en samenwerking worden hiertoe sinds eind 2018 gedaan door middel van het Landelijk Operationeel CyberOverleg (LOCO) van teamleiders van de cyberteams, cyberofficieren van het Openbaar Ministerie en leden van DLIO/Intel. Vanuit de DLIO en DRIO's wordt ook expliciet naar samenwerking met externe partijen gezocht om de informatiepositie en deskundigheid van de politie op het cybervlak te verbeteren.

In de aanpak van cybercrime zijn ook initiatieven genomen waarin externe partners, waaronder lokale overheden, een rol krijgen. Zo werkt men vanuit het 'barrièremodel', een strategie om met verschillende partijen zoveel mogelijk barrières op te werpen en het verdienmodel van criminelen te doorbreken. Dat gebeurt op verschillende manieren, zoals het waarschuwen van mensen voor phishingmails en het aangaan van een dialoog met producenten van hardware en software om applicaties veiliger te krijgen. In dit 'barrièremodel digitale criminaliteit en cybercrime' zijn enkele pilots gestart, waar men zich richt op bewustwording en 'betekenisvolle' interventies.

4.2 Conclusies

Het verkennend onderzoek naar de aanpak van cybercrime door de politie leidt tot een aantal hoofdconclusies. Deze hebben betrekking op de thema's die we in de onderzoeksvragen centraal hebben gesteld. Het betreft:

- de wijze waarop cybercrime bij de politie-eenheden is georganiseerd en de rol die cybercrimeteams hierin hebben;
- het verloop van intake en screening van cybercrime bij de politie;
- de opbouw en overdracht van deskundigheid inzake cybercrime binnen de politie-eenheid;
- de rol die informatie en analyse voor het cybercrimeteam bij de aanpak van cybercrime speelt;
- de opbrengsten van de cyberteams naar aantal cybergerelateerde zaken en naar inhoudelijke aanpak/methodiek;
- de samenwerking bij deze aanpak met andere eenheden, landelijke eenheid (THTC) en externe partijen.

Op basis van de verkenning kan een aantal constateringen worden gedaan en conclusies worden getrokken over de aanpak van cybercrime door de politie in de periode 2015 tot begin 2019. De verkenning leidt niet tot een toetsing van de voortgang die is geboekt maar tot enkele bespiegelingen over de wijze waarop de politie werk maakt van de aanpak van cybercrime. Enkele conclusies leiden ook tot aanbevelingen die als verbeterpunten voor de politieorganisatie worden geformuleerd.

Cybercrimeteams als instrument van intensivering aanpak cybercrime

De politie heeft sinds de start van het Programma Intensivering Aanpak Cybercrime (PIAC, 2016) concrete stappen gezet om de geconstateerde achterstand bij de bestrijding van cybercrime te verminderen. Naast de inzet van het THTC, is ook op regionaal niveau binnen de politie-eenheden aandacht gekomen voor deze aanpak in de vorm van acht gespecialiseerde cybercrimeteams en twee eenheden die op basis van een 'flexibele aanpak' werken.
Voor de samenstelling van de cybercrimeteams is men bij de start uitgegaan van een 'minimale ondergrens' van 10 fte tactische recherchecapaciteit. In de praktijk blijkt dat er verschei-

dene grotere en kleinere cyberteams in de eenheden zijn die boven maar ook onder deze ondergrens opereren (variërend van 4 fte tot 25 fte). In de eenheid Den Haag heeft men formeel geen capaciteit voor een cyberteam, evenals in de eenheid Oost Nederland (tot 2019).
Deze verscheidenheid in capaciteit en organisatievorm geeft vooralsnog het beeld van een 'cyberaanpak in opbouw' waarbij de eenheden zelf verschillende prioriteiten geven aan de aanpak van de cybercrime in hun eenheid. Dit betekent ook dat een aantal cyberteams onvoldoende mogelijkheden heeft om gezamenlijk met andere cyberteams landelijke onderzoeken op te pakken.

Intake en screening van cyberzaken

In een aantal voorgaande onderzoeken is de relatieve onbekendheid met cyberdelicten van medewerkers bij Intake & Service en bij het RSC als punt van aandacht benoemd. Het intakeproces inzake cybercrime blijkt ook in deze verkenning, ondanks de inzet die hiervoor in voorgaande jaren is gepleegd, nog een knelpunt te zijn. Verbetering hiervan kan worden gevonden in een nadere technische aanpassing van de query (mogelijk door 'text mining' en 'machine learning'), het instellen van een aparte helpdesk vanuit het cyberteam in de vorm van een 'Cybercenter' en gerichte ondersteuning van kernpersonen binnen I&S door aanvullende scholing waarbij nieuwe methoden van deskundigheidsoverdracht dienen te worden gevonden (alleen e-learning werkt in dit verband onvoldoende).

Verbetering van de screening van aangiften is essentieel om beter zicht op de aard en omvang van cyberzaken te krijgen. De oprichting van het 'Cybercenter' bij het cyberteam in Noord-Holland, als hulploket voor basisteams, lijkt hier de meeste inhoudelijke ondersteuning te bieden. De inzet van casescreening via de OCP's bij de basisteams in de twee andere onderzochte is niet structureel en heeft weinig inhoudelijke basis om mogelijke cyberzaken adequaat te kunnen beoordelen.

Opbouw en overdracht van deskundigheid

In de samenstelling van de cybercrimeteams is een balans gewenst in de tactische en digitale deskundigheid en mede door wisselende beschikbaarheid en inzet van deze deskundigheden zijn de teams niet altijd optimaal samengesteld.
Voor de cyberteams in de onderzochte eenheden geldt dat er een grote behoefte is om de specialistische digitale kennis binnen de generieke opsporing te versterken. De dieptekennis op digitaal vlak is met name voorhanden bij de LE (THTC) en bij de teams digitale opsporing. De TDO's zijn in veel gevallen op dit vlak ondersteunend aan onder meer de cyberteams, maar de cyberteams zelf hebben daarmee deze kennis niet altijd tot haar beschikking hetgeen een belemmering kan zijn in de kwaliteit van de opsporing.

Een aandachtspunt is ook de verspreiding van kennis en kunde binnen de verschillende lagen van de politie-eenheden. De verkenning wijst uit dat de teams hierin een modus trachten te vinden door onder meer roulatiesystemen in te bouwen waarbij er een tijdelijke, roulerende inzet is van onder meer leden van basisrechercheteams binnen het cyberteam. Een te sterke roulatie van leden van cyberteams heeft echter ook negatieve consequenties voor het niveau

van tactische en digitale deskundigheid van de cyberteams. De verspreiding van cyberdeskundigheid vraagt derhalve om een afgewogen strategie waarbij een centraal cyberteam voor een interne 'spin off' kan zorgen waarbij ook de gewenste deskundigheid binnen dit team op peil komt en kan blijven.

Informatiepositie cyberaanpak

In de politie-eenheden wordt door de DRIO's, in samenwerking met DLIO, en samen met de cyberteams gewerkt aan een noodzakelijke versterking van de informatiepositie van de politie op het terrein van cybercrime. Deze versterking vindt haar stimulans bij direct betrokkenen: er is door een aantal DRIO's en DLIO een selectie gemaakt van de vormen van cybercrime waarmee men het meest te maken krijgt en een verdeling tussen eenheden voor het nader analyseren van deze fenomenen. Uit de verkenning komt naar voren dat dit streven naar versterking van de informatiepositie binnen cybercrime een landelijke aansturing en inkadering ontbeert.

Opbrengsten naar aantal cybergerelateerde zaken en naar inhoudelijke aanpak

Bij de bestrijding van cybercrime slagen de cyberteams, i.c. de politie-eenheden, er inmiddels in meer cyberaangiften in behandeling te nemen en ook meer cyberzaken aan te leveren bij het Openbaar Ministerie. Het accent ligt daarbij op de 'veel voorkomende cybercriminaliteit'. De opsporing van daders van cybercrime blijkt echter in de praktijk een complexe aangelegenheid waarbij de kans op succes gering is. Ook bij de vervolging van cybercriminelen blijkt dat verdachten vaak buiten beeld blijven.

Andere sporen voor aanpak cybercrime

Voor een meer succesvolle aanpak van cybercrime zet men ook in op andere sporen, zoals preventie, het signaleren en het verstoren van cybercriminelen in hun activiteiten. Het versterken van barrières tegen 'digitale criminaliteit' en het focussen op specifieke fenomenen binnen de cybercrime zal naar verwachting de effectiviteit van de aanpak van cybercrime door de politie vergroten.

Samenwerking

Een belangrijk kenmerk van cybercrime is dat deze niet gebiedsgebonden is; zo beperken de meeste fenomenen van cybercrime en netwerken daarachter zich niet tot één gebied, politie-eenheid of zelfs een land. Uit de verkenning komt naar voren dat slechts op incidentele basis sprake is van een operationele samenwerking tussen de cyberteams van enkele politie-eenheden. Overdracht en samenwerking tussen de cyberteams is tot nu toe echter beperkt en de focus van de inzet van de cyberteams is vooral gericht op hun eigen werkgebied. Bij de inzet van de cyberteams ontbreekt hierdoor een herkenbare focus in welke cyberfenomenen men gezamenlijk, landelijk kan aanpakken en waarop men deskundigheid kan opbouwen. Voor de aanpak van cybercrime betekent dit dat de politie zich minder geografisch en meer thematisch zal dienen te organiseren.

In de bestrijding van cybercrime is ook de samenwerking tussen politie en publieke en private partijen als speerpunt benoemd. Uit de verkenning komt naar voren dat met enkele netwerken wordt samengewerkt (zoals in het 'bankenteam') en ook met een enkele lokale overheid bij het opzetten van een 'barrièremodel'. De verkenning wijst uit dat deze aanpak, in samenwerking met overheden en bedrijven, meer aandacht kan krijgen als een vorm van preventie bij cybercrime.

Inbedding cyberaanpak binnen de politie-eenheden

Bij een meer algemene beschouwing van de aanpak van cybercrime bij de politie komt uit de verkenning naar voren dat de organisatie van een aantal processen de staande organisatie ongemoeid laat. De cyberteams, vooralsnog met tijdelijke opdracht en status, het PIAC en het LOCO en andere initiatieven op dit vlak worden buiten de reguliere processen om georganiseerd waardoor de urgentie van een cyberaanpak ook niet binnen de hele organisatie wordt gevoeld. Er is dit kader geen duidelijkheid over welke inbedding de cyberaanpak binnen een politie-eenheid of over de eenheden heen heeft en het wordt ook niet voor de politieorganisatie duidelijk of de processen te traag worden uitgevoerd of wellicht anders moeten.

Intensivering aanpak cybercrime: keuze voor specialisme of breedte

De beleidsmatige keuze voor de oprichting en inzet van cyberteams als een specialistisch team volgde op de constatering van het ministerie dat de 'breedte-benadering' binnen de politie weinig vruchten had afgeworpen (zie ook Stol, 2018). Beide benaderingen kunnen in theorie voordelen bieden, voor enerzijds een bredere en snellere spreiding van kennis van de aanpak van cybercrime binnen de politieorganisatie, i.c. de basisteams recherche, en anderzijds een opbouw van digitale expertise die het (beter/meer) mogelijk maakt om fenomeen-onderzoek te doen, met explicieter aandacht voor de modus operandi van daders en meer mogelijkheden om samen te werken met andere (gespecialiseerde) cyberteams.
Dit zijn twee visies die invloed hebben gehad binnen de politieorganisatie: de breedtebenadering zoals bepleit door het PAC enerzijds en anderzijds de specialistenbenadering die vanwege de voorgeschreven targets in de Veiligheidsagenda door middel van de cyberteams is geïntroduceerd. De keuze voor een aanpak via de cyberteams betekent dat er ruimte komt voor specialisten, maar bergt ook het risico in zich dat 'anderen' binnen de politieorganisatie er dan niets meer aan doen.
Aangezien ook bij de traditionele vormen van criminaliteit steeds vaker sprake is van een digitale component en de politie daar binnen meerdere lagen mee te maken krijgt, is een grotere mate van aandacht voor de opbouw van de digitale expertise binnen de reguliere opsporing en politie in brede zin van belang en is de focus op alleen cybercrimeteams (te) smal. Het algemene denkkader dient daarbij meer gericht te worden op het bredere fenomeen van 'criminaliteit en digitaliteit'.

Bijlage 1 Computercriminaliteit in registraties bij drie onderzochte politie-eenheden (politiecijfers)

Tabel B1 Geregistreerde computercriminaliteit bij politie-eenheid Noord-Holland

	aangiften	opgehelderde zaken	aantal verdachten
2015	220	25	25
2016	290	20	35
2017	470	5	20
2018	538	15	22

Tabel B2 Geregistreerde computercriminaliteit bij politie-eenheid Rotterdam

	aangiften	opgehelderde zaken	aantal verdachten
2015	210	15	20
2016	150	10	10
2017	225	10	25
2018	298	100	42

Tabel B3 Geregistreerde computercriminaliteit bij politie-eenheid Oost Nederland

	aangiften	opgehelderde zaken	aantal verdachten
2015	385	30	45
2016	215	20	25
2017	270	15	20
2018	140	20	50

Bijlage 2 Cybercrime artikelen Wetboek van strafrecht

Onder cybercrime als doelstelling in de Veiligheidsagenda hangen de volgende 10 wetsartikelen en zijn ook gekoppeld aan MK 90 (computercriminaliteit):

- Art. 138ab Sr: Computervredebreuk
- Art. 138b Sr: Opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmeren door daaraan gegevens aan te bieden of toe te zenden (Ddos-aanval)
- Art. 139c Sr: Met technisch hulpmiddel gegevens afluisteren; aftappen/opnemen gegevens
- Art. 139d Sr: Plaatsen opname of aftapapparatuur
- Art. 139e Sr: Hebben en gebruiken van door wederrechtelijk afluisteren, aftappen c.q. opnemen verkregen gegevens; openbaar maken gegevens
- Art. 161sexies Sr: Opzettelijke vernieling geautomatiseerd werk of werk voor telecommunicatie; telecommunicatiewerk verstoren
- Art. 161septies Sr: Culpose vernieling van enig geautomatiseerd werk of werk voor telecommunicatie; schuldvorm telecommunicatiewerk verstoren
- Art. 350a Sr: Aantasting/manipulatie computergegevens; data wijzigen/ onbruikbaar maken (het doleuze misdrijf)
- Art. 350b Sr: Aantasting/manipulatie computergegevens; schuldvorm van data wijzigen/onbruikbaar maken (het culpose misdrijf)
- Art. 317 Sr lid 2: Afpersing middels bedreiging gegevens middels een geautomatiseerd werk op te slaan, onbruikbaar of ontoegankelijk te maken.

De volgende tabel geeft een overzicht van de verdeling van strafbare feiten in cybercrime of gedigitaliseerde criminaliteit volgens de definitie uit het besluit van Ministerie van Justitie en Veiligheid in 2015.

Tabel B4 Strafbare feiten cybercrime en gedigitaliseerde criminaliteit, bijbehorende delictsoort, wetsartikel en code maatschappelijke klasse politie

Delict groep	Delict soort	Wetsartikel(-en)	Code maatschappelijke klasse politie
Cybercrime	Hacken	138ab Sr	F90
	Gegevensdiefstal	138ab en 139c Sr	F90
	Stoornis veroorzaken (Ddos-aanval)	138b, 161sexies en 161septies Sr	F90
	Gegevens vernielen	350a en 350b Sr	F90
	Defacing	350a en 350b Sr	F90
	Malware	139d en 16sexies Sr	F90
	Identiteitsfraude	231b	F617

Gedigitaliseerde criminaliteit	Phishing	326 en 225 Sr	F90/F638
	Skimming	232 Sr	F614
	Fraude via veiling- en verkoopwebsites	326 en 225 Sr	F636
	Voorschotfraude	326 Sr	F637
	Diefstal	310 Sr	A90
	Heling (van computergegevens)	139e Sr	A81
	Afpersing/Chantage	317, 318 en 285 Sr	A82
	Stalking/Belaging	285b Sr	F533
	Smaad/Laster	261, 262 en 268 Sr	F51
	Belediging	266 en 271 Sr	F51
	Discriminatie	137c-137g en 429 quater Sr	F50
	Bedreiging	285 Sr	F530
	Kinderpornografie	240b en 246 Sr	-
	Grooming	248e Sr	-

Bijlage 3 Bestrijding cybercrime, beleidsdoelstelling voor de politie

Tabel B5 Jaarschijven en regionale verdeling taakstelling VA voor politie-eenheden[46]

Doel: naar OM ingezonden verdachten (reguliere cyberzaken voor politie-eenheid)	2015	2016	2017	2018
Noord Nederland	15	17	20	27
Oost Nederland	26	28	34	46
Midden Nederland	18	20	24	33
Noord Holland	13	14	17	23
Amsterdam	20	22	27	36
Den Haag	23	25	30	41
Rotterdam	23	25	30	40
Zeeland West Brabant	13	14	17	23
Oost Brabant	12	13	16	21
Limburg	11	12	14	19
Subtotaal	175	190	230	310
Doel: naar OM ingezonden onderzoeken (complexe zaken)				
Landelijke/Regionale eenheid*	25	30	40	50
Totaal	**200**	**220**	**270**	**360**

Registratie:
De politie registreert bij de reguliere cyberzaken het aantal naar het OM ingezonden verdachten in BOSZ en dit wordt door het OM gevalideerd door deze in BOSZ (OM-module BOSZ) te beoordelen. Het OM registreert het aantal ingestroomde verdachten in GPS/Compas. De politie telt het aantal naar het OM ingezonden verdachten. Hierbij worden de onder instroom OM en instroom OM overig in BOSZ geregistreerde verdachten met MK F90 geteld. Voor een specificatie van de onder Cybercrime vallende wetsartikelen, zie bijlage 2. Het OM telt de instroom aan de hand van het aantal verdachten (parketnummers met wetsartikelen bijlage 2) vanuit GPS/Compas.

[46] Bron: Openbaar Ministerie en Politie (2015). Uitwerking Veiligheidsagenda 2015-2018, Beleidsdoelstellingen voor de politie, Versie 1.0, 18 maart 2015.

Complexe zaken:
Een complexe zaak wordt in overleg tussen het OM (Cybercrime OVJ) met de politie (leider onderzoek) vastgesteld. Een high tech crime zaak wordt door het OM (landelijke thema OVJ) in overleg met het Team High Tech Crime van politie vastgesteld.
Hierbij worden bij het OM ingeleverde dossiers geteld, die conform de beschrijving als 'complex' worden beschouwd (zie verder).

Omvangrijke afgeronde internationale rechtshulpverzoeken met meer dan 160 uur capaciteitsinzet worden als volwaardig cybercrime onderzoek beschouwd. Afhankelijk van de aard van de zaak worden zij als reguliere of complexe zaak meegeteld.

Onderscheid complex versus regulier

In de Veiligheidsagenda wordt onderscheid gemaakt tussen complexe en reguliere cybercrime zaken. Het Toewijzingskader Opsporing geeft handvaten om het onderscheid in praktijk te kunnen maken en zaken toe te kunnen wijzen. De in de onderstaande tabel licht blauw gemarkeerde categorieën worden als 'complexe' zaak aangemerkt. Er zijn voorbeelden opgenomen om een beter beeld te kunnen vormen. De voorbeelden zijn echter aan verandering onderhevig en de scheiding tussen complex en regulier is niet absoluut. Zo kan in een onderzoek naar aanleiding van een Ddos aanval al meteen een verdachte geïdentificeerd worden en de andere keer zijn er geen sporen meer beschikbaar, hetgeen de zaak complexer maakt.
High Tech Crime zaken vormen een subset van complexe zaken, namelijk de meest innovatieve, technisch complexe en ondermijnende vormen van cybercrime.

Tabel B6 Onderscheid kenmerken cybercrime naar VVC, HIC en ondermijning (op basis van voorbeelden)

	VVC	High Impact Crime	Ondermijning
Incidentgericht	Hacken in relationele sfeer, zoals misbruik van social media (Facebook, Twitter, Instagram) of e-mail account. Vaak worden er dan foto's of berichten geplaatst of gewijzigd uit naam van de aangever	Ddos-aanval op de website van een bedrijf/instelling of het hacken van een bedrijf/instelling (al dan niet met afpersing)	Aanvallen op de vitale infrastructuur
Probleemgericht	Gebruik van Remote Access Trojans (RAT) (toegankelijk hackersprogramma)	Ransom- en cryptoware (voor gijzeling van pc's)	Fraude met online bankieren door middel van banking malware
Thematisch/ programmatisch	Beheer van een RAT-infrastructuur ten behoeve van RAT-gebruikers	Botnets die ingezet worden voor uiteenlopende vormen van cybercrime	Bad hosting

Bijlage 4 Cybercrime cijfers bij het Openbaar Ministerie

Cijfers in- en uitstroom cybercrimezaken Openbaar Ministerie 2015-2018, totaal en verdeeld naar politie-eenheden Noord-Holland, Oost Nederland en Rotterdam (cijfers ontleend aan Veiligheidsagenda-monitor)

Tabel B7 Geregistreerde cybercrime bij het Openbaar Ministerie 2015-2018 (totaal en naar de 3 onderzochte politie-eenheden)

	2015				2016				2017				2018			
	PE NHL	PE ONL	PE ROT	OM Totaal	PE NHL	PE ONL	PE ROT	OM Totaal	PE NHL	PE ONL	PE ROT	OM Totaal	PE NHL	PE ONL	PE ROT	OM Totaal
Instroom	10	8	19	137	17	13	33	184	15	41	24	231	22	36	26	311
- Adm. beëindigd/ overig				1				1	2		1	8				3
- Onvoorwaardelijk Sepot	4	2	3	38	8	2	8	52	5	6	8	80	6	17	14	140
technisch	3	1	2	18	5	1	8	36		3	2	39	2	8	10	88
beleid	1	1	1	18	3	1		13	3	3	1	28	4	9	2	43
administratief				2				3	2		5	13	0	0	2	9
- Voorwaardelijk Sepot	2	2	2	15		1		6	3	5	2	21	1	2	4	16
- OM transactie/ OMSB	2	1	2	34		2	2	11	2	1		13	5	2		20
- Voegen									1			2				2
OM-afdoeningen Totaal	8	5	7	88	8	5	10	70	11	12	10	124	12	21	18	181
- Schuldigverklaring	1	4	4	40	3	1	6	45	5	8	9	60	7	12	12	103
- Vrijspraak		2	2	10	1			7		2		6	0	4	1	16
- Overig				5			1	2		1		5	2	0		4
ZM-afdoeningen Totaal	1	6	6	55	4	1	7	54	5	11	9	71	9	16	13	123
Uitstroom in 1e aanleg	9	11	13	143	12	6	17	124	16	23	19	195	21	37	31	304

Bijlage 5 Overzicht sleutelpersonen onderzoek cybercrime politie

Eenheid Noord Holland

- teamleider cyberteam
- projectleider aanpak cybercrime politie
- teamchef Generieke Opsporing
- tactisch analist DRIO
- leader intake en screening Cyber Center
- OvJ cybercrime OM Haarlem

Eenheid Oost Nederland

- teamchef Digitale Opsporing
- analisten DRIO
- teamchef DR
- tactisch rechercheur DR
- OvJ cybercrime OM Arnhem
- beleidsadviseur intelligence/criminologie OM Arnhem

Eenheid Rotterdam

- teamleider cybercrimeteam
- projectleider cybercrimeteam (DRR)
- chef team cybercrime
- coördinator tactische recherche
- analist DRIO/cyber
- casescreener cyberteam
- OvJ cybercrime OM Rotterdam
- parketsecretaris cybercrime OM Rotterdam

Landelijk

- hoofd Operatiën eenheidsleiding Midden Nederland, voorzitter PIAC
- senior coördinerend adviseur Korpsleiding, Directie Operatiën
- landelijk programmamanager Cybercrime politie
- medewerker Programma Digitalisering en Cybercrime, eenheid Amsterdam
- analisten DLIO
- case agent Team High Tech Crime
- OvJ OM Den Haag

Bijlage 6 Lijst met gebruikte afkortingen

BOSZ	programma Betere Opsporing door Sturing op Zaken
BVH	Basisvoorziening Handhaving
CEO-fraude	fraude bij Chief Executive Officer
CSBN	Cybersecuritybeeld Nederland
CSR	Cyber Security Raad
DLIO	Dienst Landelijke Informatieorganisatie
DLR	Dienst Landelijke Recherche
DR	Districtsrecherche
DRIO	Dienst Regionale Informatieorganisatie
DRR	Dienst Regionale Recherche
ECTF	Electronic Crimes Taskforce
Finec	Financieel economische criminaliteit
I&S	Intake en Service
ICT	Informatie- en Communicatietechnologie
KMAR	Koninklijke Marechaussee
KPI	kritieke prestatie-indicatoren
LE	Landelijke Eenheid politie
LMIO	Landelijk Meldpunt Internetoplichting
LOCO	Landelijk Operationeel CyberOverleg
MKB	Midden- en Kleinbedrijf
NCB	Nationaal Cyber Beeld
NCSC	Nationaal Cyber Security Centrum
NDB	Nationaal Dreigingsbeeld
OC	Operationeel coördinator
OCP	Operationeel Coördinatie Knooppunt
OM	Openbaar Ministerie
OSINT	Open Source Intelligence
PAC	Programma Aanpak Cybercrime
PaG	Parket Generaal
PIAC	Programma Intensivering Aanpak Cybercrime
RSC	Regionaal Service Centrum
TBKK	Team ter Bestrijding van Kinderpornografie en Kindersekstoerisme
TDO	Team Digitale Opsporing
THTC	landelijk Team High Tech Crime politie
VVCC	Veel Voorkomende Cyber Crime
VM	Veiligheidsmonitor
ZSM	Aanpak Zo Spoedig, Selectief, Slim, Samen en Simpel mogelijk

Literatuur

Bernaards, F., Monsma, E., & Zin, P. (2012). High tech crime: Criminaliteitsbeeld-analyse 2012. Woerden: KLPD.

Bloem, B., A. Harteveld en K. Schuppers (2017), Cybercrime Eenheidsbeelden, Plan van aanpak. DLIO, Driebergen.

Bloem, B. en A. Harteveld (2018), Aantal gedupeerden bij cybercrime, notitie DLIO, Driebergen.

Boekhoorn, P. en J. Tolsma (2015). De aangifte van delicten bij de 'multichannelstrategie' van de politie. Nijmegen: BBSO, Bureau Boekhoorn Sociaalwetenschappelijk Onderzoek.

Boerman, Frank, Martin Grapendaal, Fred Nieuwenhuis en Ewout Stoffers (2017). Nationaal Dreigingsbeeld georganiseerde criminaliteit 2017, Politie Nederland

Bout, B. (2017). Het opsporingsproces van cybercrime en gedigitaliseerde criminaliteit in Gelderland-Midden. Van melding tot de districtsrecherche.

Campman, I., Dedert, P., Hesseling, R., Huijskes, P. J., Kegel, D., Tijsmans, N., et al. (2012). Criminaliteit in een gedigitaliseerde samenleving. Amsterdam: Nationale Politie

CBS (2019). Digitale veiligheid en criminaliteit 2018. Centraal Bureau voor de Statistiek, Den Haag/Heerlen/Bonaire, 2019.

Collee, A., Schniedermeier, S., & Kreling, T. (2014). Landelijk Werkingsdocument Opsporing. Politie Oost-Nederland: Politie Nederland.

Cuyper, R.H. de en G. Weijters (2016). Cybercrime in cijfers: Een verkenning van de mogelijkheden om cybercrime op te nemen in de Nationale Veiligheidsindices. Memorandum 2016-1. WODC, Den Haag.

Domenie, M., Leukfeldt, E., Toutenhoofd-Visser, M., & Stol, W. (2009). Werkaanbod cybercrime bij de politie. Leeuwarden: Lectoraat Cybersafety, Noordelijke Hogeschool Leeuwarden.

Domenie, M., Leukfeldt, E., Wilsem, J. v., Jansen, J., & Stol, W. (2013). Slachtofferschap in een gedigitaliseerde samenleving. Den Haag: Boom Lemma uitgevers.

Erp, Judith van, Wouter Stol en Johan van Wilsem (2013). Criminaliteit en criminologie in een gedigitaliseerde wereld. In: Tijdschrift voor Criminologie 2013 (55) 4, p. 327-341.

Helsloot, Ira en Jelle Groenendaal (2014). Naar meer inzicht in de politiële netwerkpraktijk in de casus cybercrime, zeehavens en veiligheidshuizen. Working paper BSK14-01. Radboud University Nijmegen

Huisman, S., Princen, M., Klerks, P. & Kop, N. (2016). Handelen naar waarheid. Sterkte- en zwakteanalyse van de opsporing. Amsterdam.

Hulst, R.C. van der, Neve, R.J.M (2008). High-tech crime, soorten criminaliteit en hun daders. Een literatuurinventarisatie. WODC, Den Haag, Boom Juridische uitgevers, Onderzoek en beleid 264

Inspectie Veiligheid en Justitie (2015). Aanpak van internetoplichting door de politie. Inspectieonderzoek naar een vorm van cybercrime. Den Haag: Ministerie van Veiligheid en Justitie.

Jansen, J., S. Kloppenburg, W. Stol, S. Veenstra & R. Zuurveen (2014). MKB en cybercrime. Slachtofferschap onder het Nederlandse Midden- en Kleinbedrijf in een gedigitaliseerde samenleving. Leeuwarden: NHL Hogeschool, Lectoraat Cybersafety.

Kerstens, J. & Veenstra, S. (2017). Digitaal vaardige jongeren inzetten bij politiewerk: een pilot met Teenage Crime Fighters. Tijdschrift voor de Politie, 79(9), 10-17.

Kimpe, S. de, Moor, L., Vlek, F., & van Reenen, P. (2012). Professionalisering en socialisatie. Cahiers Politiestudies.

Kloosterman, R. (2015). Slachtofferschap cybercrime en internetgebruik. Den Haag: Centraal Bureau voor de Statistiek.

Kouwehoven, R., Morée, R., & Beers, P. (2010). Het districtelijk opsporingsproces; de black box geopend. Apeldoorn: Politie & Wetenschap.

Laan, A.M. van der en H. Goudriaan (2016). Monitor Jeugdcriminaliteit. Ontwikkelingen in de jeugdcriminaliteit 1997 tot 2015. Cahier 2016-1. WODC/CBS.

Laan, A.M. van der, M.G.C.J. Beerthuizen & G. Weijters (2016). Jeugdige daders van online-criminaliteit. Cahier Politiestudies 2016-4, nr. 41, pp. 145-168.

Laan, A.M. van der en M.G.C.J. Beerthuizen (2018). Monitor Jeugdcriminaliteit 2017. Ontwikkelingen in de geregistreerde jeugdcriminaliteit in de jaren 2000 tot 2017, Cahier 2018-1, WODC/CBS.

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

Leukfeldt, E.R., Veenstra, S., Domenie, M.M.L., & Stol, W.P. (2012). De strafrechtketen in een gedigitaliseerde samenleving. Een onderzoek naar de strafrechtelijke afhandeling van cybercrime. Leeuwarden: Lectoraat Cybersafety.

Leukfeldt, E.R., Kentgens, A., Frans, B., Toutenhoofd, M., Stol, W.Ph., & Stamhuis, E. (2012). Alledaags politiewerk in een gedigitaliseerde wereld: Handreiking voor delicten met een digitale component. Den Haag: Boom Lemma uitgevers.

Leukfeldt, R., A. Kentgens, E. Prins en W. Stol (2015). Alledaags politiewerk in een gedigitaliseerde wereld, Handreiking voor de intake van delicten met een digitale component (2015). Lectoraat Cybersafety (NHL Hogeschool/Politieacademie) Open Universiteit (tweede versie).

Liedenbaum, C., & Kruijsen, M. (2008). Opsporing onder druk. (Politiewetenschap; No. 41). Den Haag: SDU Uitgevers.

Ministerie van Veiligheid en Justitie (2014). Veiligheidsagenda 2015-2018. Bijlage bij Tweede Kamerstukken, Vergaderjaar 2014-2015, 28684 nr. 412.

Morée, R., Landman, W., & Bos, A. (2014). Verschijningsvormen en overwegingen van specialisatie en despecialisatie binnen de Nederlandse politieorganisatie. Politie & Wetenschap. Reed Business, Amsterdam.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2017), Cybersecuritybeeld Nederland CSBN 2017, NCTV, 2017.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2018), Cybersecuritybeeld Nederland CSBN 2018, NCTV, 2018.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2019), Cybersecuritybeeld Nederland CSBN 2019, NCTV, 2019.

Nationale Politie, Cybercrime strategie 2020, Voor een veiliger Nederland, ook in het digitale domein, oktober 2016.

Nationale Politie, Plan van aanpak intensivering aanpak cybercrime (PIAC), oktober 2016. Openbaar Ministerie en Politie (2015). Uitwerking Veiligheidsagenda 2015-2018, Beleidsdoelstellingen voor de politie. Notitie Versie 1.0, 18 maart 2015.

Oerlemans, J.J. (2017). Investigating cybercrime (dissertatie). E.M. Meijers Instituut en Graduate School, Universiteit Leiden.

Plas, A. (2015). Cybercrime aangepakt in de basis. Een onderzoek naar het opsporingsproces van cybercrime gerelateerde zaken binnen het basisteam Ede van politie Oost-Nederland. Leeuwarden.

Politie (2012). Inrichtingsplan Nationale Politie.

Politie, Eenheid Oost-Nederland (2019). Veranderingen in criminaliteit. Een verkenning van de oorzaken in Oost-Nederland. Apeldoorn.

Rokven, J.J., Weijters, G., Van der Laan, A.M. (2017). Jeugddelinquentie in de virtuele wereld: Een nieuw type daders of nieuwe mogelijkheden voor traditionele daders. Den Haag: WODC, cahier 2017-2.

Schuppers, K., Rombouts, N., Zinn, P. en Praamstra, H. (2016). Cybercrime en gedigitaliseerde criminaliteit. Nationaal dreigingsbeeld 2017. Den Haag: Landelijke Politie.

Smit, P.R., Ghauharali, R., Veen, H.C.J. van der, Willemsen, F., Steur, J., Velde, R.A. te, Vorst, T. van der, Bongers, F., Kabki, A. (medew.), Zaitch, D. (medew.) (2018). Tasten in het duister. Een verkenning naar bronnen en methoden om de aard en omvang van de criminaliteit te meten. Deel 1: Hoofdrapport. WODC. Cahiers 2018-21a

Stol, W. Ph., E.R. Leukfeldt en H. Klap (2012). Cybercrime en politie; een schets van de Nederlandse situatie anno 2012. In: Justitiële verkenningen, jrg. 38, nr. 1, 2012 Veiligheid in cyberspace, p.25-39

Stol, W.Ph. & Strikwerda, L. (2018). Online vergaren van informatie voor opsporingsonderzoek: Een beknopte evaluatie van voorgestelde wetgeving. Tijdschrift voor Veiligheid (themanummer).

Stol, W.Ph. (2018). Politiewerk is … werken in een digitale samenleving. Tijdschrift voor de Politie, 80(5), 22-25.

Struiksma, N., de Vey Mestdagh, C., & Winter, H. (2012). De organisatie van de opsporing van cybercrime door de Nederlandse politie. Politie & Wetenschap, Apeldoorn: Reed Business, Amsterdam.

Tollenaar, N., J. Rokven, D. Macro, M. Beerthuizen en A.M. van der Laan (2019). Predictieve textmining in politieregistraties. Cyber- en gedigitaliseerde criminaliteit. Cahier 2019-2. WODC.

Toutenhoofd-Visser, M., Veenstra, S., Domenie, M., Leukfeldt, E., & Stol, W. (2009). Politie en Cybercrime Intake en eerste opvolging. Noordelijke Hogeschool Leeuwarden, Lectoraat Cybersafety.

TRIO opsporing. (2014). Landelijk Werkingsdocument Opsporing. Politie Nederland.

Valkengoed, T.M. van (2017). Competentieonderzoek cybercrimeopsporing. Managementrapportage bachelor thesis. Amsterdam: Politie-eenheid Amsterdam

Veenstra, S., R. Zuurveen en W.Ph. Stol (2015). Cybercrime onder bedrijven. Een onderzoek naar slachtofferschap van cybercrime onder het Midden- en Kleinbedrijf en Zelfstandigen zonder Personeel in Nederland. Leeuwarden: Lectoraat Cybersafety.

Vermeulen, P. en A. de Vries (2018). Eerste hulp bij cyberincidenten? Update het meldproces! In: Website voor de Politie, december 2018

Weijer, S., & Bernasco, W. (2016). Aangifte- en meldingsbereidheid: Trends en determinanten. Den Haag: Nederlands Studiecentrum Criminaliteit en Rechtshandhaving.

Wijn, R., van den Berg, H., Wetzer, I., & Broekman, C. (2016). Supertargets: Verkenning naar voorspellende en verklarende factoren voor slachtofferschap van cybercriminaliteit. TNO.

Zebel, S., de Vries, P. W., Giebels, E., Kuttschreuter, M., & Stol, W. (2014). Jeugdige daders van cybercrime in Nederland: een empirische verkenning. Enschede: Universiteit Twente.