Cybercrime strategie 2020

Voor een veiliger Nederland, ook in het digitale domein

Auteurs: Rob van Bree, Richard Nijeboer,

Godfried Klerkx, Lourens Witteveen en Eileen Monsma

Status: Definitief

Versie 1.0

10-10-2016

«waakzaam en dienstbaar»

POLITIE

‘Het is niet de sterkste soort die overleeft …

Het is degene die zich het beste kan aanpassen.’

(Charles Darwin, 1859)

1. Inleiding

In enkele decennia heeft de opkomst van informatie- en communicatietechnologie (ICT) de wereld veranderd in een netwerksamenleving. De toonaangevende internet-infrastructuur en de uitzonderlijk hoge online gebruikersdichtheid illustreren het adaptief vermogen van Nederland. Dit vraagt om een veilig digitaal domein. Nederland wil leidend zijn op het gebied van Cybersecurity.

> ***Cybersecurity*** is het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan.
>
> De schade aan ICT kan bestaan uit aantasting van de betrouwbaarheid van ICT, beperking van de beschikbaarheid en schending van de vertrouwelijkheid en/of de integriteit van in ICT opgeslagen informatie.
>
> (Nationale Cybersecurity Strategie 2)

De belangrijkste dreiging voor cybersecurity is cybercrime. Er zijn veel publieke en private partijen die een rol hebben in de bestrijding van dit fenomeen. Ook de politie draagt vanuit haar taakstelling en bevoegdheden verantwoordelijkheid voor een bijdrage aan de aanpak en bestrijding van cybercrime[1]. De snelle ontwikkelingen op dit gebied stellen het adaptief vermogen van de organisatie op de proef.

De huidige situatie is dat de politie een achterstand heeft in de aanpak van cybercrime. In de regionale eenheden wordt hier nauwelijks capaciteit op ingezet, het ontbeert de politie aan een informatiepositie op dit thema en de minimale resultaatdoelstellingen worden niet gehaald. Gezien de populariteit van Nederlandse infrastructuur onder cybercriminelen wordt Nederland hier ook internationaal op aangekeken. Het Team High Tech Crime is in deze situatie gedwongen onderzoeken en rechtshulpverzoeken op te pakken die in de regionale eenheden blijven liggen en verliest haar positie aan de top van high tech crime bestrijding. De meest zichtbare tekortkoming is dat de intake van cybercrime niet op orde is waardoor slachtoffers geen gehoor vinden bij de politie[2].

De politie zal in beweging moeten komen om een inhaalslag te maken in de kanteling naar een nieuwe werkelijkheid. Welke visie heeft de politie op de eigen bijdrage aan de bestrijding en voorkoming van cybercrime en hoe geeft de organisatie hier komende jaren uitvoering aan? Op deze vragen beoogt dit document antwoord te geven. Alhoewel er uiteindelijk ook een lange termijn strategie nodig is, concentreert dit document zich op de noodzakelijke beweging van de organisatie op korte termijn. Dit wordt gezien als een onderdeel van en tevens katalysator voor de grotere beweging die nodig is voor een effectieve aanpak van alle gedigitaliseerde criminaliteit en cybercrime evenals het benutten van de kansen die digitalisering biedt voor de uitvoering van alle politietaken. Met andere woorden: voor een toekomstbestendige politie. Voor een veiliger Nederland, ook in het digitale domein.

[1] De minimaal te behalen resultaten (aantal opsporingsonderzoeken) zijn vastgelegd in de veiligheidsagenda 2015-2018.
[2] Deze knelpunten zijn ook de EU GENVAL evaluatiecommissie cybercrime opgevallen. De aanbevelingen zijn in 2015 vastgesteld in een rapport. Op 24 december 2016 dient Nederland over de opvolging hiervan te rapporteren aan de EU voorzitter.

Deze strategie is in lijn met de uitgangspunten in de Europese Cybersecurity strategie (2013) en de Nederlandse Nationale Cybersecurity Strategie 2 (2014). Het bouwt tevens voort op de inzichten en aanbevelingen uit eerdere interne beleidsdocumenten van de politie, zoals het beleidskader Digitalisering en Cybercrime (2013) en het beleidskader cybercrime (2015).

2. Ontwikkelingen

Afhankelijkheid van ICT

Onze sociale interactie, economie, vrijheid en ons dagelijks leven zijn volledig afhankelijk van ICT. Nederlanders zijn massaal online gegaan.

In 2014 maakte 90% van de Nederlanders (bijna) dagelijks gebruik van internet. 74% van de internetgebruikers deed dit via mobiele apparatuur (CBS, 2015). Volgens 'Connected Consumer-onderzoek' van Google hadden Nederlanders in 2014 al gemiddeld 3,6 apparaten met een scherm in huis. Met 51% bleek Nederland zelfs de grootste tablet-penetratie ter wereld te hebben. 65% van de Nederlanders koopt minimaal een keer per maand via internet.

De Amsterdam Internet-Exchange (AMS-IX) is een van de grootste internetknooppunten ter wereld. In 2014 steeg het volume van het internetverkeer via de AMS-IX met 25% ten opzichte van het jaar ervoor. Een kwart van de Nederlandse economische groei van de afgelopen tien jaar komt voor rekening van ICT (circa 22 miljard euro) (CBS, 2015).

Dit is nog maar het begin van de zogenaamde digitale revolutie. De afhankelijkheid van ICT zal komende jaren verder toenemen. Denk bijvoorbeeld aan de impact van robotica, zelfrijdende auto's en 3D-printers. De verwachting is dat de trend richting een hyper connectieve wereld onverminderd doorzet: alles en iedereen wordt (draadloos) met elkaar verbonden, ook mens en apparatuur.

Dreigingen

De ontwikkeling van ICT biedt kansen, maar brengt ook risico's met zich mee. Het Cyber Security Beeld Nederland 2016 schetst een zorgelijk beeld van de veiligheidssituatie in het digitale domein. Waar in 2015 sprake was van het doorzetten van zorgelijke trends, kan nu gesproken worden van toenemende en reële cyberdreigingen. Deze dreigingen zijn gericht op diefstal van geld en kostbare commerciële informatie maar richten zich ook op de ondermijning van politiek en bestuur en het verstoren of saboteren van diensten en processen waar overheden en de samenleving van afhankelijk zijn voor hun functioneren.

> Onder ***cybercrime*** verstaan we delicten die middels ICT en gericht op ICT als doelwit gepleegd worden.
>
> Overige delicten waarbij ICT in meer of mindere mate een rol speelt noemen we ***gedigitaliseerde criminaliteit.***
>
> (Veiligheidsagenda 2015-2018)

In 2015 werd 18 % van de Nederlanders slachtoffer van cybercrime (CBS, 2016). Het aantal internetgebruikers dat aangeeft geen toegang tot een online dienst gehad te hebben door een cyber-aanval ligt in Nederland met 43% relatief hoger dan in andere landen (Eurostats, 2015). Bijna 30% van het MKB en de ZZP'ers is slachtoffer geweest van cybercrime (Lectoraat Cybersafety, 2014). Het waardeverlies voor de grootste Nederlandse bedrijven en overheid wordt op 10 miljard euro per jaar geschat (Deloitte, 2016).

Uit onderzoek van het Centraal Bureau voor Statistiek blijkt dat de politie in 2015 5% minder misdrijven registreerde dan het jaar ervoor. Van de cybercrime slachtoffers blijkt volgens het CBS slechts 2,2% aangifte te doen bij de politie. De aangiftebereidheid is hiermee een stuk lager dan bij andere vormen van criminaliteit**.** De aangiftebereidheid in de vitale sector lijkt veel hoger (88%). Wel blijkt 41% van deze aangevers sterk ontevreden te zijn over de afhandeling van de aangifte door de politie (van Wilsem, Cybercrime in de vitale sector en de relatie met de politie (CVIP), eerste bevindingen, maart 2016).

Cybercriminelen hebben zich ontwikkeld tot zeer geavanceerde actoren wier capaciteiten in een aantal gevallen gelijk staan met die van staten. Deze capaciteiten worden bovendien verkocht of verspreid waardoor kennis, kunde en tools om geavanceerde of grootschalige digitale aanvallen uit te voeren in handen komen van technisch minder vaardige partijen zoals cybervandalen en scriptkiddies. Cybercrime is daarmee zowel kwantitatief als kwalitatief een groeiend probleem voor de Nederlandse samenleving.

Nederland heeft te maken met specifieke uitwassen van het internationale probleem cybercrime. Onze toonaangevende internetconnectiviteit, grote bedrijven, welvaart en de populariteit van internetdiensten maken cybercrime op Nederlandse doelen zeer lucratief en interessant voor criminelen.

Vijf jongeren aangehouden voor ddos-aanvallen op Ziggo

Gepubliceerd: 07 oktober 2015 09:36
Laatste update: 07 oktober 2015 13:24

De politie heeft vijf jongeren aangehouden die betrokken zouden zijn geweest bij de ddos-aanvallen die internetverbindingen van Ziggo in augustus meermaals platlegden.

Het gaat om vier minderjarigen en één man van 21 jaar oud, meldt de politie woensdag. Ze woonden verspreid over het land, in Berkelland, Lochem, Den Helder en Vinkeveen.

De verdachten zijn dinsdag verhoord, maar zijn inmiddels weer vrij in afwachting van verdere onderzoeksresultaten. In de ouderlijk woningen van de jongeren zijn verschillende soorten elektronica in beslag genomen.

Bij de ddos-aanvallen werd een grote hoeveelheid internetverkeer naar de servers van Ziggo gestuurd, waardoor deze onder hevige druk kwamen te staan. Bij de aanval kwamen miljoenen mensen zonder internet te zitten. Twee ...onden achter elkaar werd de provider getroffen.

Nederlandse hosting providers zijn ongekend populair voor criminele activiteiten. Het aantal IP-adressen waar politie en OM op basis van buitenlandse rechtshulpverzoeken op moeten acteren nam in 2015 (383) met 79% toe ten opzichte van 2014 (214).

Het gebruik van ransomware door criminelen is het afgelopen jaar gemeengoed geworden. Besmettingen zijn aan de orde van de dag en raken de gehele samenleving. Waar in het verleden dezelfde prijs betaald moest worden per besmetting, wordt nu een prijs bepaald aan de hand van het type getroffen organisatie.

Ransom- en cryptoware is malware (malafide software) waarmee ICT-systemen ontoegankelijk worden gemaakt. Met cryptoware worden daarnaast de opgeslagen gegevens (mappen en/of specifieke bestanden) versleuteld. Besmetting vindt meestal plaats doordat mensen verleid worden om op een link of bijlage in een mail te klikken. De gijzeling duurt voort totdat er losgeld betaald wordt of het slachtoffer het virus zelf van de computer heeft kunnen (laten) verwijderen. De malware wordt tevens gebruikt om inloggegevens van mailaccounts en het adresboek van slachtoffers te stelen om nog meer slachtoffers te kunnen maken. Zo verspreidt het zich letterlijk als een virus over het land. In Nederland zijn talloze burgers, gemeentes, bedrijven en instellingen hier afgelopen jaren slachtoffer van geworden. De financiële schade (o.a. door het platleggen van werkprocessen), imagoschade en emotionele schade (b.v. door het verliezen van baby- of vakantiefoto's) maakt dat dergelijke criminaliteit een enorme impact heeft

(Bron: Team High Tech Crime).

Naast het grote volume aan ransom- en cryptoware aanvallen op willekeurige doelwitten vinden er steeds meer gerichte aanvallen op zorgvuldig geselecteerde systemen plaats om een zo hoog mogelijk bedrag te kunnen vragen. Hier zijn vooral ziekenhuizen het slachtoffer van geworden. In het buitenland heeft dit al tot noodtoestanden geleid. Zo maakte een Duits ziekenhuis in Neuss in februari 2016 bekend dat operaties niet door konden gaan doordat patiëntgegevens versleuteld waren en computers van de intensive care waren uitgeschakeld. Ook e-mailcommunicatie werd opgeschort. In diezelfde maand moest ook de dienstverlening in een ziekenhuis in Los Angeles onderbroken worden. Hier waren CT-scanners, laboratoriumrobots en medicijnverstrekkende machines gesaboteerd. Dit ziekenhuis besloot het losgeld, 40 bitcoins (waarde ca. 17.000 dollar), te betalen. Een aantal Nederlandse ziekenhuizen die zich bij de politie gemeld hebben om aangifte te doen van cryptoware zijn bij de balie weggestuurd met de boodschap dat de politie daar niets in kan betekenen.

(Bron: NCSC).

Cybercrime vormt een toenemende zorg voor burgers en het bedrijfsleven. Uit onderzoek blijkt dat, naast macro-economische omstandigheden, cybercrime door bankiers en andere betrokkenen beschouwd wordt als het belangrijkste risico voor de bankensector (CSFI en PwC, 2015).

De vermenging van cybercrime met traditionele georganiseerde misdaad en terrorisme levert in de toekomst mogelijk een nog veel ernstiger dreigingsbeeld op. De AIVD waarschuwt in het jaarverslag 2015 voor meer cyber-aanvallen door centraal aangestuurde jihadistische hackersgroeperingen.

Uitdagingen[3]

Een grote uitdaging in de aanpak van cybercrime is de grenzeloosheid van het digitale domein. Er is sprake van een internationaal speelveld met talloze stakeholders en uiteenlopende (inter)nationale wetgeving.

Door een daling van smartphone prijzen en de groei van draadloze netwerken zal op korte termijn een nog veel groter deel van de wereldbevolking aansluiting krijgen op het internet. Dit zou tot een verschuiving van doelwitlanden kunnen leiden, maar waarschijnlijk vooral tot nieuwe cybercrime dadergroepen. Daarnaast worden steeds meer objecten en omgevingen aangesloten op het internet. Dit 'Internet of Things' levert nieuwe kwetsbaarheden op, ook van apparaten waaraan we ons leven toevertrouwen, zoals auto's en pacemakers.

In 2015 maakten security onderzoekers (Miller en Valasek) bekend dat ze in staat waren een 2014 Jeep Cherokee te hacken en op afstand via het 3G-netwerk aan te sturen. Ze waren onder andere in staat om de rem te blokkeren en het stuur over te nemen (http://illmatics.com/Remote%20Car%20Hacking.pdf).

De grenzen tussen cybercrime en andere vormen van criminaliteit zullen verder vervagen, want alle criminaliteit digitaliseert. Het wordt steeds moeilijker om strafbare feiten te plegen zonder sporen achter de laten. Tegelijkertijd wordt door de vluchtigheid van data, de ontwikkeling van versleuteling en andere anonimiseringstechnieken het veiligstellen van bewijs een steeds grotere uitdaging. Het wetsvoorstel Computercriminaliteit III beoogt daarom het op afstand binnendringen van geautomatiseerde werken mogelijk te maken.

De ernst en omvang van cybercrime zal in korte tijd verder toenemen. Gezien de taakstelling en bevoegdheden is hier ook een belangrijke rol weggelegd voor de politie.

3. Visie

***Nederlandse visie op cybersecurity**:* Nederland zet samen met zijn internationale partners in op een veilig en open cyberdomein, waarin de kansen die digitalisering onze samenleving biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd.

(Nationale Cybersecurity Strategie 2)

Het doel van de politie is vanuit haar taakstelling bij te dragen aan een veiliger Nederland en daarmee ook aan cybersecurity. Traditionele criminaliteit neemt af en cybercrime neemt toe. Aangezien de maatschappij en het criminaliteitsbeeld verandert, verschuift ook de focus van de politie.

<< Waakzaam en dienstbaar >> Voor een veiliger Nederland, ook in het digitale domein.

[3] Dit is geen limitatieve opsomming. Voor een uitgebreider overzicht van specifiek de technologische uitdagingen zie de Technologieradar Cybercrime (LE, DLOS, ATOE).

Dit hoger doel vormt het bestaansrecht van de organisatie. Vanuit dit hoger doel kan een gewaagd doel gesteld worden met betrekking tot cybercrime. Dit is een beeld van wat de politie binnen enkele jaren met partners bereikt wil hebben:

In 2020 is de weerbaarheid van de Nederlandse samenleving tegen cybercrime verhoogd. Door een kleinere slagingskans, hogere kosten en een hogere pakkans is het business model voor cybercrime gericht op, vanuit of via Nederland niet meer zo interessant.

Op weg hiernaar toe:

- vormt de politie met relevante stakeholders een vooruitstrevende coalitie voor de bestrijding van cybercrime
- is de politie zelf ook weerbaar tegen cyberaanvallen

Een strategie gericht op het verhogen van de digitale weerbaarheid van de politie zal in een afzonderlijk document worden uitgewerkt door de directie IV. De intensivering van de aanpak van cybercrime kan leiden tot meer tegenreacties van cybercriminelen in de vorm van digitale aanvallen op politiesystemen. De inspanningen zullen dan ook op elkaar afgestemd worden.

Uitgangspunten

- Verhogen van de weerbaarheid en het vertrouwen in het digitale domein is cruciaal voor de Nederlandse economie.

- Cybersecurity dient in de eerste plaats gebaseerd te zijn op de rechten van burgers, zoals privacy en vrijheid. Echter kunnen die rechten niet gewaarborgd worden als er niet zorggedragen wordt voor de veiligheid.

- ICT-dienstverleners hebben een zorgplicht en van ICT-gebruikers mag een zekere basis-cyberhygiëne worden verwacht. Wel heeft de overheid een bijzondere rol ten opzichte van zogenaamde ‘zwakkeren in de (informatie)samenleving’, zoals ouderen. Voorkomen dient te worden dat deze doelgroepen niet meer durven of kunnen participeren in de digitale maatschappij en hierdoor (verder) geïsoleerd en/of op achterstand raken.

- Uiteenlopende partijen hebben een rol in de aanpak van cybercrime. Effectieve bestrijding is alleen mogelijk als alle partijen hun verantwoordelijkheid nemen en elkaar daar op aanspreken. De politie richt zich in de eerste plaats op activiteiten waar de politie bijzondere bevoegdheden toe heeft. Ook daarbij is samenwerking met burgers, publieke en private partners in binnen- en buitenland essentieel.

- De strafrechtelijke aanpak van cybercrime is niet de oplossing voor het probleem. Opsporing en vervolging zal niet leiden tot het beheersbaar houden van deze vorm van criminaliteit. Wel is het een middel om de rechtsstaat te waarborgen, straffeloosheid in het digitale domein te voorkomen en specifieke criminele activiteiten te doen stoppen. Het verhogen van de pakkans helpt om Nederland minder aantrekkelijk te maken voor cybercriminelen. De politie levert een bijdrage aan het verhogen van de weerbaarheid van de samenleving door naast opsporen ook aandacht te besteden aan preventie, verstoren, signaleren en adviseren. Opsporing versterkt het zicht op de modus operandi van cybercriminelen. Door de kennis over (potentiële) dreigingen te benutten en zo breed mogelijk beschikbaar te stellen kunnen beschermende maatregelen getroffen worden. Dit resulteert in hogere kosten en een lagere slagingskans voor cybercriminelen.

- Het werkaanbod op het gebied van cybercrime zal altijd groter blijven dan de beschikbare capaciteit en middelen. Er moeten, net als in andere aandachtsgebieden, keuzes gemaakt worden. Dit geldt ook voor het totale werkaanbod van de politie. Het prioriteren van de aanpak van cybercrime betekent minder aandacht voor de aanpak van andere vormen van criminaliteit.

4. Strategie

Om het gewaagde doel (verhoogde weerbaarheid van de Nederlandse samenleving tegen cybercrime in 2020) in korte tijd dichtbij te brengen gaat de politie met relevante stakeholders een vooruitstrevende coalitie voor de bestrijding van cybercrime vormen[4]. Om intern de randvoorwaarden hiervoor in te vullen zet de politie op korte termijn in op zes speerpunten. Die inzet is gericht op het hieronder per speerpunt beschreven beeld van waar de organisatie in 2020 zou moeten staan. Hiermee wordt nog geen eindplaatje voor de bijdrage van de politie aan de bestrijding van cybercrime geschetst. Het gaat om een tussenfase waarin een basis voor de toekomst gelegd wordt door een aantal noodzakelijke maatregelen te nemen.

Bewustwording

In alle lagen van de organisatie zijn politiemedewerkers en leidinggevenden zich bewust van de dreiging die van cybercrime uitgaat, de impact van slachtofferschap en de verantwoordelijkheid die de politie in dit aandachtsgebied heeft. De politie draagt bij aan de bewustwording en daarmee de weerbaarheid van de maatschappij door te signaleren en adviseren. Hierbij smelten signalen en adviezen van de verschillende regionale eenheden en het Team High Tech Crime samen in voor het publiek herkenbare en betrouwbare berichten. Er zijn woordvoerders die namens de politie als deskundigen kunnen bijdragen aan het publieke debat.

Intake en screening

De politie is via verschillende kanalen bereikbaar voor het melden of aangeven van cybercrime. Zo kan op www.politie.nl 24/7 melding of aangifte gedaan worden[5]. In het geval van veelvoorkomende cybercriminaliteit wordt de melder of aangever automatisch voorzien van handelingsperspectief om verdere schade te voorkomen. Intake & service-medewerkers aan de balie en in het Regionaal Service Centrum zijn ook goed in staat om aangifte van cybercrime op te nemen doordat zij gebruik kunnen maken van hetzelfde intelligente webformulier als bij aangifte via internet. Digitaal specialisten ondersteunen de intake van complexere zaken waar nodig. Ook grotere bedrijven of instellingen die slachtoffer zijn geworden van cybercrime worden professioneel door de politie benaderd.

Binnenkomende meldingen en aangiften worden gemonitord om nieuwe dreigingen direct te kunnen delen met overheden, bedrijven en burgers. Op deze manier voorkomen we grotere aantallen slachtoffers en beperken we schade. Ook wordt gescreend op cybercrime ten behoeve van juiste registratie, het tijdig en correct veiligstellen van (doorgaans vluchtig) digitaal bewijs, sturing en weging van zaken.

Informatiepositie

De politie heeft een informatiepositie op het gebied van cybercrime. Het veiligheidsthema is verankerd in de informatieorganisatie en diens werkprocessen en systemen zijn flexibel genoeg om de ontwikkelingen in dit dynamische aandachtsgebied bij te houden. Er wordt effectief gebruik gemaakt van de beschikbare informatiebronnen (meldingen, aangiften, criminele

[4] De operationele focus en tactiek wordt uitgewerkt in vertrouwelijke tactisch programma's.
[5] Dit is al jaren een bestuurlijke prioriteit (met IV-fiche).

inlichtingen, opsporingsonderzoeken, sociale media, input van publieke en private partners in binnen- en buitenland etc.). De politie past data science toe om grote hoeveelheden gegevens in samenhang te analyseren. Op basis daarvan kan de aard en omvang van de dreiging geduid worden en een effectieve bestrijdingsstrategie bepaald worden. Individueel slachtofferschap is hierbij niet het uitgangspunt. Er wordt voornamelijk ingezet op het verstoren van business modellen van cybercriminelen. Gezien de grenzeloosheid van cybercrime is er zowel aandacht voor de regionale aspecten als voor nationaal in- en overzicht en internationale aspecten.

Gereserveerde capaciteit

In alle eenheden is voldoende tactische en digitale capaciteit beschikbaar om gezamenlijk een betekenisvolle bijdrage te leveren aan de bestrijding van cybercrime. Om de weerbaarheid van de samenleving daadwerkelijk te verhogen wordt deze capaciteit naast opsporing ook ingezet op preventie, verstoren, signaleren en adviseren[6].

Er is sprake van gelaagdheid in de opsporing van cybercrime. Hiermee wordt de aanpak verbreed van de aanpak van high tech crime door het Team High Tech Crime (THTC) naar de aanpak van cybercrime door alle eenheden. Cybercrime-zaken worden op basis van het toewijzingskader en beschikbare expertise toegewezen aan de Dienst Landelijke Recherche (DLR), Dienst Regionale Recherche (DRR), districtsrecherche of basisteams. Doordat de regionale eenheden ook in staat zijn om complexere cybercrime zaken uit te voeren kan het THTC zich op de meest ondermijnende en innovatieve vormen richten. Zo blijft de voorkant van de ontwikkelingen in beeld, kan het THTC de top-cybercriminelen aanpakken en internationaal in hoog aanzien blijven staan. Door de sluitende aanpak bouwt de Nederlandse politie op dit aandachtsgebied een gedegen reputatie op.

De aanpak is in de regionale eenheden zo uniform mogelijk ingericht. Er is in afstemming met het lokaal gezag overal voldoende tactische capaciteit vrijgemaakt en samengebracht met (digitaal) specialisme. Zo wordt de continuïteit gewaarborgd en kan van daaruit afgestemd en (uit)geleerd worden. Hier is ook 24/7 capaciteit beschikbaar om direct minimale inzet te plegen als een cybercrime zaak zich aandient. Zo wordt voorkomen dat digitale sporen door de vluchtigheid van gegevens verloren gaan.

In het kader van het Project Intensivering Aanpak Cybercrime (PIAC) zijn binnen alle eenheden voor het onderwerp cybercrime tactisch teamleiders aangewezen. Zij fungeren als vliegwiel om de beweging binnen de eenheid te stimuleren in verbinding met de andere eenheden. Zo kan de politie in samenspraak met het OM zowel regionaal als landelijk een sluitend operationeel netwerk vormen. De gebiedsgebonden eis wordt losgelaten. Zaken kunnen ook thematisch worden toegewezen aan specifieke regionale eenheden.

Kennis en kunde

De politie investeert genoeg in kennis en kunde. Politiemedewerkers worden voldoende geïnformeerd, opgeleid en van (ICT) middelen voorzien om hun verantwoordelijkheid op het gebied van cybercrime te kunnen nemen. Er is sprake van divers samengestelde teams (in termen van achtergrond, vooropleiding, kennis en ervaring) met een can-do-mentaliteit. Experts maken integraal onderdeel uit van de operationele processen en worden van specialistische (ICT) middelen voorzien. De cultuur, manier van sturen op onderzoeken en leidinggeven aan medewerkers maken dat er ruimte is voor ieders inbreng en ontwikkeling.

De aanpak van cybercrime is mikken op een bewegend doel. De politie investeert daarom in innovatie om het veranderende aanbod het hoofd te kunnen bieden. Ondanks al deze

[6] Volgens de definitie van Klerks (2010) richt opsporing zich op ‘het voorkomen, tegengaan en oplossen van criminaliteitsproblemen’ en zouden de genoemde activiteiten dus sowieso onderdeel van de opsporing uit moeten maken.

investeringen kan de politie door de snelle ontwikkelingen nooit zelf over alle benodigde expertise beschikken. Waar nodig wordt expertise extern ingehuurd of een beroep gedaan op samenwerkingsverbanden.

Samenwerking

De politie werkt intensief samen met nationale en internationale publieke en private partners. Het gaat daarbij vooral om informatie-uitwisseling en het nemen van maatregelen. Iedereen neemt zijn verantwoordelijkheid en wordt daarop aangesproken. Dit gebeurt met respect voor elkaars belangen en inzicht in elkaars mogelijkheden en onmogelijkheden. Ook burgers leveren een belangrijke bijdrage door hun kennis en kunde in te zetten (wisdom of the crowd).

Samenhang speerpunten

Alhoewel de speerpunten hier afzonderlijk beschreven zijn versterken zij elkaar. Zo levert het verbeteren van de intake een belangrijke bijdrage aan het verbeteren van de informatiepositie. Het reserveren van tactische capaciteit maakt het mogelijk om als politie met het OM een operationeel netwerk te vormen. Het gaat om het creëren van een sluitende structuur. Zo kunnen activiteiten op elkaar afgestemd worden en kan de politie eenduidig signaleren, adviseren en duurzame samenwerkingsverbanden aangaan. Op die manier kan de politie een betekenisvolle bijdrage leveren aan het verhogen van de weerbaarheid van de samenleving tegen cybercrime.

Een randvoorwaarde voor alle speerpunten is adequate ICT. Dit betekent dat de uitvoering van de strategie gepaard zal moeten gaan met investeringen in de IV-organisatie.

De voortgang van de uitvoering van de strategie zal regelmatig geëvalueerd moeten worden om, waar nodig, de koers bij te kunnen stellen en tijdig nieuwe doelen voor de langere termijn te kunnen formuleren.

5. Toekomstbestendige politie

Deze strategie heeft een horizon van nog geen vijf jaar. Het ziet toe op een beweging op korte termijn, namelijk de periode dat cybercrime nog als ‘bijzonder’ beschouwd kan worden. Dit wordt gezien als een noodzakelijke eerste stap richting de kanteling van de politieorganisatie als geheel naar de nieuwe werkelijkheid. In andere documenten (Contourennota, Sterkte en Zwakte Analyse Opsporing en de op te stellen Strategie Politie 2020 - 2025) worden de contouren geschetst voor verdere professionalisering van het politiewerk in het digitale tijdperk. Kennis en ervaring op het gebied van cybercrime gaat de politie helpen om een visie te vormen op fundamentele vraagstukken over de toekomstige rol van de politie en om bredere ontwikkelingen aan te jagen. Het is een katalysator voor de aanpak van gedigitaliseerde criminaliteit en het benutten van de kansen die de digitale wereld biedt voor de opsporing van reguliere delicten. Als de organisatie nu niet in beweging komt speelt de politie te laat in op de ontwikkelingen die er zijn om daar zelf een positie in te kunnen bepalen. Essentieel is dat er een manier gevonden wordt waarop de politie kan meebewegen met de technologische ontwikkelingen die de samenleving blijvend veranderen. Voor een toekomstbestendige politie die waakzaam en dienstbaar is, ook in het digitale domein.