Ontwerp ‘Nationale Infrastructuur Bestrijding Cybercrime’

Den Haag, Maart 2006

INHOUDSOPGAVE

Voorwoord

In 2004 zijn twee projecten van start gegaan gericht op versterking van de aanpak van Cybercrime. Het project NHTCC (National HighTech Crime Center) concentreert zich primair op het vormgeven van de proactieve taak van de overheid en meer specifiek van de politie, op het gebied van de bestrijding van ICT criminaliteit. Het project NPAC (NPC-project Aanpak Cybercrime) richt zich met name op de niet-strafrechtelijke bestrijding door het versterken van de informatie-uitwisseling, samenwerking, en coördinatie tussen publieke en private partijen. Vanaf de aanvang participeerde het project NHTCC met een vertegenwoordiger binnen het NPAC-project.

Vanwege de samenhang tussen beide projecten gericht op hetzelfde thema, zijn vanaf het voorjaar van 2005 de projectactiviteiten op elkaar afgestemd. Uiteindelijk heeft dat geleid tot het gezamenlijk opstellen van een ontwerp voor een Nationale Infrastructuur gericht op de bestrijding van cybercrime, zoals neergelegd in deze notitie. Daarin zijn de ervaringen en de werkwijze van beide projecten geïntegreerd, zodat sprake is van een versterkte voortzetting van beide projecten maar dan onder eenzelfde noemer.

Het ontwerp is met instemming ontvangen door de Raad van Advies van het NPC (Nationaal Platform Criminaliteitsbeheersing, opdrachtgever voor het NPAC-project) en de Stuurgroep NHTCC (opdrachtgever voor het NHTCC-project). Daarmee is ook de integratie van beide projecten een feit geworden. In de vorm van een programma zullen de implementatieactiviteiten voor de Nationale Infrastructuur ter hand worden genomen. Kern van dat programma vormen vier praktijktoepassingen gericht op respectievelijk het MKB, de decentrale overheid, de bancaire sector en de grote industrie in relatie tot vitale infrastructuren. Mede op basis van de uitkomsten van deze praktijktoepassingen, zal de Nationale Infrastructuur tegen Cybercrime worden geïmplementeerd.

Onder de noemer National High Tech Crime Center wordt de inrichting van een opsporingsunit voorgesteld die zich richt op bijzondere vormen van cybercrime.

Hoofdstuk 1 Introductie Cybercrime

In dit inleidende hoofdstuk worden cybercrime als probleem en het bestrijdingsproces als oplossing, kort geïntroduceerd. Daarbij is niet gestreefd naar volledigheid. Alleen de elementen die het doorgronden van het ontwerp voor de Nationale Infrastructuur zoals dat in latere hoofdstukken wordt uiteengezet vergemakkelijken, worden in dit hoofdstuk toegelicht.

1.1 Het inhoudelijke vraagstuk

Het KLPD heeft in 2002 een rapport uitgegeven[1] over de definitie en afbakening van het begrip cybercrime: *cybercrime omvat elke strafbare en strafwaardige gedraging, voor de uitvoering waarvan het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is*. Onder strafwaardig moet worden verstaan: *gedrag waarvan verwacht wordt dat het binnen afzienbare tijd strafbaar wordt gesteld*. Hierdoor is het begrip cybercrime robuuster ten opzichte van de ontwikkelingen in de techniek en in de maatschappij. Cybercrime valt verder onder te verdelen in verschijningsvormen waarbij de computer (alleen) als middel wordt gebruikt en verschijningsvormen waarbij de computer naast middel ook doel is van het strafbare of strafwaardige gedrag (cybercrime in enge zin). In hoofdstuk 4 zijn de verschillende verschijningsvormen nader toegelicht.

Cybercrime is in het algemeen een onderbelicht fenomeen in de wereld van criminaliteitsbestrijding. Het kenmerkt zich in hoge mate door criminele activiteiten die zich in de anonimiteit van het internet afspelen, veelal buiten de fysieke omgeving om. Criminelen maken gebruik van de mogelijkheden van ICT om hun identiteit te verhullen en switchen continue van methodes en gedragingen. Zij zijn wereldwijd actief en voortdurend op zoek naar de zwakste schakels bij (publieke en private) organisaties.

1.2 De historische en maatschappelijke context

Meer en meer vinden dienstverlening en transacties plaats in of met behulp van ICT-omgevingen. Deze ICT-omgevingen zijn gemakkelijker en sneller toegankelijk geworden in de afgelopen jaren. Dit heeft geleid tot een roep om betere beveiliging van die diensten en de computernetwerken waarlangs zij worden aangeboden en verricht. Deze roep kwam in eerste instantie van de zijde van de gebruikers van die diensten en ICT-voorzieningen. Meer en meer kregen zij te maken met diverse vormen van criminaliteit gerelateerd aan het gebruik van computers, netwerken en ICT-diensten. De ICT-industrie kwam de gebruikers tegemoet, en vele beveiligingsmaatregelen volgden. Niet alleen op hardwarematig en softwarematig terrein, maar ook in relatie tot het menselijke (gebruikers-) aspect.

[1] Mooij, J. en J. van der Werf (2002) Cybercrime. Zoetermeer: KLPD (NRI 22/2002)

Sterk vereenvoudigd voorgesteld, laat de ontwikkeling van de op ICT gerichte of door ICT gefaciliteerde criminaliteit zich in drie fasen beschrijven.

Fase 1: Ontdekking van mogelijkheden. Periode: 1980-1995
In deze fase wordt in hoog tempo duidelijk dat men computers en computernetwerken voor meer doeleinden kan gebruiken dan voor louter communicatie of wetenschappelijke doeleinden. Nieuwe diensten en toepassingen die gebruikmaken van ICT volgen elkaar snel op. De gevallen waarbij de politie te maken krijgt met computercriminaliteit, cybercrime of ICT-criminaliteit leiden vaak tot daders die zich van geen kwaad bewust zijn. Meestal gaat het om eenlingen of kleine groepen die, hoewel bewust van de effecten van hun technisch handelen, geen oogmerk hebben om in georganiseerd verband zware vormen van criminaliteit te begaan. Uitgangspunt van hun illegale activiteiten is vooral de technische uitdaging.

De op dat moment bekende en actieve criminele organisaties gebruiken elektronische netwerken als communicatiemiddel, en minder als informatiebron of als infrastructurele basis voor hun organisatie.

Fase 2: Groei van crimineel gebruik. Periode: 1996-2002
Deze fase kenmerkt zich door groeiende bewustwording bij gebruikers, markt maar ook het criminele circuit. Het gebruik van ICT in de samenleving is sterk toegenomen. Er zijn mensen die alles weten van ICT, mensen die er wars van zijn en een groep mensen die gebruik maakt van ICT, maar geen idee heeft hoe de technologie (zoals elektronische zakagenda's, GPS systemen, mobiele telefoons, e-mail, www) nu eigenlijk precies in elkaar zit. Er treden nieuwe groepen ICT-misbruikers aan:
1) een nieuwe lichting technologisch goed onderlegde computercriminelen die goed weet wat de consequenties zijn of kunnen zijn van hun gedragingen in de virtuele wereld, en weet hoe daar in de fysieke wereld over wordt gedacht, en
2) groepen criminelen die geen ICT-experts genoemd kunnen worden maar goed beseffen dat het de computerwereld is waar de interessante financiële transacties plaatsvinden en continu manieren proberen te verzinnen om andere ICT-gebruikers geld afhandig te maken. Als zij het niet zelf kunnen verzinnen, dan kijken ze het desnoods af bij anderen of roepen ze de hulp van derden in. Oplossingen waarvoor -dankzij ICT- steeds makkelijker en sneller gekozen kan worden.

De criminele organisaties gaan ICT niet meer alleen als communicatiemiddel gebruikten, maar ook als instrument om extra financiën te genereren. Voorbeelden daarvan zijn: illegale handel in gekopieerde software, vormen van internetfraude via veiling en verkoopsites, oplichtingpraktijken (Nigeriaanse fraude), telecomfraude (via belhuizen en PABX centrales), witwas- en afpersingspraktijken. Organisaties – bijvoorbeeld in Oost-Europa of Zuidoost Azië - blijken deze vormen van criminaliteit te benutten als exogene financiering voor de meer traditionele en klassieke criminaliteitsvormen. Ook wordt de computer door criminelen ingezet als werktuig (bijvoorbeeld in de vorm van hacking, keylogging en andere manieren van interceptie).

ICT vormt steeds meer de basisinfrastructuur voor velerlei soorten activiteiten in de samenleving, ook voor

criminaliteit en criminaliteitsbestrijding. Criminelen lijken zich in deze fase veel meer bewust te zijn van de voordelen van het gebruik van ICT voor hun criminele activiteiten. Bij overheid en bedrijfsleven worden de gevaren van crimineel ICT-gebruik weinig tot niet onderkend.

Fase 3: Beveiliging wordt structureler. Periode 2003 e.v.
Een toenemende mate van professionalisering valt waar te nemen. Alle ICT-gebruikers (groot en klein) weten min of meer wat de gevaren zijn, dat ICT misbruikt kan worden en wat de gevolgen daarvan kunnen zijn. Waren bedrijven als slachtoffer van ICT-gebruik vroeger met name geïnteresseerd in de 'businesscontinuïteit', nu willen ze weten wie dat misbruik heeft gepleegd. ICT is nu niet meer 'de infrastructuur voor', maar het is de 'aorta van' geworden; ICT stuurt kernprocessen in de samenleving aan, nationaal en internationaal. Het belang van de continuïteit van die processen is mede daarom bijzonder groot. Daardoor nemen telecomproviders en de ICT-industrie ook meer verantwoordelijkheid voor hun rol bij het leveren van diensten of het produceren van ICT-systemen, netwerken en componenten.

Misbruik van ICT wordt in het buitenland reeds strenger gestraft. Ook in Nederland roept de samenleving hierom en worden verschillende vormen van computercriminaliteit onderdeel van het Wetboek van Strafrecht. Incidenten worden sneller gemeld en kwetsbare onderdelen van de ICT-infrastructuur worden door slachtoffers gerepareerd. De criminelen of criminele organisaties gaan echter dikwijls vrijuit. Niet alleen de roep om opsporing van de misbruiker(s) is toegenomen, maar ook het besef dat voorkomen beter is dan genezen. De ontwikkeling van de virusscanner en de firewall, naar netwerkbrede Intrusion Detection Systemen en filter technologieën zijn daarvan het resultaat. Terwijl de gebruiker ook graag de gegevens die worden uitgewisseld en de kanalen waarlangs dat plaatsvindt, zoveel mogelijk afschermt van mogelijke meeluisteraars. Als oplossing daarvoor doen Virtual Private Networks, PGP Universal en CryptoGSMs hun intrede.

1.3 Het Cybercrime-bestrijdingsproces

De aanpak van cybercrime is voor te stellen als een ketenproces. Een effect in één van de schakels van de keten heeft direct consequenties voor een ander deel. Het ontbreken van maatregelen in delen van de keten maakt deze als geheel zwakker.

De volgende processtappen worden als onderdeel van het totale bestrijdingsproces onderscheiden.

1. *Proactie*
   Deze schakel bestaat enerzijds uit het bij de basis onderwijzen van gebruikers van ICT en internet over risico's en anderzijds bij de ontwikkeling en productie van hard- en software in voldoende mate rekening houden met het potentiële criminele misbruik ervan.
2. *Preventie*
   Het gaat hierbij om de zorg voor adequate bescherming, middels virusbeschermers, firewalls, product-updates e.d.

3. *Preparatie*

   Ondanks de toepassing van proactie en preventie moet men wel voorbereid zijn op een mogelijke aanvallen. Preparatieactiviteiten voorzien daarin.

4. *Signalering*

   Er worden drie vormen van signalering onderscheiden:

   a. melding: iemand belt, mailt of anderszins en geeft aan de ontvangende instantie aan wat het probleem is (een melding kan uit het buitenland komen, van een bank, een bedrijf etc.);
   b. aangifte: iemand heeft schade geleden en doet aangifte bij de politie;
   c. detectie: er is geen melding noch een aangifte, maar er wordt via monitoringssystemen ambtshalve vastgesteld dat er iets aan de hand is.

5. *Opvolging*

   De verschillende manieren waarop een signaal binnenkomt, zijn ook bepalend voor de opvolging. Zes verschillende opvolgingsvarianten worden onderscheiden:

   a. opsporing/vervolging/berechting: een aangifte is al een opsporingsverzoek, maar ook een melding kan een aangifte worden, en politie/OM kunnen besluiten om ambtshalve op te sporen;
   b. stop-actie: het signaal kan aanleiding zijn voor het ondernemen van een stop-actie als samenwerkingsactie van verschillende nationale en/of internationale partijen;
   c. civiele actie: er kan een civiele claim worden gelegd;
   d. waarschuwing: het signaal kan in de vorm van een voorlichtingsproduct worden rond gestuurd;
   e. advies: er kunnen preventie- en (p)reparatie adviezen worden uitgebracht aan bijvoorbeeld netwerkbeheerders en het grote publiek, maar ook beleidsadviezen aan departementen;
   f. ontwikkeling: het signaal kan aanleiding zijn voor het ontwikkelen van bepaalde producten, procedures of organisatievormen.

6. *Terugkoppeling*

   Iedere opvolging kan een terugkoppeling inhouden naar de oorspronkelijke melder/aangever of anderen, opdat zij gemotiveerd blijven om meldingen door te geven. Terugkoppeling is eigenlijk geen afzonderlijke stap, maar loopt dwars door alle stappen heen. Niet alleen het kunnen volgen van de voortgang van een proces is van belang, maar vooral ook wat het tot dan heeft opgeleverd.

7. *Resultaat*

   Het resultaat bestaat uit hetgeen de keten uiteindelijk oplevert in termen van: schadevoorkoming of schadereductie, de mate waarin een doelgroep is bereikt, of een site uit de lucht gehaald, of daders zijn veroordeeld, of er door anti-virussoftware leveranciers een instrument is ontwikkeld, of er gaten in software zijn gedicht etc.

8. *Evaluatie*

   In feite is dit een bijzondere vorm van terugkoppeling. Er wordt niet alleen vastgesteld wat er is bereikt maar

ook of dat op de juiste wijze is geschiedt. Heeft het proces efficiënt plaatsgevonden, is het resultaat duurzaam, en of het resultaat voldoende is in het licht van generale- of specifieke preventie.

9. *Nazorg*

   Het resultaat wordt tijdens de nazorg in het perspectief van de toekomst geplaatst. Aan de orde is hoe belangrijke zaken onder de aandacht kunnen blijven, de herhalingsfrequentie van bepaalde activiteiten, en hoe men zaken eerder voor kan zijn.

10. *Toezicht*

    De uiteindelijke nacontrole van alle activiteiten vormt het sluitstuk, zodat betrokken partijen er op kunnen vertrouwen dat een ieder zijn of haar steentje bijdraagt. Te denken valt hierbij aan visitaties, audits, en scans. Deze vormen van toezicht vinden plaats op vrijwillige basis.

Hoofdstuk 2 Probleemstelling en ontwerpcriteria

In dit tweede hoofdstuk verschuift de oriëntatie van *probleemgericht* naar *oplossingsgericht.* Het begint met een meervoudige probleemstelling over cybercrime en de bestrijding daarvan. Die probleemstelling vormt op zijn beurt de basis voor een aantal uitgangspunten (kwaliteitscriteria) waaraan de bestrijding van cybercrime zal moeten voldoen om succesvol te zijn. Die uitgangspunten staan los van het uiteindelijk voor die bestrijding te kiezen organisatorisch ontwerp. Ze zijn te zien als algemeen geldende ontwerpcriteria, die van toepassing zijn op elk ontwerp van een aanpak. Uit de probleemstelling is de doelstelling afgeleid voor de bestrijding van cybercrime. De wijze waarop aan die doelstelling zou kunnen worden beantwoord staat centraal in de vraagstelling.
Het hoofdstuk sluit af met een conclusie, waarop in de volgende hoofdstukken wordt voortgebouwd.

2.1 Probleemstelling

In de huidige opzet van de bestrijding van cybercrime in Nederland doet zich een aantal knelpunten voor. Het begrip bestrijding wordt in deze notitie breed gehanteerd en omvat alle processtappen die in het vorige hoofdstuk zijn onderscheiden, waaronder de opsporing. De verschillende knelpunten zoals die thans worden ervaren passeren in willekeurige volgorde één voor één de revue.

2.1.1 Onduidelijkheid over het domein: wat is cybercrime?

Eerder in deze notitie zijn de inhoudelijke elementen van cybercrime beschreven. Maar daarmee is het domein van cybercrime nog niet afdoende afgebakend: waar begint het en waar houdt het op? De afbakening van het begrip is relevant om te kunnen bepalen op welk domein de aanpak van cybercrime en de daarbij te betrekken partners zich zou moeten richten.
Cybercrime laat zich maar moeilijk etiketteren. Een crimineel kan zich vandaag bezighouden met online neploterijen, hij kan morgen aan het vissen zijn naar iemands internet bankiergegevens, en volgende week een illegaal online casino runnen. Of misschien perst hij juist anderen af door te dreigen online voorzieningen plat te leggen. Dankzij ICT is hij hiertoe in staat, met behulp van telkens dezelfde computersystemen en vanuit dezelfde locatie (waar ook ter wereld en relatief afgeschermd voor politie en justitie). Bijvoorbeeld door snel en continu te wisselen van virtuele identiteit. Is dat nou allemaal cybercrime en dus onderwerp van aandacht voor de bestrijding of juist niet? Moeten we er als samenleving iets mee en zo ja, bij wie is c.q. wordt het dan als aandachtsgebied belegd?

Cybercrime is niet een zelfstandig criminaliteitsterrein zoals bijvoorbeeld drugshandel, mensenhandel, of fraude. Cybercrime heeft overal wat mee te maken en de inherente complexe ICT-component loopt als een rode draad

door vele criminaliteitsterreinen heen. Daardoor laat cybercrime zich op zich ook moeilijk zelfstandig aanpakken omdat het vaak is verbonden met een ander ‘gronddelict’. Dit levert momenteel niet alleen een probleem op bij de registratie van cybercrime incidenten (moeten we ‘phishing’ fraude noemen? Is ‘spoofing’ oplichting?), maar ook moet iedereen die zich met criminaliteit bezighoudt, op de hoogte worden gebracht van de invloed van ICT op die criminaliteit.

2.1.2 Onvoldoende inzicht in aard en omvang: is er wel een probleem?

Ook al is cybercrime een fenomeen waarmee men zich al jaren geconfronteerd ziet: de aard en omvang van het probleem zijn onduidelijk. Verschillende redenen liggen daaraan ten grondslag.

- Cybercrime wordt niet als zodanig geregistreerd maar als diefstal van gegevens, fraude, afpersing of als een ander traditioneel vergrijp;
- Organisaties die met cybercrime zijn geconfronteerd doen nauwelijks aangifte. Aan de ene kant vanuit de verwachting “dat er toch niets mee wordt gedaan”, en aan de andere kant uit angst voor imagoschade in het geval een inbreuk breder bij het publiek bekend zou worden;
- Het doen van aangifte kan ook betekenen dat de dienstverlening van de benadeelde aanbieder nog langer wordt verstoord dan al het geval is bijvoorbeeld omdat dit in het belang is van het opsporingsonderzoek.

Mede door het ontbreken van voldoende inzicht in de aard en omvang van cybercrime, is deze vorm van criminaliteit weliswaar veel besproken, maar komt ze niet voor op de prioriteitenlijsten van bijvoorbeeld opsporingsinstanties. Daardoor worden er ook geen bruikbare cijfers gegenereerd die aangeven hoe groot het probleem nu werkelijk is. Een bevestiging hiervan komt uit het Nationaal Dreigingsbeeld waarin ondermeer wordt vastgesteld dat aangaande de dreiging die voortkomt uit cybercrime nog een groot aantal zogenaamde ‘witte vlekken’ bestaat.

Als het inzicht in de aard en omvang van het cybercrimevraagstuk ontbreekt, weet men als verantwoordelijken voor het voorkomen en bestrijden van cybercrime ook niet hoe men zich daarop moet organiseren en prepareren. Al snel gaat men dan *aanbodgericht* te werk in plaats van *vraaggericht*. In de huidige bewustwordingscampagnes is dit effect duidelijk merkbaar. Op basis van de inzichten van betrokken professionals wordt (een deel van) het veld bediend met allerlei op zich mooie producten, maar zonder exact te weten of die ook daadwerkelijk aangrijpen op een onderliggend vraagstuk. Het gebrek aan inzicht in aard en omvang van het cybercrimevraagstuk werkt ook direct door op de projecten NHTCC en NPAC. Op zichzelf zijn zij als fenomeen al een voorbeeld van aanbodgerichtheid.

Het fenomeen cybercrime lijkt zich de afgelopen tijd steeds manifester voor te doen. Maar ondanks de verspreiding van miljoenen virussen en botnets, lijken echt grote crashes met een groot maatschappelijk ontwrichtend effect uit te blijven. Mogelijk dat er in de markt ook sprake is van een zelfcorrigerend effect: voordat een probleem een grote vlucht kan nemen ontstaat er besef van het risico en wordt er ingegrepen. Op mondiaal niveau wordt er bijvoorbeeeld nieuwe antivirus-software toegevoegd aan het bestaande arsenaal, een ander brengt weer een iets betere firewall op de markt, en beveiligingsgaten in software worden gedicht door

patches. Op individueel niveau formatteert een gebruiker die slachtoffer van cybercrime is geworden noodgedwongen zijn pc opnieuw, om na een paar weken het voorval weer te zijn vergeten. Een wedloop waarvan het netto-effect kennelijk positief is omdat men zich in de loop van de tijd ondanks de risico's steeds fundamenteler en vaker bedient van elektronische communicatie.

Ondertussen zijn dezelfde signalen voor beleidsmakers voldoende aanleiding om te beseffen dat er van alles onder de oppervlakte gebeurt waar niemand precies weet van heeft. Wellicht heeft dat niet zozeer een eenmalig explosief effect, maar nestelt het zich fnuikend in het normale verkeer, waarmee een vrijwel onaantastbare basis kan worden gelegd voor wederrechtelijke zelfverrijking in de vorm van elektronische diefstal. Het is zeer de vraag of de veelal afzonderlijk georganiseerde sectoren voldoende doordrongen zijn van dit gemeenschappelijke probleem.

2.1.3 Onvoldoende onderzoek rol cybercrime bij criminaliteit(sbestrijding)

ICT vormt de rode draad door vele criminaliteitsvormen en blijkt regelmatig een belemmerende of hinderende factor in opsporingsonderzoeken te zijn (of het voorkomt zelfs dat opsporingsonderzoeken worden gestart). Desondanks wordt momenteel in Nederland niet breed en gecoördineerd onderzocht of bijvoorbeeld de private partijen, de politie en veiligheids- en inlichtingendiensten in staat zijn om efficiënt en effectief reactief, proactief of zelfs realtime op te treden als het gaat om de rol van ICT bij het plegen van criminaliteit of bij het voorkomen en bestrijden van criminaliteit.

2.1.4 Dynamische ontwikkeling: achter de feiten aanlopen

ICT ontwikkelingen gaan snel. Men heeft zich nog niet op het ene verschijnsel van cybercrime geprepareerd of het is al weer ingehaald door iets anders. Deze dynamiek speelt op verschillende fronten.

- Criminelen proberen voortdurend gebruik te maken van beveiligingsgaten of juridische mazen; wat ook steeds opnieuw lukt. Daar moet de markt weer op reageren wat weer een nieuwe uitdaging voor de criminelen met zich meebrengt. Daarmee is de wedloop een feit.
- De legale soft- en hardwarebouwers komen voortdurend met nieuwe toepassingen voor de consument, waardoor er ook weer nieuwe mogelijkheden en manieren van misbruik ontstaan. Vaak moet dat misbruik eerst in de praktijk optreden, voordat men doorheeft dat de nieuwe technologie of functionaliteit zwakke plekken bevat.

Het probleem is dat men als bestrijders van cybercrime nauwelijks toekomt aan het voeren van proactief beleid: de voorkant van het probleem. De bestrijding van cybercrime vergt een even snelle omgeving als die van de wereld van ICT en Internet. Een wereld die zich laat kenmerken door snelheid, flexibiliteit, mobiliteit en gebruiksvriendelijkheid. Tot op heden is het op de voet volgen van de ontwikkelingen door handhavers niet haalbaar gebleken o.a. als gevolg van het gegeven dat er onvoldoende inzicht bestaat in de aard van de problematiek, en in de ontwikkelingen op de markt van vandaag, die het probleem van morgen vormen.

2.1.5 Beleidsmatige en commerciële aandacht is groot

Ondertussen maken steeds meer (commerciële) aanbieders handig gebruik van het gevoel dat cybercrime een groot probleem is. Kennelijk is het met de bewustwording van de individuele consument nog niet zo slecht gesteld, want er wordt breed gebruik gemaakt van virusscanners, firewalls, en anti-spywaresoftware. Een markt die niet gauw verzadigd raakt door de steeds wisselende en opvolgende dreigingen.
Hoewel iets meer bescheiden, neemt ook het aantal (semi-)overheidsinstanties toe dat op het terrein van cybercrime actief is. De hoeveelheid voorlichtingsproducten gericht op jong tot oud is de laatste jaren sterk toegenomen. Er lopen allerlei programma's ter versterking van de bewustwording en van preventie. Daarbij moet meer gestreefd worden naar onderlinge coördinatie en afstemming, vooral ook met private partijen. Mede om die reden moet worden gestreefd naar één landelijke aanpak van cybercrime waarin de verschillende publieke en private bijdragen bij elkaar komen.

2.1.6 Urgentiebeleving is gering

De geringe zichtbaarheid van de massaliteit

Ogenschijnlijk in tegenspraak met het vorige element uit de probleemstelling, is de urgentiebeleving van cybercrime gering. Het probleem met cybercrime is dat de cumulatieve effecten vaak onzichtbaar blijven. Iedereen kent wel iemand die er last van heeft gehad, maar stuk voor stuk betreft het individuele gevallen die op zichzelf genomen geen ernstige verontrusting met zich meebrengen. Om het echte probleem te kunnen zien, moet men opschalen naar nationaal en internationaal niveau. Dan worden de getallen zo ontzagwekkend groot, dat het de gemiddelde professional, zowel bij de markt als bij de overheid al gauw gaat duizelen. Door het enorme volume ('miljoenen gegijzelde computers') slaat de boodschap ook dood. Het is niet meer te omvatten, en bovendien speelt het dan niet meer in de directe omgeving van betrokkene. In tegenstelling tot veel andere problemen die wel op aandacht kunnen rekenen, is cybercrime onvoldoende lokaal herkenbaar. Het speelt zich gevoelsmatig niet af in de eigen achtertuin.

Gering schade- en slachtofferbesef

De schade door, en impact van, cybercrime wordt dikwijls sterk gebagatelliseerd door argumenten als: 'de slachtoffers hadden zichzelf maar beter moeten beschermen' of 'schade aan computers en netwerken is moeilijk te kwantificeren en is zeker minder van belang als 'echte' financiële schade'. Vaak valt die schade in de beleving van professionals ook nog wel mee. Bijvoorbeeld in het geval van het ontfutselen van gegevens van internetbankieren door internetcriminelen of andere vormen van internetfraude, waarvan meestal slechts een beperkt aantal individuele burgers het slachtoffer wordt.

Ook leeft bij velen die niet thuis zijn in de materie de gedachte, dat cybercrime te etiketteren valt als 'aangiftecriminaliteit'. In die beleving staat dit type criminaliteit gelijk aan een gering heterdaad-karakter en hoog civiel gehalte. Geleden schade wordt vooral materieel vertaald en niet in termen van bijvoorbeeld schending van de lichamelijke integriteit. Een fysieke inbraak waarbij men een huis binnendringt, kan zowel bij het slachtoffer als bij de opsporing en vervolging op meer aandacht rekenen dan een van afstand gepleegde computerinbraak. Ook al blijkt de buit daarbij veel groter te zijn. Het besef een slachtoffer te zijn, is bij de

fysieke inbraak groter dan bij de elektronische inbraak. Een begrijpelijk gevoel want het maakt wel degelijk verschil of er iemand ongewenst in huis is geweest en langs de kinderkamer is geslopen, of dat op de computer is ingebroken.

Geringe urgentiebeleving = geen prioriteit

In het geval van aangifte of opsporing, gebeurt de intake van een zaak in overleg met het Openbaar Ministerie. Cybercrime-zaken worden vaak niet aangegeven en als dat wel gebeurt, passeren ze vaker niet dan wel een dergelijke casescreening. Hiervoor zijn verschillende redenen aan te voeren. Het kan zijn dat de beoordelaars niet over de benodigde cybercrime-kennis beschikken. Maar ook is gebleken dat het niet direct voorhanden hebben van een pasklare oplossing voor de aanpak van het onderzoek een factor kan zijn. In het laatste geval bestaat de vrees voor een langdurig en ingewikkeld technisch onderzoek naar een vaak evenzo ingewikkeld cybercrime-incident, waarbij uitkomst en rendement dikwijls onzeker zijn. Ook levert angst voor imagoschade bij de aangever en de daaruit voortvloeiende terughoudendheid bij het doen van aangifte een bijdrage aan de geringe urgentiebeleving. Als het slachtoffer er al geen probleem van maakt, hoe druk moet de opsporing en vervolging zich dan nog maken. Zeker omdat er zoveel andere zaken liggen om te worden aangepakt waaraan wel een hoge prioriteit wordt toegekend.

2.1.7 Heterogene doelgroepen: sterk uiteenlopende verwachtingen

Sectoren binnen de samenleving zijn sterk heterogeen samengesteld. Dat vertaalt zich ook in de mate waarin men afhankelijk is van het elektronisch verkeer en bereid is op dat punt risico's te nemen of uit te komen voor geleden schade. Aangevers hebben verschillende verwachtingen van de effectiviteit of de mogelijke resultaten van hun eigen optreden of dat van bijvoorbeeld de politie. Zo is er lang niet altijd de wens dat de crimineel wordt opgepakt. Belangrijker is het vaak dat de criminele activiteit wordt gestaakt, want dankzij ICT zijn dat tegenwoordig los van elkaar staande zaken: de veroorzaker kan achter slot en grendel worden gezet, terwijl de criminele activiteit in de digitale omgeving gewoon doorgang vindt.

Soms wordt gehoopt dat - zoals dit ook in de fysieke omgevingen het geval is – de politie of anderen kunnen bijdragen aan een permanente verhoogde veiligheid van digitale omgevingen. Nog los van de bereidheid daartoe, maken territorialiteitsvraagstukken dit soort preventie bijzonder lastig.

2.1.8 Territorialiteitsvraagstukken: waar zijn de cybercrime en de crimineel?

Zo gemakkelijk er over cybercrime wordt gesproken, zo moeilijk is het om die cybercrime te traceren. Kenmerk van het internet is dat men vanuit willekeurig elke plaats op aarde diensten kan aanbieden en dus ook criminele handelingen kan verrichten. Zo kan de ontwerper van een botnet zich bevinden in een land A, terwijl hij de beschikking over een aantal duizenden computers heeft verkocht aan iemand in land B die deze computers activeert vanuit land C. De geactiveerde computers bevinden zich mogelijk in tientallen verschillende landen en kunnen worden ingezet voor aanvallen op systemen in land D. Beperkten territorialiteitsvraagstukken zich vroeger tot een schip of een vliegtuig, en een plaats waar de dader woonachtig was: de plaats delict was gesitueerd. Tegenwoordig ligt dat bij cybercrime een stuk ingewikkelder. Voor slachtoffers die hun recht willen

halen of een daadwerkelijke beëindiging van een maar voortdurende inbreuk nastreven, is dit probleem een nachtmerrie. Evengoed als voor bijvoorbeeld de opsporing en vervolging. Men concentreert zich noodzakelijkerwijs op het kleine stukje van de totale keten aan cybercrime dat door het eigen land loopt. De ingewikkelde internationale aspecten worden terecht geassocieerd met allerlei bewijsproblemen, waarvan de oplossing vraagt om tijd en ruimte.
Internationale aanpak van cybercrime is per definitie noodzakelijk maar ook erg moeilijk. Successen zijn er zeker, zowel in de zin van het stopzetten van inbreuken als het aanhouden van daders, maar ze zijn nog te incidenteel.

2.1.9 Onvoldoende (gemobiliseerde) kennis en deskundigheid

Er is veel inhoudelijke kennis van cybercrimevraagstukken, alleen bevindt die zich op alle plaatsen van het veld. Private en opsporings- en vervolgingsinstanties zijn onvoldoende toegerust voor hun taak op het terrein van het voorkomen en bestrijden van cybercrime. Aangevers willen goed zijn in hun primaire dienstverlening, maar zijn lang niet altijd deskundig in het beschermen van die dienstverlening tegen aanvallen van buiten. Met aanvallen die het gevolg zijn van mazen in de eigen beveiliging klopt men ook liever niet bij de politie aan, bang om het terechte verwijt te krijgen dat men zich onvoldoende heeft beschermd of geprepareerd. Aan de andere kant hebben ook politiemensen vaak onvoldoende kennis van de specifieke problematiek of de technisch complexe aspecten van een zaak. Dit is inmiddels door de politie onderkend en er is gestart met een traject om politiemensen hiervoor beter te equiperen. Private partijen zijn nog onvoldoende gemeenschappelijk georganiseerd om ook daar dergelijke preparatie-activiteiten van de grond te krijgen. Voor de benodigde vervolgstappen van een aangifte bij de politie zijn diepte-investeringen nodig aan zowel private als publieke zijde, wil de kans dat een zaak op een goede manier terecht komt in het rechercheproces en leidt tot succesvolle vervolging, toenemen.

De bestrijding van cybercrime zal het maar beperkt moeten hebben van de opsporing en vervolging. Het afdekken van het totale bestrijdingsproces vraagt om meer activiteiten dan uitsluitend die van politie of justitie. En dan valt op dat op enkele positieve uitzonderingen na, veel organisaties kampen met een gebrek aan deskundigheid om de juiste preventieve maatregelen te nemen en zich op voordoende situaties voor te bereiden c.q. die het hoofd te kunnen bieden. Hoewel er ook organisaties zijn die zeggen alles goed op orde te hebben. Juist deze organisaties zouden als belangrijke kennisleveranciers van anderen kunnen dienen die minder ver zijn. Nu wordt kennis nog onvoldoende gemobiliseerd en gedeeld. Met behulp van communicatie, informatie uitwisseling over daders, doelwitten en tools, kan men bevorderen dat bestaande initiatieven gericht op het voorkomen of terugdringen van cybercrime worden gecoördineerd en gestroomlijnd. Met name de informatie-uitwisseling tussen partijen in de publieke én de private sector lijkt een probleem. Zowel waar het slachtoffers, onderzoekers en de bestrijders van cybercrime betreft.

2.1.10 Onduidelijkheid over de rolverdeling

Wanneer het veld wordt beschouwd dat is betrokken c.q. zou kunnen worden betrokken bij de bestrijding van

cybercrime, dan zijn de rollen van actoren op dit moment met name in het publieke domein gedefinieerd. Zo is er bijvoorbeeld kennis en opsporingscapaciteit beschikbaar binnen het opsporingsapparaat. Denk hierbij ook aan de bijzondere opsporingsdiensten zoals FIOD/ECD en SIOD; of aan de expertise bij organisaties zoals GOVCERT, en toezichthouders in diverse sectoren (AFM, OPTA en NMA, Agentschap Telecom, De Consumenten Autoriteit i.o.). De private partijen zijn minder expliciet georganiseerd op het tegengaan van cybercrime, zodat per sector niet altijd duidelijk is of en waar bedrijven terecht kunnen. Het is niet direct duidelijk wat de behoefte, rol(len) en eigen verantwoordelijkheden zijn van overheidsinstellingen en het bedrijfsleven bij de aanpak van cybercrime. Samenwerking (ook in internationaal verband) tussen organisaties (publiek en privaat) is nog niet in alle onderdelen van de keten in voldoende mate ingesleten en vindt nog teveel ad hoc plaats (namelijk per geconstateerd incident).

2.1.11 Versnippering van aandacht: witte vlekken

Temidden van alle actoren en projecten die zich meer of minder bewegen rondom het cybercrimevraagstuk in al zijn facetten, publiek en privaat, moet er op worden gelet dat de diverse sectoren voldoende worden bediend. Er bestaan op verschillende niveaus en bij verschillende sectoren (met het MKB als voorbeeld) ‘witte vlekken’ in de aandacht voor cybercrime. De witte vlekken doen zich op de volgende niveaus voor.

- Processtappen: een groot deel van de processtappen waarin het bestrijdingsproces van cybercrime kan worden opgedeeld, is niet of slechts ten dele afgedekt;
- Domeinen: niet alle typen van misbruik en illegaal gebruik die tot cybercrime kunnen worden gerekend zijn ergens belegd;
- Functies: in een aantal functies waaruit de bestrijding van cybercrime zou moeten zijn opgebouwd is niet of slechts ten dele voorzien.

2.2 Doelstelling

In een dergelijk woud aan elementen van de probleemstelling is het niet gemakkelijk om überhaupt nog tot een doelstelling te komen. Daarom is het juist in een groot, complex en verweven vraagstuk als het voorkomen en bestrijden van cybercrime, belangrijk om scherp voor ogen te houden waartoe verschillende inspanningen zouden moeten leiden. Die centrale doelstelling is als volgt verwoord:

Het verminderen van de kwetsbaarheid van *overheid en bedrijfsleven* voor cybercrime,
- door verhoging van het bewustzijn over gevolgen ervan;
- door verhoging van het kennisniveau;
- door het organiseren van preventieve maatregelen;
- door verbetering van het collectieve reactievermogen op zich voordoende incidenten;

De doelstelling kan inhoud krijgen door:

- zich gezamenlijk voor te bereiden op eventuele aanvallen;
- gezamenlijk zich voordoende aanvallen te stoppen;

- gezamenlijk zich manifesterende (potentiële) daders te ontmoedigen;
- gezamenlijk te werken aan het voorkomen en herstel van schade in de volgorde van belangrijkheid:
    a. Levensbedreiging
    b. Maatschappelijke ontwrichting
    c. Continuïteit bedrijfsvoering
    d. Financiële schade

Kortom: het gezamenlijk als overheid en bedrijfsleven voorkomen, stoppen en zo mogelijk herstellen van de schade als gevolg van cybercrime.

2.3 Vraagstelling

In deze notitie schemert ongerustheid over het te beperkte inzicht in aard en omvang van het cybercrimevraagstuk door. Ondanks dit gegeven is nietsdoen ook geen optie. Zowaar geen eenvoudige ingrediënten voor een vraagstelling die het scharnierpunt vormt van probleemgerichtheid naar oplossingsgerichtheid.

De eerste hoofdvraag is ingegeven door de behoefte aan fundamenteel inzicht in het cybercrimevraagstuk. Ze is op metaniveau gedefinieerd, omdat er al diverse pogingen zijn gedaan om het inzicht te vergroten. Daarbij steeds stuitend op onvoldoende vervulde randvoorwaarden, en het probleem dat van snelle vervulling ook geen sprake zal zijn. Een voorbeeld van een dergelijke niet snel te realiseren randvoorwaarde betreft het aangiftegedrag van slachtoffers.

Hoofdvraag 1: het inzicht in cybercrime

a. Als gevolg waarvan blijft het zo lastig om inzicht te geven in aard en omvang van cybercrime?
b. Welke alternatieve wegen zijn denkbaar om tot dit inzicht te komen zonder herhaling van zetten?
c. Wat vraagt het aan condities om deze alternatieve wegen in te slaan?

Indien deze samengestelde hoofdvraag positief kan worden beantwoord komt uiteraard direct een aantal subvragen naar boven. Zoals (niet limitatief):

- Wat is de aard en omvang en het (maatschappelijk) effect?
- Met welke frequentie, welke omvang en bij wie komen deze voor?
- Wie doet wat bij de aanpak hiervan?
- Welke knelpunten worden door wie bij deze aanpak ervaren?
- Welke trends worden waargenomen? (techniek, criminaliteit, organisatie)

Hoofdvraag 2: de noodzaak tot aanpak

a. Dient zich nu reeds een noodzaak aan om cybercrime aan te pakken, ook al ontbreekt het nog aan voldoende inzicht?
b. Bij wie bestaat het gevoel van die noodzaak?

c. Om welk type aanpak vraagt die noodzaak?
d. Bij wie bestaat de behoefte voor dat type aanpak?
e. In hoeverre is die behoefte eenduidig?
f. Waarop is de behoefte gebaseerd?

Hoofdvraag 3: het ontwerp van een aanpak

a. Welke instituties vervullen al bepaalde functies die (kunnen) voorzien in de behoefte?
b. Welke witte vlekken blijven er over?
c. In hoeverre kunnen die door bestaande instituties worden ingevuld?
d. Blijft er nog iets over voor noodzakelijke 'nieuwbouw' (qua beleid, werkwijze en organisatie) en hoe zou die eruit moeten zien? Met als specifiek aandachtsgebied binnen deze algemeen vraagstelling: op welke wijze kunnen het Openbaar Ministerie en de Nederlandse politie voorzien in de aanpak van die vormen van ICT-criminaliteit waarvan de exclusiviteit en bijzonderheid ervan een bovenregionale c.q. (inter-) nationale aanpak rechtvaardigt?

2.4 Uitgangspunten

De keuze voor een aanpak is niet willekeurig. Het contingentieprincipe zegt dat wil een aanpak succesvol zijn, die dient aan te sluiten bij de specifieke context waarop de aanpak zich richt. Zo is de probleemstelling te vertalen in een aantal uitgangspunten waaraan een aanpak moet voldoen. Die uitgangspunten vormen als het ware de kwaliteitscriteria of in organisatiekundige termen de ontwerpparameters. Het bijzondere aan de uitgangspunten is dat ze niet alleen eisen stellen aan het organisatiekundige ontwerp van een oplossing, maar ook aan de wijze waarop die aanpak wordt geïmplementeerd. Ook het veranderkundig ontwerp dient zich tot de uitgangspunten te verhouden.

Van buiten naar binnen (vraaggericht i.p.v. aanbodgericht)

Veel van de huidige aandacht gericht op de bestrijding van cybercrime is niet gebaseerd op inzicht in de daadwerkelijke problematiek, of inzicht in de belangen van degenen die bij die problematiek zijn betrokken. Wil een aanpak succes hebben, dan dient die aan te grijpen op onderliggende vraagstukken. Ontbreekt het zicht daarop, dan moet de aanpak dat mede genereren. Alle voorstellen voor verbetering van de bestrijding van cybercrime dienen hun legitimatie te ontlenen aan 'buiten', of anders gezegd: aan wat er in de samenleving speelt en nodig is. Een projectvoorstel of activiteit is alleen wenselijk wanneer het ook daadwerkelijk voorziet in, en bijdraagt aan, een externe behoefte. In zijn ultieme vorm bestaat die behoefte uit meer veiligheid voor de burger en het bedrijfsleven.

Er is niet één oorzaak en dus ook niet één oplossing

De aandacht voor cybercrime is niet vanzelfsprekend. Dat is immers één van de redenen waarom projecten als het NHTCC en het NPAC zijn aangegaan. Men mag aannemen dat daarvoor een complex van samenhangende factoren verantwoordelijk is en niet slechts één. Dat betekent dat het vraagstuk ook niet zal zijn opgelost met één of enkele oplossingsrichtingen. Meerdere zaken zullen gelijktijdig moeten worden aangepakt om tot

beïnvloeding te komen.

De verantwoordelijkheid op de juiste plaats

In relatie tot lastige vraagstukken is men altijd blij wanneer iemand anders zich over dat vraagstuk ontfermt en zich er verantwoordelijk voor maakt. Projecten als het NPAC en het NHTCC moeten evenals hun opvolgers, alert zijn op dit verschijnsel, en vraagstukken niet over nemen van regulier verantwoordelijken.

Consistentie tussen het inhoudelijke thema en de aanpak

Een snelle omgeving als die waarin cybercrime zich voordoet en van gedaante en van medium wisselt, vraagt om een benadering die met die wisseling kan omgaan en er op is gebouwd. Een standaard aanpak met in serie geschakelde activiteiten past daar minder bij. Parallelschakeling van activiteiten moet het uitgangspunt zijn, daarbij gebruik makend van de dynamiek in de markt en die vervolgens ook voedend. Resultaten komen niet pas aan het eind van projecten beschikbaar maar ontstaan tussentijds. Om ze vervolgens werkende weg te vervolmaken met behulp van het voortschrijdend inzicht.

Dicht aansluiten op belangen en belanghebbenden

Omdat cybercrime zich afspeelt in veel verschillende sectoren en branches, loopt men bij de bestrijding per definitie aan tegen uiteenlopende belangen. In plaats van de verschillende belangen aan elkaar ondergeschikt te maken of te vervangen door een abstract belang waarin een ieder zich altijd kan vinden, worden de verschillende belangen gelegitimeerd en blijven ze zo lang mogelijk naast elkaar bestaan. Dat betekent dat de bestrijding van cybercrime voor elk van de betrokken wat moet opleveren wil men hen bereid vinden om aan die bestrijding mee te werken. Het basisprincipe dat ten grondslag ligt aan succesvolle publiekprivate samenwerking is ruil.

Ontwikkeling en implementatie gelijktijdig met elkaar op laten trekken

Waar het fundamentele inzicht in aard en omvang van cybercrime ontbreekt en men ook niet met de armen over elkaar kan afwachten, is het van belang te kiezen voor een traject waarin ontwikkeling en implementatie met elkaar optrekken. Zodat er aan de ene kant daadwerkelijk actie wordt ondernomen, maar ook nog ten tijde van de ontwikkeling van de bestrijding kan worden bijgestuurd. Een bijkomend voordeel van het gelijktijdig laten verlopen van ontwikkeling en implementatie, is dat de implementatie-inspanningen worden uitgesmeerd in de tijd, in plaats dat deze na afloop van een ontwikkeltraject in één keer in haar volle omvang ter hand moeten worden genomen. In dat laatste geval moet het veld in korte tijd veel capaciteit vrijmaken en is er minder tijd beschikbaar voor het inleven in het transformatieproces dat tot de te implementeren voorstellen heeft geleid.

Gebruik maken van wat al in de goede richting gaat

Er gebeurt van alles op het terrein van cybercrime. Vaak zijn verschillende activiteiten vanuit verschillende plaatsen en verschillende actoren in gang gezet. Men kan vervolgens proberen dat allemaal op één lijn te krijgen maar dat is geen eenvoudige opgave. Parallelle coördinatie waarin gebruik gemaakt wordt van wat er allemaal gebeurt, om het vervolgens te leiden in de gewenste richting ligt meer voor de hand. Verschillende lopende projecten zullen zonder het altijd van elkaar door te hebben, bijdragen aan een gezamenlijk effect. Wat in de goede richting gaat wordt gefaciliteerd, bij voorkeur zonder zware coördinatie.

Aaneenschakeling van experimenten

Daar waar een aantal inzichten ontbreekt, is het verstandig om alvorens tot ingrijpende keuzes over te gaan te werken met experimenten. In een relatief kleinschalige omgeving kunnen gemakkelijk effecten worden verkend en bestudeerd. Experimenten kosten niet veel geld en kunnen snel worden gerealiseerd. Blijken ze te werken, dan doen ze het heel goed als generatoren van goodwill, financiën en draagvlak.

2.5 Conclusie

De probleemstelling rond de bestrijding van cybercrime is complex. Het risico van die complexiteit is dat ze alleen nog interessant is voor een aantal ingewijde professionals die trachten de rest van de wereld te laten inzien dat er zich pal onder hun neus ernstige dingen afspelen. Ondertussen moeten die professionals, tot hun eigen frustratie, tot op heden het antwoord schuldig blijven op de vraag wat die ernstige dingen dan zijn. Professionals zullen het gebrek aan dat inzicht vervolgens weer wijten aan een niet-coöperatieve en onkundige omgeving, waarmee de vicieuze cirkel rond is.

Ook al is het inzicht gebrekkig in de cyberproblematiek en de mate waarin de samenleving daarvan het slachtoffer is, het is ook weer niet zo dat er helemaal niets bekend is. Uit het NHTCC-project blijkt dat dagelijks vele cybercrime-incidenten plaatsvinden. Die worden niet allemaal gemeld, maar als iedereen alleen al afgaat op de frequentie waarmee de eigen pc van buiten wordt belaagd, dan kan men gevoeglijk aannemen dat er iets aan de hand is. Inmiddels is de probleemstelling wel duidelijk. Het lijkt ernstig en toch weten we niet hoe ernstig het is. Daar zijn op zichzelf ook al weer vele rapporten over geschreven. Omdat men steevast begint met vast te stellen dat het inhoudelijke vraagstuk qua aard en omvang niet bekend is, vallen aanbevelingen daarna in feite in een vacuüm. Niet wetende of ze aangrijpen op een vraagstuk, wordt er iets gedaan omdat niet kan worden afgewacht en er vanuit gegaan wordt dat het zal helpen. Maar waarbij?

Hoofdstuk 3 Ontwerpscenario's

De organisatie van de aanpak van cybercrime kan langs verschillende ontwerpscenario's plaatsvinden. Dit hoofdstuk beschrijft vier hoofdvormen, elk met hun eigen verschijningsvorm en de bijbehorende voor- en nadelen. Na een weging van de argumenten voor en tegen wordt per scenario de mate van wenselijkheid geschetst. Het hoofdstuk eindigt met een onderlinge vergelijking van de conclusies van de scenario's en een onderbouwde aanbeveling voor wat betreft de scenariokeuze voor het ontwerp van een Nationale Infrastructuur voor de aanpak van cybercrime.

3.1 Vier ontwerpscenario's

Ook als men overtuigd is van de probleemstelling en van de noodzaak dat aan cybercrime iets moet worden gedaan, dan nog kan men van mening verschillen over de manier waarop. De in het voorgaande hoofdstuk beschreven uitgangspunten zijn vergelijkbaar met een notenschrift: ze zijn onderling op verschillende manieren te combineren. Die combinaties werken niet alleen door op het inhoudelijk ontwerp van een landelijke aanpak gericht op het tegengaan van cybercrime, maar ook op de wijze waarop dat ontwerp wordt gerealiseerd. Rond de organisatiekundige (het ontwerp) en de veranderkundige (de realisatie) consequenties van de te ontwerpen aanpak zijn verschillende ontwerpscenario's geconstrueerd. Ze zijn te zien als alternatieven waaruit gekozen kan worden. Maar aan de andere kant betekent de keuze voor het ene soms ook automatisch een keuze voor het andere. Geen van de scenario's kent alleen maar voordelen; nadelen krijgt men bij iedere keuze op de koop toe.

De ontwerpscenario's zijn theoretisch wel te onderscheiden maar in de praktijk slechts beperkt van elkaar te scheiden. Ze worden in dit hoofdstuk geïntroduceerd om snel dilemma's te kunnen detecteren. De uitwerking in ontwerpscenario's draagt er mede aan bij dat besluitvorming evenwichtig kan plaatsvinden met inachtneming van alternatieven met niet alleen voordelen maar ook nadelen. Overigens ook met als doel dat niet alleen wordt gekozen voor veilige oplossingen waaraan niemand zich een buil kan vallen, die weinig ambitie uitstralen, en meer lijken te worden ingegeven door de wens van politieke rust, dan om hun bijdrage aan de bestrijding van cybercrime.

Vier ontwerpscenario's worden uitgewerkt:
- scenario 1: laten leiden door autonome ontwikkelingen;
- scenario 2: het ontwerp van losstaande oplossingen;
- scenario 3: het ontwerp van integrale oplossingen;
- scenario 4: nieuw ontwerp van scratch af aan.

De verschijningsvormen waaraan het scenario, als het zich in de praktijk voordoet, kan worden herkend, worden beschreven. De wenselijkheid van het scenario voor de bestrijding van cybercrime wordt verkend middels

argumenten pro en contra. In een afsluitende paragraaf worden de argumenten tegen elkaar afgewogen.

3.2 Scenario 1: laten leiden door autonome ontwikkelingen

Het eerste scenario gaat er van uit dat de bestrijding van cybercrime zich laat leiden door autonome ontwikkelingen. Dit is een ontwerpbenadering waarbij de huidige incrementele wijze van werken gewoon wordt voortgezet. Dus zonder nadrukkelijk ingrijpen en zonder centrale sturing. Dit is een *reactief* scenario waarin men reageert op hetgeen zich min of meer toevallig voordoet aan positieve en negatieve gebeurtenissen. Er is in dit scenario geen eenduidig samenwerkingsverband, maar verschillende actoren met hun eigen belangen en daarop al dan niet gebaseerde afzonderlijke acties. Via incrementele stappen wordt door iedereen zelfstandig meer of minder aan de bestrijding van cybercrime gedaan. Het ontwerpproces is niet centraal geregisseerd: het is gefragmenteerd en toevallig.

Scenariokenmerken

Het eerste scenario lijkt op continuering van de huidige situatie. Wordt het stilzwijgend gevolgd, dan betekent dit bijvoorbeeld voor de opsporing dat naar verwachting de aanpak van cybercrime als nationale functie wordt ondergebracht bij het KLPD. De vervolging wordt in het verlengde daarvan uitgevoerd door het Landelijk Parket van het openbaar Ministerie. Voor de meeste cybercrime gerelateerde delicten zal gelden dat ze meer als methode interessant zijn (vanwege het digitale opsporen) dan als zelfstandig strafbaar feit.

Incidenten van verscheidene aard, variërend van een grote phishing-aanval tot een terroristische aanslag, zullen naar verwachting bepalend zijn voor de verdere ontwikkelingen van de diverse spelers. Komt er een belangrijk strafbaar feit aan het licht waarbij internet wordt gebruikt om toegang te geven en uit te wisselen, zoals bijvoorbeeld en kinderpornozaak, dan krijgt dat prioriteit.
GOVCERT zal blijven werken voor de overheid. Er komt een opvolging van het programma KWINT, waarin overheid en bedrijfsleven samenwerken om de kwetsbaarheid van het internet aan te pakken. Het bedrijfsleven houdt de zaken op orde. Informatie wordt gedeeld zodra men daartoe behoefte heeft en partijen hebben op basis van hun eigen overwegingen contacten met door hen zelf geselecteerde anderen. De marktwerking is bepalend evenals het historisch verloop der dingen. Witte vlekken neemt men voor lief als geen van de partijen zich opwerpt om zich erover te ontfermen.

Argumenten pro

Er zijn in dit scenario geen ingrijpende politieke beslissingen nodig. Departementen blijven gewoon doorgaan in de lijn van de huidige activiteiten. Er behoeft geen extra financiële inspanning geleverd te worden. Er wordt steeds op tijd ingegrepen, vlak voordat een situatie onbeheersbaar wordt. Het kan daarom wel een effectieve strategie zijn.

Argumenten contra

De aanpak van cybercrime ontwikkelt zich ongeregisseerd. De beheersing is daarmee in dit scenario minimaal. Er bestaat zodoende het risico van achter de feiten aanlopen: er gebeurt iets en vervolgens organiseert men zich

op het gebeurde, een sterk incrementele en incidentgestuurde benadering. Met als risico dat men een keer echt te laat is. Witte vlekken zullen alleen worden ingevuld als er ergens iets is mis gegaan. Publiek-private samenwerking zal ad hoc en beperkt tot stand komen. Kans op overlap en wellicht competitie tussen diverse spelers is groot. In geval van crisis is het risico op chaotische reacties en het ontbreken van eenduidige commandostructuren reëel. Ook het risico van onbedoelde verergering van het vraagstuk door gebrek aan afstemming ligt op de loer. Mogelijkheden om via een integrale aanpak cybercrime te voorkomen, te stoppen, op te sporen of te vervolgen worden slechts spaarzaam benut. Internationale afstemming zal slechts sectorgeoriënteerd plaatsvinden, voor zover er sprake is van een Nederlands equivalent van de buitenlandse organisaties. Bestaat deze niet, dan zal Nederland vanuit een internationale context een weinig waardevolle samenwerkingspartner lijken.

Conclusie

Met de keuze voor een NHTCC- en NPAC-project lijkt de waarschijnlijkheid dat dit eerste scenario zich voordoet nu al te zijn afgenomen. Wenselijk is het eerste scenario niet. Voorkomen en anticiperen verdient sterk de voorkeur boven achteraf te moeten repareren.

Overigens gaat achter het scenario een gedachtegang schuil die met name veranderkundig van grote betekenis is. In tijden van betrekkelijk rust waarin het veiligheidsrisico als laag wordt beleefd, bestaat de neiging om weinig ingrijpende maatregelen te nemen. Er is immers geen gevaar. De urgentiebeleving is in dat geval laag, waardoor ook preparatieactiviteiten op geringe steun kunnen rekenen. Zodra er echter wel iets gebeurt, dan moet er ook per omgaande actie worden ondernomen. Vaak is er dan geen tijd om daar goed over na te denken en de consequenties in brede samenhang te overzien. De waarschijnlijkheid dat dit verschijnsel ook speelt in de sfeer van cybercrime is groot. Dat betekent dat plannen waarvoor de tijd in periodes van relatieve beleidsrust niet rijp lijkt te zijn, grote kans van slagen hebben wanneer zich een concreet grootschalig incident voordoet. Veranderkundig kan van dit incrementele principe gebruik worden gemaakt door plannen reeds klaar te hebben, en in te dienen op het moment dat de gelegenheid zich voordoet.

3.3 Scenario 2: het ontwerp van losstaande oplossingen

In academische termen zou het tweede scenario ook de ‘*niet-integrale ontwerpbenadering*’ kunnen worden genoemd. De autonome ontwikkelingen van cybercrime worden in dit scenario niet afgewacht. Er wordt gestuurd, maar dan op het tot stand brengen van op zichzelf staande oplossingen, zonder eisen te stellen aan de integrale samenhang. Als die samenhang er al is dan berust ze op toeval. Het ontwerp bestaat in dit scenario uit een optelsom van actoren die zich met bepaalde functies bezighouden.

Scenariokenmerken

Witte vlekken worden opgelost door middel van ‘inbreiding’: zoveel mogelijk bestaande clubs krijgen er taken bij totdat de vlekken zijn ingevuld. Tussen de bestaande clubs worden geen stevige verbanden gekweekt. Het integrale staat niet voorop maar het afdekken van witte vlekken. Iedereen doet zijn eigen ding. Versnippering is niet erg, mits alles maar door tenminste één snipper wordt afgedekt. Dit scenario lijdt niet tot een afzonderlijk

politieteam voor de bestrijding van cybercrime, want de politie heeft immers al digitale opsporingseenheden.

Naast de ontwikkeling van ‘inbreiding’ kan er bij dit scenario ook sprake zijn van een uitbreidingsvariant. In dat geval worden witte vlekken niet opgelost met bestaande, maar met nieuw op te richten organisaties. De versnippering neemt toe, maar dat past in deze variant. Er worden nog steeds geen onderlinge verbanden gekweekt. Uitgangspunt is het bedekken van de witte vlekken. Er komt volgens deze subvariant een afzonderlijk politieteam voor met name grootschalige onderzoeken.
Naast GOVCERT dat is gericht op de overheid, komt er een zelfstandig equivalent dat zich richt op de private sector. Beide instanties doen hetzelfde, maar voor verschillende markten.

Argumenten pro

Doordat bij dit scenario de aanpak van cybercrime tamelijk enkelvoudig wordt benaderd, zullen zowel inbreidingen als uitbreidingen relatief snel kunnen worden gerealiseerd. De witte vlekken worden onderkend en van een organisatie voorzien die zich er over ontfermd. Zeker wanneer internationale ontwikkelingen nauwgezet worden gevolgd en waarschijnlijk gekopieerd, voldoen de Nederlandse instellingen aan het verwachtingspatroon van haar buitenlandse tegenhangers. Kosten van afstemming en coördinatie zullen beperkt blijven.

Argumenten contra

De complexiteit, reikwijdte en dynamiek van cybercrime maken het waarschijnlijk dat zowel bij in- als uitbreiding sprake zal zijn van doublures in bepaalde functies tussen instellingen. Voor zover deze onzichtbaar blijven is er alleen sprake van verkwiste middelen. Het is denkbaar dat sommige vormen van functieoverlap tussen organisaties zullen leiden tot een ongewenste competitie op het betreffende terrein. De negatieve effecten hiervan zullen met name op het niet samenwerken en/of informatie delen betrekking hebben. Zeker wanneer het kernspelers betreft kunnen mogelijk kansrijke samenwerkingsvormen onbenut blijven. Mochten (publieke/private) partijen elkaar vinden voor samenwerking op het gebied van voorkomen, stoppen of vervolgen dan zullen deze naar verwachting slechts bilateraal van aard zijn. Zeker bij informatie-uitwisseling zal de totstandkoming vanwege (gezond) wantrouwen moeizaam zijn. Door het ontbreken van een generiek principe van ruilvoeten, zullen de spreekwoordelijke transactiekosten van een ruil hoog zijn. Bij het bedekken van witte vlekken zal alleen gekeken worden naar de ontbrekende functies die op basis van bestaande problematiek bekend zijn. Mogelijkheden om op basis van overleg tussen meer partijen in opkomst zijnde witte vlekken in een vroegtijdig stadium te ontdekken zijn beperkt door het gebrek aan samenwerking.

Conclusie

Goed beschouwd kunnen de ontwikkelingen van de laatste twaalf maanden geplaatst worden binnen de context van dit ontwerpscenario. De originele taakdoelstelling van het project NHTCC kent een grote mate van overlap met de ambitie van het NPAC en de feitelijke taakuitvoering van GOVCERT. Uit deze gezamenlijke notitie van beide projecten die gerealiseerd is in nauwe samenwerking met GOVCERT, blijkt wel dat deze spelers de noodzaak tot een integrale benadering onderkennen. Vanwege de notie dat brede samenwerking de sleutel kan vormen voor een adequate bestrijding van het dynamische vraagstuk cybercrime, brengt dit scenario een te groot afbreukrisico met zich mee voor de beoogde samenwerking. Het scenario wordt dan ook logischerwijs niet als

het meest wenselijk beschouwd.

3.4 Scenario 3: het ontwerp van samenhangende oplossingen

De samenhang staat binnen deze derde ontwerpbenadering centraal. De landelijke aanpak bestaat uit een samenhangend geheel van op elkaar afgestemde functionaliteiten en dito actoren. Uitgegaan wordt van bestaande structuren die aan elkaar worden geknoopt door middel van een soort ringleiding. Samenwerking en informatiedeling staan aan de basis van dit ontwerpscenario.

Scenariokenmerken

Net als bij het vorige scenario gaat deze optie uit van bestaande structuren. Via hetzelfde principe van 'inbreiding' worden hun functies uitgebreid totdat ze samen de witte vlekken bedekken. Er komen in principe geen nieuwe structuren bij. GOVCERT bijvoorbeeld, verleent in deze variant dus ook diensten aan de private sector. In tegenstelling tot het tweede scenario, worden in deze variant wel sterke onderlinge banden gekweekt. Er vindt nauwe afstemming van taken en verantwoordelijkheden plaats. Informatiedeling en een meer generieke ruilsystematiek gelden als basisprincipes voor de brede samenwerking binnen de infrastructuur. Nieuwe organisaties die willen aanhaken krijgen algemene spelregels voorgeschoteld en draaien vervolgens mee binnen de infrastructuur. Voor sommige witte vlekken kan gelden dat er geen bestaande organisatie is voor wie inbreiding richting de witte vlek een logische keuze is. Vandaar dat voor sommige witte vlekken uitbreiding in de vorm van nieuw op te zetten organisaties mogelijk is. Volgens deze benadering ontstaat er dan een samenhangende *Nationale Infrastructuur* die bestaat uit op elkaar betrokken bestaande instituties, plus eventueel een aantal nieuwe. De nieuwe ontstaan op die plaatsen waar lastig te bereiken witte vlekken bestaan c.q. een specifieke deskundigheid is vereist.

Argumenten pro

Doordat de doorontwikkeling van de cybercrime bestrijdingsfunctie op basis van brede afstemming plaatsvindt, is de kans op doublures van functies minimaal. Het brede perspectief op het vraagstuk maakt de kans dat huidige en toekomstige witte vlekken door geen van de bestaande of nieuwe partijen afgedekt wordt, eveneens minimaal. Het streven naar samenwerking en informatiedeling op basis van natuurlijke ruilverhoudingen, optimaliseert de mogelijkheden om cybercrime integraal en blijvend succesvol te bestrijden. Op het gebied van vervolging kan de betrokkenheid van specialistische medewerkers van aangesloten organisaties bij bepaalde opsporingsonderzoeken nadrukkelijk meerwaarde bieden.

Argumenten contra

Achter dit ontwerpscenario ligt de veronderstelling dat een belangrijk deel van de voor de bestrijding van cybercrime benodigde functies al binnen bestaande instituties is georganiseerd. Op het moment dat zou blijken dat dit niet het geval is, kan het afstemmen van de doorontwikkeling richting nieuwe functies binnen de infrastructuur een langdurig en kostbaar traject zijn.

Conclusie

Vanuit het perspectief van de bestrijding van cybercrime lijkt dit scenario een snelle en doeltreffende aanpak van het vraagstuk. Echter, hoe groot en wezenlijk het vraagstuk op dit moment is, valt met weinig zekerheid te zeggen. Daardoor is er ook slechts beperkt zicht op de functies van de infrastructuur, en de mate waarin deze binnen de infrastructuur aanwezig zouden moeten zijn. Over de benodigde in- of uitbreiding van bestaande spelers valt derhalve op dit moment ook nog weinig te zeggen. Dit scenario verdient daarom op zichzelf een sterke voorkeur, mits binnen afzienbare tijd duidelijk wordt op basis van welke vraag uit de maatschappij de infrastructuur als hulpmiddel ingericht zou moeten worden. In het verlengde daarvan ligt het vraagstuk wat betreft de mate waarin deze gewenste functies vanuit bestaande organisaties kunnen worden ingevuld.

3.5 Scenario 4: nieuw ontwerp van scratch af aan

Net als scenario 3, is ook het vierde scenario een voorbeeld van de samenhangende ontwerpbenadering. Alleen wordt uitgegaan van een blanco-situatie die volgens het *zero-base* principe vanaf nul wordt opgebouwd. Op die manier kan de meest wenselijke situatie worden gerealiseerd, zonder vast te zitten aan historisch gegroeide suboptimalisatie. In zijn uiterste consequentie betekent dit vierde scenario dat er constant wordt vernieuwd. Dus niet eenmalig ter invulling van een nul-situatie die, nadat ze is ingevuld, vervolgens geen nul-situatie meer is.

Scenariokenmerken

Consequente uitvoering van dit scenario betekent dat men zich volstrekt laat leiden door ontwikkelingen die het cybercrimevraagstuk doormaakt. Er wordt gebouwd naar behoefte en er wordt ook afgebroken naar behoefte. Het oprichten van vaste instituties voor de eeuwigheid past niet in dit scenario. Een steeds wisselende projectorganisatie met flying squads en afgeronde en nieuwe activiteiten is eerder het gevolg. Het zich snel aanpassen aan wisselende verschijningsvormen van cybercrime is een belangrijk kenmerk van het werken volgens dit scenario. In plaats van instituties, is de vraag maatgevend. Die vraag vertaalt zich in al dan niet tijdelijke functies en in informatiedeling. Er wordt in dit scenario geen onderscheid gemaakt tussen overheid en niet-overheid. Een GOVCERT bijvoorbeeld werkt op basis van (voorzienbare) problemen en niet volgens wie er mee te maken kan krijgen. Als organisatie zal GOVCERT ook minder herkenbaar zijn. Er is veel eerder sprake van, naar gelang het vraagstuk, steeds wisselende coalities van deskundigheden.

Argumenten pro

Het vierde scenario past bij het wisselende karakter qua verschijningsvormen van cybercrime. De inhoud van het werk staat centraal, zonder te worden verstoord door allerlei organisatorische kwesties. Die zijn volstrekt van ondergeschikt belang. Men heeft geen last van een gegroeide situatie, waarbij incrementeel met steeds meer uitstulpingen doorontwikkeld wordt. Een dergelijke situatie kan ook niet ontstaan omdat het scenario institutionalisering niet als doel heeft. Inspanningen om bestaande organisaties in te passen binnen de integrale infrastructuur zijn overbodig, ook na verloop van tijd. Want er ontstaan geen instituties, maar alleen coalities rond deskundigheid, ervaring en informatie. Flexibiliteit en het snel inspelen op vraagstukken en de plaats waar ze zich voordoen, zijn de belangrijkste voordelen van dit scenario.

Argumenten contra

Het belangrijkste tegenargument van dit scenario is dat er feitelijk al instituties zijn die zich geheel of gedeeltelijk met de bestrijding van cybercrime bezighouden. Er is geen blanco-situatie. Een tweede tegenargument is dat het maar zeer de vraag is of cybercrime zo snel wisselt dat het steeds op een andere wijze met behulp van andere deskundigheden moet worden aangepakt. Het is maar de vraag of een 'koortsachtige' wijze van organiseren nodig is. Wellicht borduren ook cybercrime-bedreigingen voort op bestaande concepten en zijn ze daarvan hooguit een variant. Daarnaast zorgt de snelle wisseling van organisatievormen wellicht voor verwarring bij de afnemers, die telkens zullen moeten zoeken naar de juiste benadering van hun wisselende problemen. Een nieuw probleem betekent immers ook een nieuwe aanpak.

Conclusie

De huidige NPAC-aanpak heeft kenmerken in zich van dit scenario. Niet zozeer vanuit de overtuiging dat het cybercrimevraagstuk zo snel van gedaante wisselt dat er steeds een nieuwe aanpak en een nieuw arsenaal aan vaardigheden moet worden gemobiliseerd, maar meer vanuit de achtergrond dat er onvoldoende bekend is van cybercrime (aard en omvang) om al tot zinvolle institutionalisering over te gaan. De vraag welke instituties dat vooral zouden kunnen zijn en met welke functies is theoretisch wel te beantwoorden, maar wordt nog onvoldoende onderbouwd door de praktijk. In dit scenario zou moeten worden gestart met een programma bestaande uit een verzameling van functies en vaardigheden met behulp waarvan die praktijk wordt onderzocht. Daarbij worden de grenzen qua opdracht en taak van bestaande instituties overschreden en worden ze op basis van hun deskundigheid aan sectoren en problemen gekoppeld.

Concluderend lijkt het vierde scenario een goede manier om te onderzoeken op welke wijze men zich wel en niet moet organiseren op het verschijnsel cybercrime. Gaandeweg de programmatische uitvoering van dit scenario kan blijken dat binnen de bestaande instituties niet datgene geregeld is dat de maatschappij op het gebied van de aanpak van cybercrime vraagt. Zoals eerder aangegeven ontbreekt echter momenteel inzicht in deze specifieke vraagkant. Mocht op enig moment blijken dat er een grote mismatch bestaat tussen de binnen de bestaande instituties aanwezige functies en de door de samenleving gevraagde, dan komt pregnant naar boven dat sanering en wellicht nieuwbouw nodig is. Er is dan wel moed voor nodig om binnen de bestaande instituties in te grijpen. Voordeel van dit scenario is dat het niet alleen informeert naar 'hoe heeft het zo kunnen komen', maar ook vraagt om kritisch te kijken naar de huidige institutionele vormgeving.

Het zal niet meevallen om zich daadwerkelijk permanent op basis van de uitgangspunten van dit vierde scenario te organiseren. Ook als inhoudelijk en bedrijfskundig gezien een constante zero-based benadering wenselijk zou zijn, dan verhoudt een voortdurende wisseling zich moeizaam tot de wens van bijvoorbeeld eenduidige politieke verantwoordelijkheid en duidelijkheid over de vraag wie waarvoor verantwoordelijk moet worden gesteld (bij wie moet de probleemhebber aankloppen?). Het voorlopig als geïntegreerd NPAC- en NHTCC-project werken volgens een programma dat kenmerken vertoont van dit vierde scenario, zal ongetwijfeld ook veel ervaring opleveren met wat aan de ene kant nodig en aan de andere kant haalbaar is. Het vierde scenario moet gezien worden als ontwikkelscenario.

3.6 Conclusie

Het ontstaan van de projecten NPAC en NHTCC is op zichzelf een illustratie dat het volgen van het eerste scenario (ongewijzigd beleid) niet wordt onderschreven. Het eerste scenario is te risicovol want het zal maar gebeuren dat men met het reactieve optreden echt te laat is, met mogelijk grote gevolgen. Voorkomen is beter dan genezen, past als motto in dit verband. Maar het eerste scenario levert ook een belangrijk veranderkundig uitgangspunt op: dat juist onder de druk van bepaalde niet voorziene en onverhoopte gebeurtenissen, bepaalde wenselijke beleidskeuzen gemakkelijker en sneller tot stand komen.

Het belangrijkste probleem dat uit de scenario-beschrijvingen naar voren komt, is het gebrek aan inzicht in de feitelijke aard en omvang van cybercrime en dan met name de effecten daarvan. Als men niet weet hoe erg de problematiek is, dan is een ontwerpvraag voor een mogelijke aanpak al helemaal lastig. In algemene zin verdienen integrale benaderingen de voorkeur boven niet integrale, en wil men zo min mogelijk in het bereiken van ideale oplossingen geblokkeerd worden door een gegroeide situatie. Maar op die algemene, normatieve, uitgangspunten kan men geen Nationale Infrastructuur ontwerpen. Een door het geïntegreerde NPAC-NHTCC-project uit te voeren programma zal hiermee sterk rekening moeten houden. Te snel aandringen op institutionalisering zonder dat duidelijk is waarop dat precies het antwoord zou moeten zijn is niet wenselijk. Het volgen van een uit de geschetste vier scenario's samengesteld scenario, ligt daarom vooralsnog het meest voor de hand met als belangrijkste ingrediënten:

- meeliften op de actualiteit met bepaalde wenselijke beleidskeuzen (scenario 1);
- witte vlekken die zich vrij zelfstandig voordoen zoveel mogelijke bedienen door eenvoudige taakwijzigingen van zoveel mogelijk bestaande instituties (scenario 2);
- het ontwerpen van samenhang tot norm verheffen voor die aspecten van de cybercrime waarvoor het noodzakelijk is (scenario 3);
- een onderzoeksprogramma in te richten dat gebruik maakt van de vaardigheden en deskundigheden die er zijn om meer zicht te krijgen op aard en omvang van het vraagstuk en degene die dat ervaart (scenario 4).

Hoofdstuk 4 Ontwerp Nationale Infrastructuur Bestrijding Cybercrime

De conclusies uit de diverse scenario's, afgezet tegen de maatschappelijke en historische context, en geplaatst binnen de ontwikkelingen in het veld leiden tot een gezamenlijk ontwerp van de projecten NPAC en NHTCC. Het ontwerp heeft het karakter van geïntegreerde aanbevelingen. Het is een samenhangend concept. Een Nationale Infrastructuur gericht op de bestrijding van cybercrime is wenselijk. Dat klinkt als heel zwaar en gecompliceerd, maar rechtdoende aan de in hoofdstuk 2 geïntroduceerde uitgangspunten wordt een basaal concept neergezet. Dat concept wordt in dit hoofdstuk uiteengezet, om vervolgens aan het eind terug te blikken op de mate waarin het concept tegemoet komt aan de doelstelling en vraagstelling uit het eerder aangehaalde hoofdstuk 2.

4.1 Meest bepalende ontwerpvraagstukken

Tal van ontwerpvraagstukken kunnen worden afgeleid uit de oorspronkelijke probleemstelling, maar de vraagstukken waren niet van gelijke orde. De meest bepalende ontwerpvraagstukken worden aan het begin van dit hoofdstuk geïntroduceerd evenals het type benadering dat voor de oplossing ervan is gekozen. In die zin is het een soort verantwoording van keuzes en aannames die aan de basis liggen van het uiteindelijke ontwerp.

4.1.1 De domeinafbakening

Aan de basis van het ontwerp van oplossingsrichtingen ligt het vraagstuk op welke elementen van cybercrime die oplossingen zich zouden moeten richten. We onderscheiden vier verschijningsvormen van cybercrime die bij elkaar opgeteld het totale terrein bestrijken van wat men onder cybercrime kan verstaan.

1. **Illegale communicatie**. In deze variant bedienen criminelen zich van publieke netwerken voor onderlinge communicatie voor het uitwisselen van strafbare zaken, zoals bijvoorbeeld kinderporno,. Het netwerk als infrastructuur op zich, leidt door deze vorm van communicatie geen schade. Het klinkt wat raar maar in feite wordt het netwerk gebruikt waarvoor het is bedoeld: gegevensuitwisseling.
2. **Inbreuk op de integriteit van gegevensbeheer**. Het netwerk wordt gebruikt om ergens binnen te komen voor het moedwillig beschadigen van gegevens of voor het stelen van gegevens. Het fysieke netwerk als zodanig wordt niet beschadigd en blijft intact. Het netwerk is in dit geval een middel zoals de koevoet een middel is van de klassieke inbreker. In de wetgeving valt dit onder de term computervredebreuk.
3. **Beschadiging van het netwerk**. Niet gegevens op het netwerk zijn het eerste doelwit, maar het netwerk of aangesloten apparatuur zelf. Waardoor die apparatuur bijvoorbeeld niet meer werkt, of werkt volgens de specificaties van degene die inbreuk maakt, zoals in het geval van botnets

Daarnaast is er nog een categorie die hier wel benoemd wordt maar slechts zijdelings aan het onderwerp cybercrime raakt:

4. **legale communicatie voor illegale doeleinden**, waarbij men zich net als in variant 1 als misdadigers bedient van publieke netwerken voor onderlinge communicatie. In feite het doel waarvoor iedere gebruiker zich van het netwerk bedient. Alleen het type van de communicatie verschilt. Bellen via internet, mailen en chatten maar ook het doen van financiële transacties valt onder regulier gebruik, of dat nu door een crimineel of een niet-crimineel plaatsvindt. Kenmerk van regulier gebruik is dat het gebruik van het netwerk op zich zichzelf genomen niet illegaal is, ook al gaat het voor het uitvoeren of bespreken van duistere zaken.

In de eerste plaats is gekozen om de bestrijding van cybercrime betrekking te laten hebben op publieke elektronische netwerken en de daarop aangesloten apparatuur. Bedrijfsinterne netwerken die niet in verbinding staan met de buitenwereld vallen niet onder de scope omdat het cyberspace-karakter ontbreekt. Een keuze die een beperking inhoudt ten opzichte van de in hoofdstuk 2 geïntroduceerde definitie van cybercrime. Volgens die definitie zou iedere misdaad met behulp van (of gericht tegen) informatie- en communicatietechnologie onderwerp van bestrijding dienen te zijn. Dus ook het doorknippen van een kabel tussen de verkeerstoren op Schiphol en de bediening van de lampen op de start- en landingsbanen via het elektronische netwerk. Een en ander laat onverlet dat deze vormen van criminaliteit wel aangepakt zouden kunnen worden door een cybercrime unit bij de politie op basis van een besluit van het OM tot vervolging.

Men kan verschillend oordelen over welke van de vier verschijningsvormen te rekenen tot het aandachtsgebied van de bestrijding van cybercrime. Over de tweede en derde verschijningsvorm bestaat weinig discussie. Anders wordt het bij de vierde en iets minder bij de eerste. In beide gevallen is het netwerk geen doel op zich en wordt het ook niet aangetast. Voor het moment is het voorstel om alle vier verschijningsvormen tot de bestrijding van cybercrime te rekenen. In de maatschappelijke beleving zijn de verschijningsvormen namelijk sterk met elkaar verweven, minimaal al omdat ze allemaal op eenzelfde medium betrekking hebben. Het is ook bijna ondoenlijk om de verschijningsvormen praktisch van elkaar te scheiden in bijvoorbeeld preventieve activiteiten. Ook een argument om alle vier verschijningsvormen als uitgangspunt te nemen voor de bestrijding van cybercrime is dat in een situatie waarin men niet goed weet wat de aard en omvang is in ieder geval moet zorgen dat alle informatie die daarover inzicht zou kunnen geven bij elkaar komt. De praktijk zal dan uitwijzen welke verschijningsvormen zinvol zijn om aangepakt te worden.

Het zou vervolgens de kwaliteit van de Nationale Infrastructuur moeten zijn om te zorgen dat de uiteenlopende informatie op de juiste plaats terecht komt. Een *intern coördinatieprobleem* dus, in plaats van een extern coördinatieprobleem dat door de burger zelf moet worden opgelost door zich te verdiepen in nuancering over bij welke loketten hij of zij waarvoor terecht kan.

De toelichting op de afbakening in deze paragraaf is zuiver begonnen door bedrijfsinterne netwerken niet te rekenen tot het aandachtsgebied cybercrime. Maar wat te doen wanneer als onderdeel van een bedrijfsscan in het

kader van de aanpak van cybercrime wordt gestuit op een intern bedrijfsnetwerk dat niet wordt geback-upt? Volgens de letter zou dat niet tot de scope behoren. Het voorbeeld maakt goed duidelijk dat de domeinkeuze gezien moet worden als een taakessentie waar de aandacht primair naar uitgaat, en niet als een onomstotelijk criterium. Een bedrijfsscan gaat dus gewoon in op alle relevante aspecten (inclusief back-ups, het bewaren daarvan buiten het bedrijf, etc.), wetende dat in de hoofden van mensen sprake is van één type bewustwording.

Tot slot dient er bij de inzet vanuit het afgebakende domein ook rekening te worden houden met wisselende maatschappelijke en politieke verontwaardiging in het verlengde waarvan ook prioriteiten kunnen wisselen. Het is nu eenmaal een feit dat afhankelijk van zich voordoende gebeurtenissen een bepaald inhoudelijk item opeens zeer in de belangstelling kan komen te staan. De infrastructuur die is gericht op de bestrijding van cybercrime zou in staat moeten zijn daarop (tijdelijk) aan te sluiten. Zonder dat er weer een geheel nieuwe institutie uit de grond gestampt moet worden om zich exclusief op een splintervorm van cybercrime te storten.

4.1.2 De procesafbakening

Vertrokken is vanuit het standpunt dat het voor een succesvolle bestrijding van cybercrime is vereist dat alle onderscheiden processtappen worden afgedekt middels actoren en producten. Hoe zwaar die afdekking per processtap moet zijn en feitelijk is, was één van de discussiepunten. Uiteindelijk werden met name als witte vlekken in het cybercrimeproces ervaren: de pro-actie, de preparatie, de signalering (het melden en het doen van aangifte), de opsporing en vervolging (opvolging), en de terugkoppeling naar aangevers. Vooral deze processtappen zouden in een ontwerp voor de bestrijding van cybercrime nadrukkelijker aan bod dienen te komen. Dwars over deze processtappen heen werd vooral als ontwerpvraagstuk gezien de wijze van delen van informatie.

Een volgend ontwerpvraagstuk ging over de vraag welke processtappen wel en welke niet op te nemen in het ontwerp voor de bestrijding van cybercrime. De discussie spitste zich toe op de opvolgingsfase en meer specifiek de opsporing en vervolging. Over de bijdrage van opsporing en vervolging aan de doelstelling als geformuleerd in hoofdstuk 2 wordt verschillend gedacht. Dat verschil in denken wordt niet zozeer principieel ingegeven. Er bestaat in de kring van betrokkenen bij deze notitie een behoorlijke gemeenschappelijkheid over wat de rol van politie en OM zou kunnen zijn. In het recente verleden is er binnen de politie en het OM discussie geweest over de aandacht die de bestrijding van financieel-economische criminaliteit en/of het gebruik van het instrument financieel rechercheren, moest hebben tegenover de meer zichtbare vormen van criminaliteit. Ook nu weer speelt dit aspect: in de altijd krappe capaciteitstoewijzing binnen de politie zijn goede argumenten nodig om cybercrime op hetzelfde niveau te plaatsen als bijvoorbeeld drugssmokkel. Passend binnen de huidige structuur van de politie wordt het uitgangspunt van de Raad van Hoofdcommissarissen, dat de opsporing van ICT-gerelateerde criminaliteit in principe een zaak is voor de regio, qua beginsel onderschreven. Dit betekent niet dat de politie en het OM geen aandacht voor de bestrijding van cybercrime zouden hebben, integendeel: op basis van de ervaringen opgedaan in het project NHTCC is bij het KLPD een voorstel in voorbereiding om, naast de investering in de breedte op basis van het Landelijk Project Digitale Opsporing, een diepte-investering te doen voor de bestrijding van cybercrime op landelijk niveau. Daarbij wordt aandacht gegeven aan die bijzondere en

exclusieve vormen van computergerelateerde criminaliteit die vooralsnog niet op regionaal niveau kunnen worden behandeld. Weliswaar zal hetgeen dat nu bijzonder en exclusief is straks weer min of meer gemeengoed worden, zodat daar geen “exclusieve” voorziening meer voor noodzakelijk is. Daarvoor in de plaats komen dan waarschijnlijk weer andere vormen van ICT-gerelateerde criminaliteit die al dan niet tijdelijk bijzondere expertise en capaciteit vereisen. Een uitgangspunt dat aansluit op de aan het eind van de vorige paragraaf voorspelde wisseling van prioriteiten.

Als ontwerpvraagstuk speelde onder de noemer ‘procesafbakening’ ook hoe moest worden omgegaan met processen die weliswaar door bestaande organisaties worden afgedekt maar dan slechts voor een bepaalde doelgroep. GOVCERT is daarvan het duidelijkste voorbeeld. Het verricht bepaalde functies die deel uitmaken van de bestrijding van cybercrime maar dan sec voor de overheid als doelgroep. Bij de oprichting destijds heeft GOVCERT zich beperkt tot de overheid om geen valse concurrentie te vormen voor private ICT-dienstverleners. In het uiteindelijke ontwerp is dit principe geëerbiedigd. Het concurrentieprobleem is er zelfs in ondervangen door zich juist op die ICT-bedrijven te richten in plaats van er naast te opereren.

4.1.3 De multi-agency-problematiek

Voor het ontwerp is er vanuit gegaan dat de bestrijding van cybercrime per definitie een multi-agency aangelegenheid is: samenwerking tussen verschillende publieke en private partijen, met verschillende rollen en informatieposities, die actief zijn c.q. kunnen worden in verschillende stappen van het bestrijdingproces en in relatie tot verschillende doelgroepen. Op dat punt is het logisch scenario 3 te volgen: het aanbrengen van onderlinge samenhang waarbij zoveel mogelijk gebruik wordt gemaakt van bestaande actoren en structuren.

Met die keuze ligt er ook een lastig ontwerpvraagstuk op tafel dat direct aansluit op het onderdeel uit de probleemstelling van onvoldoende informatie- en kennisdeling. De verschillende actoren die in multi-agencyverband worden geacht samen te werken hebben ieder hun eigen type informatie en verstrekkingsregimes die op die informatie van toepassing zijn. Daardoor kan de één niet zonder meer informatie delen met de ander. Terwijl juist de toegevoegde waarde van gemeenschappelijke bestrijding van cybercrime zou moeten liggen in het op elkaar betrekken van informatie. Over dat uitgangspunt bestaat weinig verschil van mening. De vraag is alleen hoe aan het uitgangspunt invulling te geven met eerbiediging van ieders informatieregime. Het is gelukt om daar een oplossing voor te vinden door het verstrekkingenregime aan te vullen met een ontvangstregime. Hoe dit vorm krijgt zal verder in dit hoofdstuk nader worden toegelicht.

Een tweede ontwerpvraagstuk dat zich aandient wanneer voor het multi-agency principe wordt gekozen is dat van de eindverantwoordelijkheid. De vraag ligt voor hoe de verantwoordelijkheden en bevoegdheden worden belegd wanneer voor een samenhangende (multi-agency) benadering wordt gekozen. Een eerste reactie zou kunnen zijn dat die blijven liggen bij de afzonderlijke partijen. Als eerste stap in een implementatieproces is dat ook denkbaar. Maar naarmate het vertrouwen toeneemt en daadwerkelijk informatie naast elkaar wordt gelegd, ontstaat de facto een soort gemeenschappelijke informatievoorziening. Met als hamvraag wie voor een dergelijke voorziening verantwoordelijk kan worden gesteld. Hoe kan voorkomen worden dat instellingen zich weerhouden

van het geven van informatie, omdat zij er niet meer over gaan en de politiek openheid van zaken kan afdwingen terwijl private partijen dat over hun informatie mogelijk niet willen. Voor dit ontwerp vraagstuk zijn enkele alternatieve oplossingsrichtingen aangedragen, elk met voor- en nadelen.

4.1.4 Positionering ten opzichte van het buitenland

Als laatste vraagstuk dat het ontwerp van de bestrijding van cybercrime heeft beïnvloed, was de vraag naar de status van de Nationale Infrastructuur in relatie tot het buitenland. Wil het buitenland informatie delen dan wil men ook weten met welk type instantie men van doen heeft, met als cruciaal onderscheid het al dan niet zijn van een opsporingsorganisatie. Zowel voor de law-enforcement als voor de internationale CERT-community geldt dat zij het liefst één nationaal aanspreekpunt hebben. Op basis van de huidige ervaringen van GOVCERT blijkt het al dan niet zijn van opsporingsinstantie overigens geen struikelblok voor vergaande internationale uitwisseling van informatie, zolang het maar geen exclusieve opsporingsinformatie betreft. Wel is de vraag gesteld of die uitwisseling voor wat betreft GOVCERT zich qua gebruik van informatie wel mag beperken tot de overheid sec. In deze notitie wordt die beperking losgelaten. Dat leidt binnen het ontwerp van de bestrijding van cybercrime tot hooguit twee informatierelaties met het buitenland op: één op het niveau van de CERTS die loopt via het breder te positioneren GOVCERT, en één op het niveau van HTCC's waar het gaat om specifieke informatie op het vlak van opsporing en vervolging. Voorwaarde voor het functioneren van deze relaties in het kader van het geheel van bestrijdingsactiviteiten is wel dat de informatie bij elkaar terechtkomt. In het geval van integratie van beide typen informatie onder één dienst zou dat zijn gegarandeerd, maar over de effecten van die oplossing wordt verschillend gedacht. De één vindt dat daarmee het huidige wettelijke stelsel voor de organisatie van de opsporing en vervolging wordt aangetast, terwijl de ander vindt dat dit stelsel geen doel op zich mag zijn en ten dienste moet staan van wat in de praktijk wenselijk is.

4.2 Ontwerp voor een Nationale Infrastructuur Bestrijding Cybercrime

4.2.1 Ingrediënten van de Nationale Infrastructuur

De kern van de infrastructuur is dat publiek-private informatie-uitwisseling wordt gerealiseerd. Het primaire doel is niet om een nieuwe organisatie in te richten maar verbindingen te leggen tussen betrokken partijen, zoals bedrijfsleven, GOVCERT, NHTCC en het Meldpunt Cybercrime. Het mobiliseren van het bedrijfsleven gebeurt via het Nationaal Platform Criminaliteitsbeheersing (NPC), waarin overheid en bedrijfsleven samenwerken.

Met de Nationale Infrastructuur ontstaat een ringleiding die bestaande partijen met elkaar verbindt. Dit proces dient geïnitieerd te worden door partijen actief bij elkaar te brengen. Informatie-uitwisseling is een eerste stap in de bestrijding van cybercrime. De daadwerkelijke bestrijding vergt de uitvoering van diverse taken zoals waarschuwen, voorlichten, detecteren, tegenhouden/stoppen en opsporen/vervolgen. De participanten van de Nationale Infrastructuur geven invulling aan de verschillende functies die met deze taken verband houden, welke

verderop in dit hoofdstuk nader besproken worden.

Bovenstaande neemt niet weg dat bepaalde soorten incidenten hun eigen regime kennen. Bij nationale crises coördineert het Nationaal Coördinatie Centrum (NCC), ingeval van terroristische dreigingen heeft de Nationaal Coördinator Terrorismebestrijding (NCTb) een taak, en bij cybercrime waarbij de nationale veiligheid in het geding is, speelt de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) een rol. Bij het ontwikkelen van de Nationale Infrastructuur moet hiermee rekening worden gehouden.

4.2.2 Publiek-privaat samengestelde informatie-uitwisselingstructuur

Naarmate het vertrouwen tussen de deelnemers in de Nationale Infrastructuur groeit, zal informatie en daarmee ook vertrouwelijke informatie uit de vertegenwoordigde sectoren beschikbaar kunnen worden gesteld. De afspraken met deelnemende sectoren over het leveren van informatie en de ruimte om die informatie in bewerkte vorm te mogen doorgeven, worden vastgelegd in een reglement. In situaties die daardoor niet zijn afgedekt, maar die wel om informatieverstrekking vragen (bijvoorbeeld in het geval van zaken van groot maatschappelijk belang) wordt afzonderlijk om toestemming gevraagd aan de organisatie die de informatie heeft geleverd. Behoudens wettelijke verplichting wordt de informatie alleen aan derden verstrekt na toestemming van de eigenaar van de informatie. In die zin werkt de informatie-uitwisselingstructuur als een membraan: doorlatend van buiten naar binnen, maar beperkt doorlatend van binnen naar buiten. De doorlaatbaarheid van het membraan wordt bepaald door het doel dat met de informatie wordt gediend en het verstrekkingenregime dat daarvoor vervolgens geldt[2].

In de Nationale Infrastructuur zal precies uitgewerkt worden hoe informatie-opslag, verwerking en verstrekking plaatsvindt. De bij de gemeenschappelijke informatieuitwisselingstructuur betrokken medewerkers hebben toegang tot de systemen zoals aanwezig en gebruikelijk in hun eigen achterban. Voorlichting en advisering op het gebied van bestrijding, zowel vanuit justitieel als niet-justitieel perspectief, loopt vanuit de hieronder genoemde informatiefuncties.

4.2.3 Functies

Door informatie van verschillende kanten bij elkaar te leggen ontstaan zowel beelden van dreigingen, als oplossingsstrategieën. Daarmee gaat de Nationale Infrastructuur op verschillende manieren aan de slag. Vertaald naar functies levert dat het volgende beeld op:

Aanspreekpunt

Vanuit verschillende invalshoeken is en wordt er in aanspreekpunten op het terrein van cybercrime voorzien. Een gunstige ontwikkeling, maar met mogelijk ook als risico dat het de verschillende partijen bij aanvang nog niet altijd direct duidelijk is waar men waarvoor terecht kan. Het NIBC ondervangt dat probleem en is voor iedereen

[2] Faber, W., A.A.A. van Nunen, Uit onverdachte bron. Evaluatie van de keten ongebruikelijke transacties, WODC, 2004, p. 325

aanspreekbaar. Om vervolgens direct een koppeling te leggen naar de juiste instantie. Waar die ontbreekt, fungeert het NIBC zelf als zodanig.

Het NIBC is aanspreekbaar namens de partijen die met elkaar verantwoordelijk zijn voor het instandhouden van de nationale infrastructuur. Ieder van hen brengt zijn (inter)nationale netwerk in en zorgt waar nodig voor adequate doorverwijzing.

Als er contacten moeten worden gelegd/medewerking is vereist van het buitenland zonder dat daarvoor een eerst verantwoordelijke organisatie kan worden gevonden, dan zorgt het NIBC voor het contact en voor de activiteit die met behulp van het contact dient plaats te vinden. Andere activiteiten die tot de functie van aanspreekpunt worden gerekend zijn:

- voorlichting en advisering op het gebied van bestrijding, zowel vanuit justitieel als niet-justitieel perspectief;
- verzoeken tot een (inter-) nationaal gecoördineerde aanpak van zware en georganiseerde vormen van criminaliteit die technisch complex (lijken te) zijn en / of een grensoverschrijdend karakter hebben;
- innovatieve en multidisciplinaire (inter)nationale onderzoeken die kunnen worden geïnitieerd in relatie tot cybercrime.

Voor alle activiteiten geldt dat zij worden verricht voorzover er geen andere eerder aangewezen partij aanwezig is.

Meldpunt

Als onderdeel van het Nationale Infrastructuur programma zal worden onderzocht op welke plaats het meldpunt het beste permanent kan worden gepositioneerd. Voorlopig is het meldpunt ondergebracht bij het KLPD. Het meldpunt ontvangt meldingen van zowel concrete voorvallen, waargenomen dreigingen, als (technische) signalen. De herkomst van de diverse typen meldingen kan zowel van particulieren als organisaties zijn. In het verlengde van het meldpunt ligt bij serieuze meldingen de mogelijkheid tot een zogenaamde ‘notice-&-takedown’-functie gericht op het direct stoppen van het criminele feit.

Trendwatching

Het is zaak om nauwgezet functionele en technische ontwikkelingen gerelateerd aan internetcommunicatie te volgen. Om een dergelijke vorm van trendwatching op een doelmatige wijze te kunnen uitvoeren, zijn korte en structurele lijnen met de belangrijkste vertegenwoordigers binnen de ICT-industrie van belang. Een of meerdere liaisons richting organisaties zoals Microsoft, Cisco en IBM zijn derhalve van belang voor deze functie. Maar deze functie richt zich niet alleen op de algemene ontwikkeling van ICT-functies en techniek. Ook de wijze waarop daarvan misbruik wordt gemaakt, en de ontwikkelingen qua doelwit en modus operandi die cybercrime doormaakt, vallen onder deze noemer.

Monitoren

Opvallende ontwikkelingen binnen het internetverkeer zullen waar mogelijk gemonitord worden op basis van de beschikbare informatie binnen de Nationale Infrastructuur. Met name nationale en internationale serviceproviders spelen hierbij een cruciale rol.

Detecteren

Er wordt op verschillende manieren door de Nationale Infrastructuur gedetecteerd. In de eerste plaats zoals gezegd door internetverkeer te monitoren opdat aanvallen en dreigingen al worden gedetecteerd voordat er meldingen van aangevallen zijn binnenkomen.

Ook proactief wordt er gedetecteerd op ontwikkelingen die op ICT-gebied plaatsvinden binnen bijvoorbeeld telecommunicatiebedrijven. Die ontwikkelingen worden beoordeeld op mogelijke gevoeligheid voor cybercrime. Blijkt die gevoeligheid te bestaan dan wordt deze informatie teruggekoppeld naar de betreffende ontwikkelaar zodat deze nog tijdens de ontwikkelfase het ontwerp kan aanpassen ter voorkoming van misbruik.

Informatieverstrekking

Als gevolg van de gewenste informatiedeling zullen organisaties binnen de Nationale Infrastructuur gaan beschikken over een veelheid aan informatie uit uiteenlopende bronnen, die gecombineerd kan leiden tot een zeer krachtig instrument om cybercrime te bestrijden. Naast stoppen en bestrijden speelt hierbij voorkomen een zeer wezenlijke rol. Voor een brede informatievoorziening over de mogelijkheden hiertoe, geldt dat het vertrouwelijke karakter van de informatie waar organisaties over beschikken deze brede verstrekking in de weg kan staan. In dat geval wordt de informatie veralgemeniseerd in generieke informatie (aanbevelingen en beschermingsconstructies) ten behoeve van de op de Nationale Infrastructuur aangesloten organisaties.

Voorlichting

In situaties waarbij informatieverstrekking gericht op voorkoming bedoeld is voor professionele en direct via liaisons te bereiken organisaties kan in de regel volstaan worden met simpelweg beschikbaar stellen van de (veralgemeniseerde) informatie. Echter voor sommige groepen potentiële slachtoffers zoals bijvoorbeeld het MKB en locale overheden levert het alleen beschikbaar stellen onvoldoende resultaat. Voor dit type groepen zal daarom met betrokken koepelorganisaties voorlichtingscampagnes worden opgezet om via een intensieve en gerichte communicatie de beschikbare informatie te verspreiden.

Waarschuwen

Voor sommige te signaleren ontwikkelingen geldt dat er voldoende tijd bestaat om generieke informatieverstrekking of daarop gebaseerde voorlichting via gangbare kanalen te laten plaatsvinden. In sommige situaties zoals virusdreigingen is hiervoor echter geen tijd. Een zeer snelle informatievoorziening is daarbij essentieel.

Waarschuwen is daarom een eerste lijnsfunctie binnen de Nationale Infrastructuur. Dat betekent dat iedereen (individuele burger, bedrijven, overheidsorganisaties) deel uitmaken van het waarschuwingssysteem. Waarschuwen vindt plaats op basis van een risico-inschatting voor de sectoren. Contactpersonen spelen een belangrijke rol in het specifiek voorlichten van hun specifieke deel van een sector. Waarschuwen gebeurt via de geautoriseerde die toegang heeft tot een markt. Bijvoorbeeld de klanten van een bepaalde bank worden gewaarschuwd via hun bank. Dat creëert goodwill voor de bank en indiceert voor de klant de betrouwbaarheid. Op die manier kunnen alle klanten van bank X bijvoorbeeld in één keer worden bereikt (mits zij bijvoorbeeld met dit doel hun emailadres hebben opgegeven).

Ontwikkelen

Op basis van meldingen uit de deelnemende organisaties en meldingen die bij het meldpunt binnengekomen zijn, wordt bekeken of er bestrijding- of reparatieproducten beschikbaar zijn. Zo ja, dan worden de liaisons op die producten gewezen. Dit zal voor grote en professionele organisaties op het gebied van ICT geen probleem zijn. Voor het verspreiden van oplossingen voor bestrijding of reparatie naar grote, moeilijk direct te bereiken doelgroepen, is een belangrijke rol voor de lokale ICT-dienstverleners weggelegd. Zowel via bestaande branchestructuren als breed benaderde kanalen à la Microsoft TechNet zullen deze ICT-dienstverleners met oplossingen benaderd worden.

In situaties waar nog geen directe oplossing voor handen is, wordt beoordeeld of het zinvol is om tot dergelijke producten te komen. Zo ja, dan worden de eisen waaraan die producten moeten voldoen gespecificeerd, worden leveranciers uitgenodigd om aanbiedingen te doen en volgt aanbesteding. Daarna gevolgd door bouwmanagement en testen. Eventueel worden allianties aangegaan met CERT's uit andere landen.

Kennis ontwikkelen en delen

Door succesvolle toepassing van de beschikbare informatie binnen de diverse functie van de Nationale Infrastructuur ontstaat een schat aan kennis.

Naast het delen van kennis, ligt er ook een taak om kennis verder te ontwikkelen. Hiervoor wordt ook de buitenwereld actief benaderd. Onderdeel hiervan is het initiëren van innovatieve en multidisciplinaire (inter)nationale onderzoeken ter bestrijding van cybercrime bijvoorbeeld in de vorm van experimenten. Daarnaast is er behoefte aan een nationaal forum gericht op de bestrijding van cybercrime. Naar gelang de belangstelling voor dit forum en de mogelijk uiteenlopende deelnemers, zou het forum verder kunnen worden toegesneden op bepaalde rollen in de bestrijding van cybercrime. Maar dan zonder het integrale karakter van de bestrijding te doorbreken.

Toezicht

Voor bijna alle functies van de Nationale Infrastructuur – of het gaat om voorkomen, stoppen of bestrijden – geldt dat het effect van de maatregelen naar verwachting met een vertraging tot stand komt. Om de effectiviteit van typen maatregelen te kunnen waarnemen en daarmee de toekomstige effectiviteit te kunnen verbeteren, is een structurele toezichtfunctie gericht op zowel voortgangsbewaking van de voorgenomen maatregelen maar vooral ook op de timing en omvang van het gerealiseerde effect, cruciaal. Voor een deel kan dit op basis van de informatie-infrastructuur uitgevoerd worden. Een ander deel zal via expliciete terugkoppeling via liaisons en/of aanvullende onderzoek onder (potentiële) slachtoffergroepen moeten plaatsvinden.

Tegenhouden/stoppen

Er bestaan verscheidene technische en a-technische methoden om bepaalde vormen van cybercrime te stoppen. Een van de kernfuncties van organisaties binnen de Nationale Infrastructuur is het zelfstandig oplossen van situaties waar stoppen wenselijk is en waarvoor geen andere partij beschikbaar is op. Dit kan gebeuren hetzij op verzoek van (potentiële) slachtoffers zelf of op eigen initiatief. Dit laatste zal met name gebeuren bij acute dreiging met een groot aantal potentiële slachtoffers. Omdat de factor tijd bij het stoppen van een cybercrime-

aanval van groot belang is, dienen organisaties binnen de Nationale Infrastructuur op een dusdanig adequate wijze informatie te kunnen uitwisselen dat erop geen enkele wijze een hapering in het tegenhouden of stoppen van de aanval kan ontstaan. Zoals bij de meldfunctie reeds aangegeven ligt in het verlengde van deze functie de mogelijkheid tot een zogenaamde 'notice-&-takedown'-functie gericht op het direct stoppen van het criminele feit.

Verstoren

In het verlengde van het stoppen van een aanval liggen situaties waarbij het volledig tegenhouden ervan niet mogelijk is. Door samenwerking met serviceproviders en andere technisch betrokkenen is het echter vaak wel mogelijk om de aanval op een dusdanige wijze te verstoren dat de aanval geen of slechts beperkte gevolgen heeft voor de aangevallen infrastructuur. Bij zogenaamde dDOS-aanvallen met behulp van botnets wordt deze verstoringfunctie steeds belangrijker.

Schadebeperking

Op het moment dat er sprake is van een cybercrime-aanval die niet direct gestopt kan worden, kan ook voor schadebeperking gekozen worden. Binnen de Nationale Infrastructuur zullen in dergelijke situaties procedures en adviezen worden ontwikkelen om de schade daadwerkelijk zoveel mogelijk te beperken. Ten behoeve van schadeherstel stelt de Nationale Infrastructuur haar kennis beschikbaar aan ICT-bedrijven die op hun beurt die kennis weer kunnen benutten voor de eigen commerciële dienstverlening.

4.2.4 Belangrijke publieke partijen in de Nationale Infrastructuur

a. GOVCERT

GOVCERT is een operationele organisatie op het gebied van ICT-veiligheid onder de verantwoordelijkheid van de Minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties en de Minister van Economische Zaken. Overheidsorganisaties kunnen door GOVCERT worden ondersteund bij het invullen van hun informatiebeveiligingsverantwoordelijkheid. Daarnaast informeert en waarschuwt GOVCERT burgers en bedrijven over ICT-security en informatiebeveiliging (waarschuwingsdienst) Het optimaal hergebruiken van kennis is daarbij een belangrijk uitgangspunt. Deze kennis brengt GOVCERT middels zijn zogenaamde. kenniscentrum bij de verschillende doelgroepen. Het is de missie van GOVCERT om de ICT-veiligheid op een hoger peil te brengen. GOVCERT doet dit door 7x24 uur operationele dienstverlening op de volgende gebieden: preventie: bewustzijn creëren en kennis vergroten bij doelgroepen ten aanzien van ICT-veiligheid, detectie: monitoring en "early warning" van mogelijke ICT bedreigingen, en reactie: afhandeling van incidenten op gebied van ICT-veiligheid. In de afgelopen drieëneenhalf jaar heeft GOVCERT zich ontwikkeld tot een serieuze speler in het veld van de CERTs. In het internationale netwerk heeft het een stevige positie verworven, waarbij de rol van GOVCERT vooral gericht is geweest op kennisoverdracht en het delen van best practices.

Zoals aangegeven is GOVCERT nu gepositioneerd binnen de overheid, maar lijkt er een groeiende behoefte in de markt – naast de waarschuwingdienst- aan de diensten en expertise van een organisatie als GOVCERT. Denkbaar is de werkzaamheden van GOVCERT een bredere positionering naar de deelnemende doelgroepen van

de Nationale Infrastructuur te geven. Of en in welke mate dat voldoende is om de witte vlekken te bedekken zal in het implementatietraject moeten blijken.

b. National High Tech Crime Center (NHTCC)

Het vijfde hoofdstuk van deze notitie is volledig gewijd aan de opsporing en vervolging in het kader van cybercrime. Onder de naam NHTCC, zal het KLPD onder leiding van het Landelijk Parket invulling geven aan de opsporing van cybercrime voor zover die het regionaal en bovenregionaal niveau overschrijdt. Verzoeken tot een (inter-)nationaal gecoördineerde aanpak van zware en georganiseerde vormen van criminaliteit die technisch complex (lijken te) zijn en / of een grensoverschrijdend karakter hebben, lopen via dit NHTCC.

c. Meldpunt

Het op te richten Meldpunt voor cybercrime zal uiteindelijk onderdeel uit gaan maken van de Nationale Infrastructuur. Omdat het Meldpunt in eerste instantie ziet op terrorismebestrijding en kinderporno is het vooralsnog ondergebracht bij het KLPD.

4.2.5 Belangrijke private partijen in de Nationale Infrastructuur

Ook private sectoren die bij de bestrijding van cybercrime betrokken zijn, dienen te participeren in de gemeenschappelijke informatie-uitwisselingstructuur. Het mobiliseren van het bedrijfsleven gebeurt via het Nationaal Platform Criminaliteitsbeheersing (NPC), waarin overheid en bedrijfsleven samenwerken. In het NPC participeren ondermeer: VNO-NCW, MKB Nederland, Nederlandse Verenging van Banken en het Verbond van Verzekeraars.

Participatie kent twee mogelijke vormen:

- men neemt fysiek deel in de vorm van structurele personele capaciteit in overlegorganen,werkgroepen e.d.;
- men neemt deel door het aanleveren van informatie en kennis.

Sectoren met een grote diversiteit en die als gevolg daarvan minder collectief zijn georganiseerd en toch van belang zijn voor de bestrijding van cybercrime, zullen worden bijgestaan vanuit de organisaties in de Nationale Infrastructuur. Zowel bij het waar mogelijk tot stand brengen van gezamenlijkheid binnen de sector, als bij het invullen van hun relatie naar de aan de Nationale Infrastructuur deelnemende organisatie.

Iedere deelnemende sector organiseert de eigen achterban

Iedere deelnemende sector regelt zoveel mogelijk een eigen eerste lijnszorg. Voor een groot deel is die zorg al belegd bij ICT-afdelingen, maar dat geldt minder voor bijvoorbeeld kleinere MKB-bedrijven.

Contactpersonen

Van de Nationale Infrastructuur maken zogenaamde ‘Human Interfaces’ van de organisaties per sector deel uit. Zij bevinden zich in het veld en treden namens dat veld op als contactpersoon naar de gemeenschappelijke informatie-uitwisselingstructuur. Een contactpersoon krijgt deze rol als vast onderdeel van diens taak zodat men

ook zeker weet dat er bediend wordt De contactpersonen kennen hun specifieke deel van de markt en halen uit de informatie die hen door de gemeenschappelijke informatie-uitwisselingstructuur wordt toegespeeld, de zaken die relevant zijn voor hun achterban. Zij vertalen die zaken ook in voor de achterban begrijpelijke taal. Het zijn van contactpersoon krijgen zij specifiek in hun taakomschrijving neergelegd. Zij bedienen zich voor de onderlinge communicatie van een vertrouwelijk info netwerk (de ccWiki)

4.2.6 Samenwerkingsverbanden met ICT-bedrijven en grote organisaties

Naast de contactpersonen wordt het brede veld nog op een andere manier betrokken bij de bestrijding van cybercrime in de brede zin van het woord. Deze eerste lijnszorg geschiedt via de ICT-bedrijven. Die bedrijven worden een belangrijke structurele schakel in het bereiken van de eindgebruiker, wat met name in de sector van het MKB tot nu toe een probleem was. Van de ICT-bedrijven zal worden gevraagd om periodiek een voorgestructureerd (internet)staatje in te vullen met onder hun klanten geconstateerde cybercrime problemen. Uiteraard niet herleidbaar naar individuele klanten. Van zelfstandige bedrijven met een eigen ICT-afdeling zal hetzelfde worden gevraagd. De bereidheid om op dit punt met de gemeenschappelijke informatie-uitwisselingsinfrastructuur samen te werken wordt gestimuleerd door middel van ruil. Gedacht wordt aan kennisdeling.

4.3 Conclusie

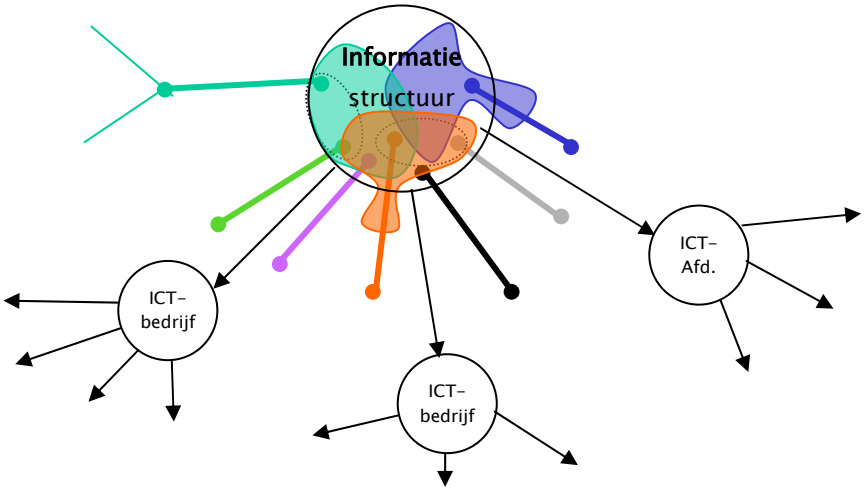
Als eerste conclusie kan uit dit ontwerphoofdstuk worden getrokken dat het mogelijk is om gebruikmakend van de uitgangspunten zoals geïntroduceerd in hoofdstuk 2 een infrastructuur te ontwerpen die voor een belangrijk deel tegemoet komt aan de probleemstelling.

Met inachtneming van de gepresenteerde varianten, is gekozen voor één gemeenschappelijke informatie-uitwisselingstructuur. In het ontwerp zijn de fundamentele inzichten zoals opgedaan uit recent onderzoek naar de samenwerking rond multi-agency vraagstukken, verwerkt[3].

Onderstaande figuur vat het ontwerp voor een Nationale Infrastructuur nog eens samen. De kern (deel binnen de cirkel) wordt gevormd door publieke en private partijen. Deze organisaties zullen op zichzelf blijven functioneren. Deels zullen zij dat doen in onderlinge afstemming en samenhang binnen de gemeenschappelijke informatie-uitwisselingstructuur (voorgesteld door de overlappende organische vlakken). Deels zullen zij dat ook doen buiten de informatie-uitwisselingstructuur waar het zelfstandige taken betreft die niet samenvallen met de informatie-uitwisselingstructuur (voorgesteld door de uitstulpende vlakken buiten de cirkel). Het NHTCC is weliswaar onderdeel van de Nationale Infrastructuur, maar neemt een bijzondere plaats in vanwege haar specifieke taak. De gedachte is dat een (vertrouwelijke) informatie-uitwisseling met de private sector alleen tot stand komt als preventie en opsporing in beginsel gescheiden zijn.
Iedere in de informatie-uitwisselingstructuur deelnemende organisatie onderhoudt het contact naar de human

[3] Faber, W., A.A.A. van Nunen, *Uit onverdachte bron. Evaluatie van de keten ongebruikelijke transacties*, WODC, Den Haag, 2004, p. 324-326

interfaces binnen de eigen achterban (voorgesteld door de lijnen met aan begin en eind een stip). Achterbannen die niet eenduidig zijn georganiseerd of sterk heterogeen zijn samengesteld kennen geen human interface maar worden bediend via de reguliere ICT-bedrijven of –afdelingen.



Figuur 1. De Nationale Infrastructuur

Hoofdstuk 5 De organisatie van de opsporing en vervolging

Als bijzonder onderdeel van de Nationale Infrastructuur Bestrijding Cybercrime, gaat dit hoofdstuk in op de organisatie van de opsporing en vervolging van deze delictsoort. De ervaringen met het project NHTCC en het NPAC-project zijn integraal verwerkt. Het hoofdstuk vertrekt vanuit het specifieke doel dat met de opsporing en vervolging van cybercrime wordt nagestreefd, en de doelgroepen waarvoor het effect van die opsporing met name merkbaar moet zijn. Daarna wordt antwoord gegeven op de vraag aan welke functies op het gebied van opsporing en vervolging van cybercrime behoefte bestaat. Om vervolgens de belangrijkste ontwerpvraagstukken en dilemma's langs te lopen die een rol spelen als men die functies binnen de bestaande opsporings- en vervolgingsorganisaties wil positioneren en verankeren. De conclusies waarmee de beschrijving van elk afzonderlijk ontwerpvraagstuk eindigt, zijn tot slot vertaald in een aantal ontwerpalternatieven die, na ten opzichte van elkaar te zijn gewogen, uitmonden in één structuurvoorstel.

5.1 Doel van opsporing en vervolging

Binnen de centrale doelstelling voor de bestrijding van cybercrime zoals die werd geïntroduceerd, neemt opsporing en vervolging een bijzondere plaats in. De toegevoegde waarde van de totale Nationale Infrastructuur Bestrijding Cybercrime aan het waarborgen van die integriteit bestaat voor een belangrijk deel uit het zoveel mogelijk voorkomen en stoppen van cybercrime. Maar de cybercrimineel die uitsluitend wordt geconfronteerd met een (tijdelijk) stopzetten van zijn activiteiten, zonder daarvan ook persoonlijk consequenties te ondervinden, kan gemakkelijk op een andere manier zijn activiteiten voortzetten. Uit het NHTCC-project en het NPAC-project is dan ook naar voren gekomen dat opsporings- en vervolgingsinspanningen noodzakelijk zijn, binnen de nationale infrastructuur.

5.2 Doelgroepen en hoe die te bedienen

Zowel de individuele computergebruiker als organisaties die bedrijfsmatig gebruik maken van de infrastructuur aan communicatievoorzieningen hebben baat bij de strafrechtelijke aanpak van cybercrime. In de praktijk komt het beperkt voor dat één enkele gebruiker het slachtoffer wordt van cybercrime . De gemiddelde cybercrimineel is vooral uit op een zo groot mogelijk effect. Een strafrechtelijke aanpak zal dan betrekking hebben op dreigingen of misbruik die potentieel grote groepen van gebruikers treffen, zodat van de effecten van die aanpak ook zoveel mogelijk risicodragende of getroffen gebruikers profiteren. Net als in het geval van commune criminaliteit, worden ook cybercrimedreigingen en voorvallen ingedeeld naar aard en omvang. Om vervolgens in

het verlengde daarvan het meest geëigende opsporingsniveau te kiezen om de dreiging of feitelijke voorvallen en degene die daarvan het slachtoffer zijn geworden, te voorzien van een passende opvolging. Op basis van afweging en toedeling is het mogelijk om de verschillende belanghebbenden bij verschillende vormen van cybercrime tegemoet te komen met een passende opsporings- en vervolgingsreactie. Voor de individuele gebruiker en individuele organisaties (zowel publiek als privaat) zal dat vooral een opsporingsreactie zijn uit de eigen politieregio. Voor de bedrijven met vele nationale en internationale vertakkingen en organisaties die zelf verantwoordelijk zijn voor het instandhouden van communicatieve voorzieningen ligt opvolging op bovenregionaal of landelijk niveau meer voor de hand.

5.3 Wenselijke functies opsporing en vervolging cybercrime

Alvorens binnen de doelstelling een wenselijk ontwerp te kunnen schetsen van de opsporing en vervolging van cybercrime, is het van belang vast te stellen in welke functies die opsporing en vervolging moet voorzien. Rond deze vraag hebben als onderdeel van het NHTCC-project workshops plaatsgevonden met een brede vertegenwoordiging van het professionele veld dat bij de verschillende processtappen in het voorkomen en bestrijden van cybercrime is betrokken. Het NPAC-project heeft zich aan de andere kant gericht op de behoefte van (potentiële) slachtoffers/aangevers. De uitkomsten van beide projecten zijn geïntegreerd, en afgestemd op het bredere functieontwerp van de Nationale Infrastructuur Bestrijding Cybercrime waarin ook niet aan de opsporing gerelateerde functies (privaat en publiek) zijn ondergebracht. Voor alle opsporings- en vervolgingsfuncties geldt dat ze nauw moeten aansluiten op de inspanningen van anderen binnen de nationale infrastructuur.

5.3.1 De gewenste opsporingsfunctie

Bij het definiëren van functies gericht op de opsporing van cybercrime is nog niet gedifferentieerd naar het organisatorisch niveau waarop deze functies al zijn belegd of het beste kunnen worden belegd. Conclusies daaromtrent volgen later in dit hoofdstuk.

1. **Het verrichten van opsporingsonderzoeken naar cybercrime**
   In het veld wordt voor deze delictsoort een opsporingsvacuüm ervaren. Concreet wil men dat er daadwerkelijk opsporingsonderzoeken naar cybercrime worden verricht, en dat daarvoor ook capaciteit beschikbaar is. Dat die capaciteit snel beschikbaar komt, is belangrijker dan de exacte beantwoording van de vraag hoe groot die capaciteit precies moet zijn.

2. **Het ontwikkelen en uitvoeren van strategieën op het gebied van tegenhouden van cybercrime.**
   Cybercrime kan zich zeer snel verspreiden, met mogelijk in korte tijd optredende grote gevolgen. Ten opzichte van meer traditionele vormen van criminaliteit is tegenhouden als onderdeel van de opsporings- en vervolgingsactiviteiten daarom zo mogelijk nog meer geboden. Een belang dat extra wordt onderstreept door de complicerende en vertragende doorwerking van territorialiteitskwesties op het aanwenden van bevoegdheden, het mobiliseren van partijen in het buitenland, en op de bewijsgaring en bewijsvoering.

Daartoe moeten tegenhoudstrategieën ontwikkeld en uitgevoerd worden

3. **Het benutten, opbouwen en uitdragen van expertise**

   Voor succesvolle opsporing en vervolging is naast samenwerking met ketenpartners binnen de Nationale Infrastructuur specifieke expertise nodig. De toegevoegde waarde van expertise ligt niet in het voor handen zijn op zichzelf, maar in het feitelijk gebruik in het kader van de opsporing en vervolging. Expertise is geen product, maar het feitelijk ondersteunen van aangifteprocessen en van opsporingsonderzoeken met behulp van die expertise zijn producten. Onder de noemer expertise vallen ook het ontwikkelen en vooral het aanwenden van nieuwe opsporingsmethodieken, evenals het duiden van trends en het leveren van input ten behoeve van gewenste aanpassing van beleid en wetgeving.

4. **Het vergaren en uitwisselen van informatie**

   Informatie is de voorwaarde voor het kunnen vervullen van de verschillende opsporingsfuncties. Vanwege dit belang is het vergaren en uitwisselen van die informatie als afzonderlijke functie van de opsporing benoemd. De essentie van de Nationale Infrastructuur Bestrijding Cybercrime waarvan ook de opsporing en vervolging deel uitmaken, bestaat uit informatieverzameling en informatiedeling. De NIBC zal een belangrijke leverancier zijn van informatie ten dienste van de opsporing en vervolging, net zoals de opsporing en vervolging hun informatie zullen delen met de NIBC. Binnen de opsporing zal de informatie worden aangewend voor operationele doeleinden, maar ook voor strategische analyse zodat wordt bijgedragen aan het Nationaal Dreigingsbeeld, dat thans nog witte vlekken laat zien rond het thema cybercrime. Onder deze vierde opsporingsfunctie wordt ook de afhandeling van rechtshulpverzoeken begrepen.

5. **Beschikbaarheid en inzetbaarheid 24 uur en 7 dagen per week**

   Het alleen zijn van een aanspreekpunt is geen product. Continue beschikbaarheid als functie van de opsporing gaat verder. Er is niet alleen behoefte aan een opsporingsfunctie op het gebied van cybercrime die voor binnen en buitenland 24 uur bereikbaar is, maar die ook in staat is op ieder moment noodzakelijke actie te ondernemen. De cyberomgeving met zijn wereldwijde karakter is per definitie 24 uur actief. Dat stelt bijzondere eisen aan de inzetbaarheid van de opsporingsfunctie.

5.3.2 De gewenste vervolgingsfunctie

De gewenste vervolgingsfuncties op het terrein van cybercrime lopen voor een belangrijke deel parallel met de in de vorige paragraaf geschetst opsporingsfuncties. Opsporing en vervolging beïnvloeden elkaar over en weer, wat ook tot uitdrukking komt in de voorgestelde organisatie van beide functies in de sfeer van de bestrijding van cybercrime.

1. **Weging van rechtsbelangen**

   De tijd van het legaliteitsbeginsel waarin elke overtreding van een strafrechtelijke norm aanleiding gaf tot een strafrechtelijke reactie ligt ver achter ons. Het strafrecht zelf is mede vanwege de massaliteit van zich

voordoende overtredingen als beleidsinstrument gaan functioneren. Niet alle cybercrimevraagstukken kunnen strafrechtelijk worden aangepakt en ook niet alle vraagstukken hoeven strafrechtelijk te worden aangepakt Het is de functie van het OM om te beoordelen of publieke normstelling is gewenst door het toepassen van een eigen interventie of door te vragen om inmenging van de strafrechter. Zelfs in die gevallen waarin technisch met een niet-strafrechtelijke interventie zou kunnen volstaan om een cybercrimedelict een halt toe te roepen, kan het rechtsbelang vragen om publieke normstelling.

Het is wenselijk dat deze beoordeling door het OM voor cybercrimevraagstukken op drie momenten plaatsvindt[4]:

- *vooraf*, bij het vaststellen van het opsporingsbeleid zodat bekend is welke verschijningsvormen van cybercrimevraagstukken binnen welke sectoren met name prioriteit dienen te krijgen;
- *tijdens*, op het moment dat cybercrime zich heeft aangediend en de vraag aan de orde is hoe aangiftes of ambtshalve verkregen inzichten die zouden kunnen leiden tot een opsporingsonderzoek, zich verhouden tot de ernst van de normschending;
- *achteraf*, op het moment dat interventies (zowel strafrechtelijke als niet-strafrechtelijke) hebben plaatsgevonden, dient te worden beoordeeld of en op welke wijze ze hebben bijgedragen aan het gewenste maatschappelijk effect.

2. Ontwikkelen en beheren van het wegingskader

Bij alle drie beoordelingsmomenten door het OM spelen dezelfde ingrediënten een rol. Zoals de kans op herhaling en de ernst van de normschending, die niet alleen kan bestaan uit bijvoorbeeld de omvang van door cybercrime toegebrachte financiële schade, maar ook uit geschonden vertrouwen in de integriteit van bepaalde communicatievoorzieningen. Ook wordt in de beoordeling door het OM betrokken wat partijen zelf hebben gedaan om inbreuken door cybercrime te voorkomen c.q. hoe zij zich op eventuele inbreuken hebben voorbereid. Het is gewenst om onder verantwoordelijkheid van het OM in het kader van de Nationale Infrastructuur Bestrijding Cybercrime het beoordelingskader voor het wegen van rechtsbelangen rond cybercrimevraagstukken verder te ontwikkelen. Niet alleen gericht op het aanwenden van strafrechtelijke interventies, maar ook op niet-strafrechtelijke. Inzicht in de aard en omvang van cybercrime geldt daarbij als voorwaarde. Naast beleids- en jaarplannen waarin vervolgingsbeleid is terug te vinden, hanteert het OM instrumenten om de instroom aan processen-verbaal te sturen, de eigen verantwoordelijkheid voor de handhaving door publieke en private partijen te benadrukken, als ook om te garanderen dat bepaalde ernstige normschendingen ter kennis van het OM worden gebracht om te worden beoordeeld op de wenselijkheid van normstellend optreden. Geadviseerd wordt om Het beoordelingskader van cybercrime zal in ieder geval bestaan uit handhavingsarrangementen met belangrijke sectoren uit het veld. In het kader van de bestrijding van cybercrime is het afsluiten en opvolgen van handhavingsarrangementen een belangrijke vervolgingsfunctie die bovendien de werking van de Nationale Infrastructuur belangrijk kan ondersteunen.

Handhavingsarrangementen bevatten wederzijdse afspraken tussen een bepaalde sector en het OM, over gegarandeerde instroom en afdoening van bepaalde delictsoorten, en over daaraan voorafgaande door de sector zelf te nemen maatregelen om inbreuken tegen te gaan. De afspraken gelden voor een hele sector, en

[4] Zie ook de nota ‘De strafrechtelijke aanpak van georganiseerde misdaad in Nederland 2005-2010’, (OM, 2004)

niet voor bijvoorbeeld slechts één dienst uit een sector. Bestaande handhavingsarrangementen met banken, met verzekeraars en met telecommunicatie-aanbieders worden uitgebreid met afspraken over het voorkomen en bestrijden van cybercrime. Voor nieuwe marktpartijen als internetproviders worden trajecten ingezet om tot handhavingsarrangementen te komen.
Handhavingsarrangementen gericht op het voorkomen en bestrijden van cybercrime bevatten afspraken over handhaving op alle niveaus binnen de politie en bij het OM, en over alle soorten cybercrime. De in de handhavingsarrangementen te maken afspraken en de prestatieafspraken tussen de politieministers en de politieregio's, zullen op elkaar worden afgestemd.

3. Het voeden van beoordelingsorganen

Het OM participeert op verschillende niveaus in de opsporing in beoordelingsorganen. Onder uiteenlopende namen als stuurploegen (op het niveau van de politieregio), weegploegen (op bovenregionaal niveau), het Bovenregionaal Recherche Overleg (op multiregionaal niveau) en het Landelijk Parket (op nationaal niveau), worden onder verantwoordelijkheid van het OM voorstellen voor rechercheonderzoeken beoordeeld en ten opzichte van elkaar gewogen. Met als uiteindelijk resultaat het toewijzen van prioritaire onderzoeken aan opsporingseenheden. Het is wenselijk om de werkzaamheden van deze organen te laten aansluiten op het wegingskader.. Gebruikmakend van bestaande beoordelingsorganen, is het aan te bevelen dat het OM vanuit haar informatiepositie binnen de Nationale Infrastructuur Cybercrime, haar participanten in de verschillende beoordelingsorganen voedt met het gedefinieerde opsporingsbeleid, met het formele wegingskader en met informatie over de aard en omvang van cybercrime. De verantwoordelijkheid voor het doen aanvullen van het Nationaal Dreigingsbeeld met een overzicht van de aard en omvang van het cybercrimevraagstuk maakt van dat laatste deel uit. Op deze manier gaan de beoordelingsorganen op het gebied van het toewijzen van cybercrimevraagstukken aanvullend werken ten opzichte van elkaar.

4. Feitelijke vervolging van cybercrimedelicten

Passend binnen het geheel van opsporing- en handhavingsafspraken dient het OM in het verlengde van de feitelijke opsporing in haar vervolgingstaak te voorzien. Dankzij de afspraken die gemakshalve zijn aangeduid met wegingskader, leidt dat tot een gegarandeerde inzet en toestroom van zaken op het niveau van zowel de territoriale arrondissementsparketten, als het Landelijk Parket en het Functioneel Parket. Uiteraard voorzover er ook daadwerkelijk sprake is van zich voordoende cybercrime.

5. Het benutten, opbouwen en uitdragen van expertise

De expertise van opsporing en vervolging zijn zo nauw met elkaar verweven, dat het wenselijk is om ze gemeenschappelijk onder verantwoordelijkheid van het OM vorm te geven. Bestaande expertise en de eenheden die thans met een expertisetaak zijn belast zullen daarin worden betrokken. Niet door het ontwerpen van nieuwe organisatieonderdelen, maar door gebruik te maken van de filosofie binnen de NIBC en kennis en ervaring met elkaar te delen. Daardoor zal de expertisefunctie voor opsporing en vervolging veel breder worden gevoed en ook anderen kunnen voeden

5.3.3 Vergelijking gewenste en huidige functies

In de politieregio's bevinden zich goed opgeleide specialisten op het terrein van digitale opsporing die ook kunnen ondersteunen bij onderzoeken gericht op cybercrime. De opsporingsonderzoeken zelf worden uitgevoerd door algemene tactische opsporingsteams die niet specifiek zijn opgeleid voor de aanpak van cybercrime, en niet exclusief op dit terrein worden ingezet. Voor regionale opsporingsonderzoeken gericht op lokale verschijningsvormen of de lokale uitstraling van cybercrime met vooral individuele slachtoffers, kan een kennistekort ontstaan.

Zodra cybercrime-onderzoeken kunnen worden gerekend tot de zogenaamde middencriminaliteit die meerdere politieregio's betreft, komen ze in beginsel in aanmerking voor aanpak door de Bovenregionale Recherche (BR). De eenheden van de BR hebben geen specifieke opdracht om cybercrimevraagstukken aan te pakken, maar kunnen deze capaciteit wel inhuren vanuit de regio's. Het orgaan dat de toewijzing van onderzoeken aan de BR verzorgt, kent geen specifieke taakstelling bestaande uit bijvoorbeeld een minimum aantal toe te wijzen onderzoeken dat betrekking heeft op cybercrime. Toch kan in meerdere gevallen sprake zijn van een delict dat desalniettemin binnen het aandachtsgebied van de BR ligt zoals bijvoorbeeld aan cybercrime gerelateerde afpersing of oplichting.

De inzet van de Nationale Recherche is gekoppeld aan de aandachtsgebieden zoals die uit het Nationale Dreigingsbeeld naar voren zijn gekomen. Cybercrime is tot nu toe geen aandachtsgebied, omdat het Nationale Dreigingsbeeld terzake constateert nog over onvoldoende informatie te beschikken. Als onderdeel van andere aandachtsgebieden zoals terrorisme, past cybercrime wel binnen de aandacht van de Nationale Recherche maar de meeste vormen van cybercrime behoren thans niet tot de taakstelling van de NR.

Bij het OM zijn binnen het Landelijk Parket een Officier van Justitie en een tweetal beleidsmedewerkers specifiek aangewezen voor de ondersteuning en coördinatie van de vervolging aangaande onderzoeken met een relatie naar cybercrime en ICT. Bij het KLPD is een meldpunt in voorbereiding voor de ontvangst van o.a. cybercrimesignalen.

Worden de gewenste functies van opsporing en vervolging betrokken op de huidige inrichting en werkwijze van de opsporing en vervolging, dan wordt vastgesteld dat niet in alle gewenste functies van opsporing en vervolging van cybercrime wordt voorzien. Ondanks dat een volledig inzicht in de aard en omvang van de problematiek ontbreekt, zijn door het NHTCC-project en het NPAC-project voldoende signalen ontvangen om concreet invulling te geven aan de beschreven opsporing- en vervolgingsfuncties. Zoals reeds gesteld zal op zo kort mogelijke termijn overgegaan moeten worden tot realisatie van de wenselijke opsporing- en vervolgingsfuncties, en nietgewacht moeten worden tot over een completer overzicht van de aard en omvang wordt beschikt.

5.4 Realisatie van gewenste functies: ontwerpvraagstukken

Bij het ontwerpen van een opsporings- en vervolgingsomgeving die is toegesneden op de bestrijding van cybercrime, heeft men te maken met reeds bestaande structuren. De huidige wijze waarop de opsporing en

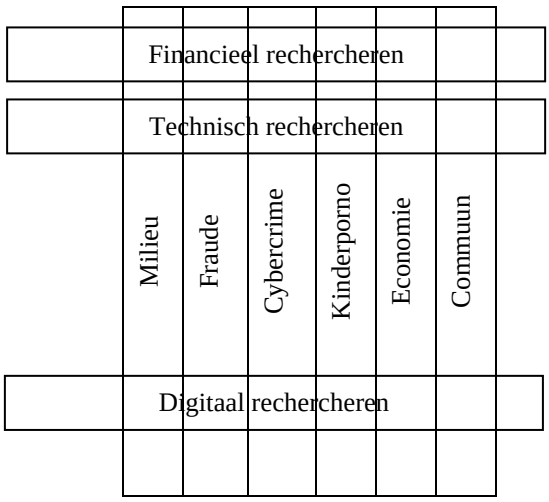
vervolging in Nederland zijn georganiseerd, is de uitkomst van een langdurig proces van checks and balances. Een blanco ontwerpbenadering volgens het vierde ontwerpscenario uit hoofdstuk drie, verhoudt zich moeizaam tot deze gegroeide werkelijkheid. Aan te dragen oplossingen sluiten aan op de bestaande structuren. Deze oplossingen moeten antwoord geven op vier centrale ontwerpvraagstukken die achtereenvolgens worden toegelicht en ieder afzonderlijk zijn voorzien van een advies.

5.4.1 Cybercrime of high tech crime?

Het vorige hoofdstuk begon met een afbakening van het domein waarop de Nationale Infrastructuur voor de bestrijding van cybercrime van toepassing is. Centraal in die keuze stond het gebruik, misbruik en de beschadiging van openbare netwerken en de daarop aangesloten apparatuur. Daarmee werd de aandacht voor bedrijfsinterne netwerken niet tot de nationale infrastructuur voor de bestrijding van cybercrime gerekend, evenmin als fysieke aanvallen op ICT-structuren. Op basis van deze keuze kan men met de aandacht voor veel van de processtappen waaruit de bestrijding van cybercrime is opgebouwd wel uit de voeten, maar in het geval van de opsporing en vervolging ontstaan toch dilemma's. Bijvoorbeeld rond de zogenaamde vitale infrastructuren. Het belang om vitale ICT-infrastructuren als bijvoorbeeld Schiphol te beschermen tegen inbreuken van buiten is groot. Ongeacht of het om fysieke of virtuele inbreuken gaat, en of het een openbare of een bedrijfsinterne netwerkinfrastructuur betreft. Vanwege de onderlinge samenhang van beide invalshoeken, wordt ter oplossing van het dilemma voorgesteld om in relatie tot de organisatie van de opsporing en vervolging, geen onderscheid te maken tussen cybercrime of hightechcrime.

5.4.2 Cybercrime: delict of techniek?

Bij de bestrijding van cybercrime is het van belang om het aanwenden van opsporingstechniek (digitale recherche of opsporing) te onderscheiden van het delict waarop die techniek zich richt (de cybercrime). ***Figuur 2*** stelt dat onderscheid schematisch voor[5].



Figuur 2 :Positionering van het instrument digitale opsporing (en andere instrumenten) ten opzichte van delictsoorten

[5] W. Faber, A.A.A. van Nunen, *Het ei van Columbo? Evaluatie van het project Financieel Rechercheren*, 2002, Oss, p. 72

Het digitaal opsporen is in veel rechercheonderzoeken goed bruikbaar, ongeacht welke delictsoort die onderzoeken betreffen. In het verlengde daarvan is het een goed uitgangspunt dat volgens de Raad van Hoofdcommissarissen (Landelijk Project Digitaal Opsporen, juni 2005) digitaal opsporen in de toekomst deel uit dient te maken te maken van het gehele spectrum van opsporend handelen; als een normaal aspect van de dagelijkse politiepraktijk. Om deze visie te realiseren, dienen volgens de Raad op grote schaal tactische rechercheurs te worden opgeleid en dienen de (regio-) Bureaus Digitale Recherche (BDR) en de Bureaus Digitale Expertise (BDE) te worden geïntegreerd met de Technische Recherche.
Voor de digitale opsporing als breed inzetbare techniek is nu dus al veel aandacht. Maar dat is niet hetzelfde als aandacht voor het delict cybercrime. Door de nationale politiek wordt de aanpak van cybercrime van groot belang geacht. Wil men daadwerkelijk garanties dat dit belang ook leidt tot significante inspanningen van politie en openbaar ministerie, dan zal die opsporings- en vervolgingsaandacht voor cybercrime als delictsoort expliciet benoemd en belegd moeten worden.

5.4.3 Cybercrime: generaal of specifiek?

In hoofdstuk twee werd als onderdeel van de probleemstelling het verschil tussen aangifte- en niet-aangiftecriminaliteit geïntroduceerd. Aangiftecriminaliteit komt de aangever uit zichzelf melden, zoals bijvoorbeeld diefstal of mishandeling. Belastingontduiking of mensensmokkel zijn daarentegen voorbeelden van normschendingen waarvan iemand niet gauw aangifte komt doen. Als opsporings- en vervolgingsinstanties deze criminaliteitsterreinen van belang vinden, dan zullen ze de zaken zelf ‘moeten halen’. Vandaar dat het verschil tussen aangifte- en niet-aangiftecriminaliteit vaak het verschil wordt genoemd tussen ‘breng- en haalwerk’.

Als paradox doet zich voor, dat een deel van de cybercrime in feite gewoon aangiftecriminaliteit is (iemands computer is gehacked en wil dat de politie de dader opspoort), terwijl het qua aard en ernstbeleving gelijk lijkt te scoren aan niet-aangiftecriminaliteit. Dat heeft andermaal te maken met het geringe slachtoffer- en schadebesef zoals al in de probleemstelling is toegelicht. Wil men dus dat de bestrijding van cybercrime kan worden gegarandeerd, dan moet worden voorkomen dat bij het stellen van prioriteiten binnen het totale aanbod dat politie en OM bereiken, cybercrimevoorvallen eigenlijk per definitie laag scoren. Als onderdeel van de generale politietaak met tal van delicten met een hogere ernstbeleving dan cybercrime, is de kans daarop groot. Dat maakt het wenselijk om de opsporing en vervolging van bijzondere en exclusieve vormen van ICT-gerelateerde criminaliteit, waarvan men niet het risico wil lopen dat ze afvallen in de afweging van prioriteiten, te verbijzonderen en specifiek te organiseren.

5.4.4 Positionering opsporing/vervolging cybercrime: centraal of decentraal?

Conform het hiervoor aangehaalde advies van de Raad van Hoofdcommissarissen naar aanleiding van het Landelijk Project Digitale Opsporing, is de opsporing van ICT-gerelateerde criminaliteit in principe een zaak voor de politieregio. Als uitkomst van het ontwerpvraagstuk ‘generaal of specifiek’, werd geadviseerd om ten behoeve van zaken waarbij sprake is van bijzondere en exclusieve vormen van ICT-gerelateerde criminaliteit, te

kiezen voor verbijzondering van de opsporings- en vervolgingstaak. Als verbijzondering in de rede ligt, is vervolgens een ontwerpvraag op welk niveau die verbijzondering vorm moet krijgen. Vrij algemeen in de sfeer van opsporing en vervolging wordt bij het positioneren van organisatieonderdelen uitgegaan van het principe 'decentraal tenzij'. Oftewel: in beginsel vallen alle taken en daarvoor in het leven te roepen organisatorische eenheden onder de politieregio's en de arrondissementsparketten. Tenzij er doorslaggevende argumenten zijn voor positionering op een ander, meer centraal niveau. De organisatiekundige aspecten waarop die argumenten betrekking zouden kunnen hebben passeren één voor één de revue[6].

Schaalgrootte

Ondanks het feit dat de opsporing en vervolging van cybercrime in beginsel tot het reguliere takenpakket van respectievelijk de politieregio's en de arrondissementsparketten behoren, zijn er argumenten op basis waarvan niet alle vormen van cybercrime binnen de grenzen van een regio of arrondissement kunnen worden aangepakt en opgelost. De nationale maar vooral internationale verwevenheid van cybercrime is regelmatig zo groot (zie het eerder beschreven territorialiteitsvraagstuk en de bevindingen van het project NHTCC), dat het vrijwel onmogelijk is om de aanpak van cybercrime tot de grenzen van een regio of meerdere regio's te beperken. Dat is zelf al moeilijk op het nationale niveau. Het karakter van bepaalde vormen van cybercrime maakt voldoende schaalgrootte voor informatieverzameling en opsporingsinspanningen noodzakelijk. Zelfs al zou men zich willen beperken tot bijvoorbeeld een dader die vanuit de eigen regio opereert, dan nog is het voor het verzamelen van bewijsmiddelen meestal noodzakelijk om de sterke arm veel verder uit te strekken dan die eigen regio, tot over de landsgrenzen.

De moeilijkheidsgraad van de aanpak van cybercrime

De te leveren opsporingsprestatie op het terrein van cybercrime bestaat uit meerdere componenten: tegenhouden, opsporing, vervolging, expertiseopbouw, netwerkbeheer en beleidsvoorbereiding. Door de verwevenheid, landelijke betekenis, technische aspecten, en het gewicht van de partners waarmee nationaal en internationaal moet worden samengewerkt, is de inhoudelijke bestrijding van veel cybercrimevraagstukken, en de omgeving waarin wordt gefunctioneerd, redelijk complex. Dat vraagt om een netwerk waarvan niet mag worden verwacht dat iedere politieregio of ieder arrondissement dat er zelfstandig op na houdt. Bovendien is een belangrijk deel van de cybercrimematerie zo specifiek, dat men met een generaal of zelfs meer specifiek kennisniveau niet in staat zal zijn om bijzondere vormen van cybercrime-onderzoeken tot een goed einde te brengen. Dat laatste vraagt om een kennisniveau dat niet in korte tijd is aan te brengen, en het vraagt om een zekere vaardigheid en routine in het toepassen van die kennis, die alleen kan ontstaan en op peil gehouden, waneer met een zekere frequentie onderzoeken naar bijzondere vormen van cybercrime worden verricht.

De behoefte aan maatwerk

In het algemeen ligt een reden voor decentralisatie van de aanpak van welke delictsoort ook, in de behoefte aan maatwerk. De noodzaak van maatwerk veronderstelt dat de aanpak dicht 'op de klant' moet worden georganiseerd. Maatwerk is bovendien aan de orde wanneer een aanpak vraagt om differentiatie en variatie naar gelang de omstandigheden. Zijn groeperingen interregionaal actief, dan moeten ze volgens het principe van

[6] F. Fleurke, R. Hulst, P.J. de Vries, *Decentraliseren met beleid*, SDU, Den Haag, 1997, p. 20 e.v.

maatwerk interregionaal worden aangepakt. Concentreert de delictvorm zich echter in een beperkt gebied, dan kan regionale aanpak geboden zijn. Handelt het zich om bijzondere en exclusieve vormen van ICT-gerelateerde criminaliteit, dan is vooral het landelijke niveau het uitgangspunt voor maatwerk. Daders van cybercrime opereren zelden uitsluitend regionaal, en de kanalen waarvan zij zich bij het plegen van hun delicten bedienen, worden vooral nationaal en internationaal beheerd. Een effectieve bestrijding van een aantal bijzondere vormen van cybercrime is juist niet gediend met een afzonderlijke aanpak per politieregio. Een uniforme aanpak is geëigend op het niveau waar ook belangrijke partners (en tevens slachtoffers) zoals internetproviders, banken en telecommunicatiepartijen zijn georganiseerd.

Slagvaardigheid

Het gaat hierbij om de vraag in hoeverre met de bestrijding van cybercrime te belasten organisatorische eenheden tijdig en adequaat kunnen reageren op wijzigingen in:

- de verschijningsvormen van cybercrime;
- de maatschappelijke behoefte aan bestrijding;
- de voor een succesvolle aanpak benodigde condities.

Met name de verschijningsvormen van cybercrime ondergaan snelle wisselingen, waardoor ook de aanpak ervan steeds aan veranderingen onderhevig is. Waar bijvoorbeeld een paar jaar geleden het betalingsverkeer met banken nog vooral via loketten en de postverzending verliep, is dat thans hoofdzakelijk vervangen door het internet. Het type aanval, het doelwit en de methoden zijn continu in beweging. Dit geldt eveneens voor de methoden ter bestrijding van cybercrime. De slagvaardigheid om op deze veranderingen flexibel in te spelen is niet gebaat bij een sterk gedecentraliseerde vorm van bestrijding. De snelle wisseling in het karakter van cybercrime en de snelle verplaatsing over het land en daarbuiten zou om een sterke coördinatie vragen tussen de afzonderlijke regio's. En die coördinatie brengt hoge kosten met zich mee.

Efficiëntie

De aanpak van cybercrime vraagt om veel overleg, kennisuitwisseling, internationale contacten etc. Dupliceert men die over veel opsporingseenheden op bijvoorbeeld regionaal niveau, dan is de efficiëntie sterk in het geding. Mede omdat belangrijke (private) gesprekspartners in de strijd tegen cybercrime op nationaal niveau zijn georganiseerd, en vervolgens met 25 verschillende opsporingseenheden zouden moeten overleggen over hun problemen. Bij de bestrijding van cybercrime zou een uitsluitend decentrale inrichting al snel tot inefficiëntie leiden.

Toegankelijkheid

Één van de problemen die zich in relatie tot de bestrijding van cybercrime voordoet, is de mogelijkheid om aangifte te doen. In de eerste plaats wordt dat al weinig gedaan, maar als men daartoe al besloten heeft is het thans niet eenvoudig om een deskundige ingang te vinden bij de opsporing en vervolging. De toegankelijkheid van de bestrijding van cybercrime als voorziening, dient voor de burger te zijn gewaarborgd. Daarin ligt een duidelijke taak voor de politieregio's als decentrale voorziening. Een taak die niet afwijkt van andere delictsoorten waarvan de burger als slachtoffer terecht moet kunnen bij een regionale voorziening. De kans op een aangifte wordt bovendien kleiner met het toenemen van de afstand tussen aangever en de

bestrijdingsorganisatie tot wie men zich moet wenden.
In het geval van bijzondere en exclusieve vormen van cybercrime zal er meestal geen sprake zijn van een uitsluitend lokaal slachtofferschap. Nationaal georganiseerde aangevers komen dan in beeld. Zij zijn juist gebaat met de mogelijkheid van het centraal doen van aangifte, bij bovendien een deskundige partner die van de specifieke context van de organisatie en haar dienstverlening op de hoogte is. Op dit niveau zullen vaak vooraf al afspraken worden gemaakt hoe in het geval van een cybercrimedreiging te handelen en als (potentieel) slachtoffer en bestrijdingsorganisatie gezamenlijk op te trekken.

5.5 Realisatie van gewenste functies: ontwerpvarianten

Eerder in dit hoofdstuk is vastgesteld dat in de gewenste opsporings- en vervolgingsfuncties betreffende cybercrime nog onvoldoende wordt voorzien. Vervolgens is een aantal ontwerpvraagstukken belicht dat een rol speelt wanneer men de gewenste opsporings- en vervolgingsfunctie wil beleggen binnen de organisatie van de handhaving en opsporing. De constateringen bij ieder ontwerpvraagstuk zijn uitgewerkt in drie varianten voor het inbouwen van de gewenste functies binnen de organisatie van de opsporing en vervolging.

5.5.1 Variant A: regionale organisatie van de opsporing en vervolging

De ingrediënten voor deze ontwerpvariant van de opsporing en vervolging van cybercrime bestaan uit: de Districtsrecherche, de Regionale divisie recherche en het arrondissementsparket.

In variant A, wordt de bestrijding van cybercrime zo dicht mogelijk op de plaats waar het vraagstuk zich manifesteert belegd. In casu is dat de politieregio. Beleggen kan op drie manieren plaatsvinden:

- door middel van het positioneren van organisatorische eenheden als teams of afdelingen;
- door het aanwijzen van taakaccenthouders met een deeltaak op het gebied van cybercrime;
- door het maken van productieafspraken over aan cybercrime gerelateerde aantallen processen-verbaal of andere producten.

In de regionale ontwerpvariant berust het gezag over de opsporing van cybercrime op het arrondissementelijk niveau met als exponent de hoofdofficier van Justitie. In beginsel komt de regionale variant 25 keer in het land voor zij het, naar gelang het vraagstuk, in uiteenlopende omvang. Het maken van handhavingafspraken is dan geen eenvoudige zaak. Buiten de derde partij met wie de afspraken worden gemaakt, zijn daar al 25 korpsen bij zijn betrokken. Hecht men aan een stuk centrale regie op de aanpak van cybercrime, dan is de regionale variant geen voor de hand liggende keuze.

De uitsluitend regionale variant heeft verder nog als nadeel dat moet worden afgewogen tussen lokale prioriteiten met een hoge ernstbeleving, en cybercrimezaken met een lage ernstbeleving.
Het voordeel van de regionale variant is de toegankelijkheid voor de aangever uit het regionale verzorgingsgebied, en de (theoretische) mogelijkheid tot het bieden van maatwerk. Op de punten slagvaardigheid, efficiëntie en schaalgrootte scoort deze variant negatief.

De internationale oriëntatie op het cybercrimevraagstuk is vanuit de regionale variant moeilijk zo niet onmogelijk waar te maken. Kiest men desalniettemin voor het positioneren van de bestrijding van cybercrime dicht op de bestaande verzorgingsgebieden, dan is de kans groot dat zo de bestrijding van cybercrime al aandacht krijgt, die zich uitsluitend gaat richten op lokale zaken. Dat is geen probleem voor de beperkte zaken waarbij een individuele computergebruiker het slachtoffer is. De politieregio overstijgende zaken lopen een risico om tussen wal en schip te raken. Een groot deel van de cybercrime die zich voordoet moet minimaal tot de middencriminaliteit en daarmee tot het taakveld van de Bovenregionale Recherche worden gerekend. Variant B sluit aan op deze bovenregionale structuur.

5.5.2 Variant B: bovenregionale organisatie van de opsporing en vervolging

De ingrediënten voor deze ontwerpvariant bestaan uit de politieregio's, de centrumregio, de Bovenregionale Recherche, de arrondissementsparketten en de centrumarrondissementsparketten.

De Bovenregionale Recherche verricht tactische en financiële opsporingsonderzoeken of handelt rechtshulpverzoeken af, naar vormen van middencriminaliteit die criminele groeperingen betreffen die in verschillende regio's actief zijn of criminele verschijnselen betreffen die zich in samenhang voordoen in het gehele land en de regionale recherchedienst van een politiekorps gedurende te lange tijd te zwaar zou belasten[7].
Taak van de Bovenregionale Recherche is ook het verrichten van zware en middelzware opsporingsonderzoeken en het afhandelen van rechtshulpverzoeken naar horizontale fraude in het samenwerkingsgebied of binnen het opgedragen taakaccent. De taak die eerder door de IFT's werd verricht. Hiertoe hoort ook het vervullen van de expertisefunctie op het gebied van horizontale fraude en financieel rechercheren en het in stand houden van een fraudemeldpunt op het aangewezen taakaccent.

In tegenstelling tot het beeld dat zich in het veld aan het vestigen is, opereert de Bovenregionale Recherche ten aanzien van dezelfde criminaliteitsterreinen als doorgaans de Districtsrecherches uit de politieregio's. Voor zowel Bovenregionale, Regionale en Districtsrecherche is de politieregio het uitgangspunt waar ook de zeggenschap berust. Zij opereren ook namens de politieregio. Alleen richt de Bovenregionale Recherche zich op onderzoeken van criminaliteit en criminele groeperingen waarvan meerdere politieregio's last hebben.

Formeel kent de BR geen specifieke aandachtsgebieden. Maar bij de positionering van de aanpak van de horizontale fraude en de milieutaak heeft men daarvan afgeweken. Naar analogie zou ook de bestrijding van cybercrime op bovenregionaal niveau kunnen worden belegd. Wil men ieder risico uitsluiten dat de voor de bestrijding van cybercrime beschikbaar gestelde capaciteit ook voor andere doeleinden kan worden gebruikt, dan is verbijzondering in een aparte eenheid aan te bevelen. Het maken van prestatieafspraken over het aantal uit te voeren onderzoeken of aan te houden verdachten, is een mildere vorm van sturing voor het geval men geen structuuroplossing wil die de flexibiliteit van de inzet van de BR beperkt.

[7] Regeling van 15 januari 2004 nr. EA2003/86484, DGOOV/Pol/BJZ, houdende de organisatie van de nationale en bovenregionale recherche en bepalingen over de samenwerking tussen de Nationale en Bovenregionale Recherche en de regionale politiekorpsen (regeling Nationale en Bovenregionale Recherche)

Overigens gaat de vergelijking tussen de milieutaak en de fraudebestrijdingstaak van de BR aan de ene kant en cybercrime aan de andere kant, op een aantal punten mank. Net als is opgemerkt bij de regionale variant A, zijn de internationale en de niet-regio gebonden kenmerken van cybercrime een probleem bij het koppelen van de bestrijding aan een bepaalde verzorgingsgebeid van de BR. Vrijwel per definitie zal zich voordoende cybercrime dat verzorgingsgebied overstijgen. Met wederom als gevolg dat de BR, als cybercrime-onderzoeken al door de weging heenkomen, zich zal gaan richten op die vormen van cybercrime met een sterke uitstraling in dat verzorgingsgebeid. Stijgt het daarboven uit, dan is de kans groot dat het veel minder op aandacht kan rekenen.

In de bovenregionale variant is de vervolgingstaak belegd bij het centrumarrondissement.

De bovenregionale variant past wel goed bij het inhoudelijk karakter van cybercrime dat in veel gevallen als middencriminaliteit is te kwalificeren. Op de aspecten schaalgrootte, efficiëntie en slagvaardigheid scoort de bovenregionale variant beter dan de regionale. Maar vanwege de bijna per definitie internationale aspecten van cybercrime is afhandeling in een bovenregionale voorziening in veel gevallen niet voldoende.

5.5.3 Variant C: nationale organisatie van de opsporing en vervolging

De nationale organisatie van de opsporing en vervolging van cybercrime is opgesplitst in twee subvarianten. De eerste gaat uit van onderbrenging van cybercrime als resultaatsgebied binnen de dienst Nationale Recherche (NR). De NR zelf en het Landelijk parket als bijbehorend gezag, zijn de belangrijkste ingrediënten van deze oplossingsvariant. Omdat de NR werkt met gedeconcentreerde eenheden volgens dezelfde schaal als de BR, kunnen vooruitgeschoven posten worden gecreëerd in de buurt van de politieregio's.

Volgens de regeling Nationale en Bovenregionale recherche[8] bestaan de kerntaken van de Dienst Nationale Recherche uit opsporen en tegenhouden. De NR werkt met aandachtsgebieden die zijn ontleend aan het Nationaal Dreigingsbeeld. Hoewel op basis van het Nationaal Dreigingsbeeld cybercrime niet als apart aandachtsgebeid voor de NR is benoemd, ligt op basis van de analyse in dit rapport een rol voor de NR wel voor de hand.

Een aanpak op nationaal niveau heeft schaal- en efficiëntie voordelen, die ook passen bij het karakter van de NR en haar internationale oriëntatie. De schaal van de NR en haar oriëntatie verhouden zich goed tot een vraagstuk als cybercrime, alleen de zwaarte van de onderzoeken voldoet wellicht niet altijd aan haar intakecriteria. Maar dat probleem is te ondervangen door die bestrijding net als in het geval van synthetische drugs als aandachtsgebied expliciet aan de NR op te dragen. In dat geval kan de (inter)nationale aandacht voor de bestrijding van cybercrime wel door de NR worden verzorgd. Wordt voor deze pragmatische maar goed te verdedigen benadering gekozen, dan bestaat er enig risico dat de aanpak van cybercrime meer de kant op wordt getrokken van digitale opsporing c.q. de bestrijding van terrorisme. In de keuze voor prioriteiten door het

[8] Regeling van 15 januari 2004 nr. EA2003/86484, DGOOV/Pol/BJZ, houdende de organisatie van de nationale en bovenregionale recherche en bepalingen over de samenwerking tussen de Nationale en Bovenregionale Recherche en de regionale politiekorpsen (regeling Nationale en Bovenregionale Recherche)

Landelijk parket dat de vervolgingstaak voor de NR vervult, zou hierop gestuurd moeten worden. Bijvoorbeeld op basis van de volgende (enigszins opgerekte) criteria waaraan een zaak zou dienen te voldoen om op nationaal niveau opgepakt te worden:

- Nationaal belang: de Staatsveiligheid, openbare orde (verstoring van) en veiligheid of democratische rechtsorde, is in geding;
- Vitaal: vitale sectoren of knooppunten zijn object van de criminele gedraging.
- Internationaal: het betreft het een internationaal of mondiaal probleem in combinatie met een bepaalde innovatiegraad.
- Innovatiegraad: het gaat het over een verschijningsvorm waarin een nieuwe technologie, een techniek of methodes gebruikt worden.
- Infectiegraad: complexe computersystemen en netwerken zijn geïnfecteerd en/of gemanipuleerd.
- Snel en daadkrachtig optreden: direct handelen en optreden op (inter)nationaal niveau is noodzakelijk om bedreigende situaties te voorkomen of te doen stoppen.
- Landelijke coördinatie. Er is (direct) landelijke coördinatie noodzakelijk (bijvoorbeeld dDOS-attack op vitaal systeem ten behoeve van de samenleving).
- Multi-jurisdictie: het strafbare feit heeft meerdere linken naar het buitenland.

Het ook onderbrengen van de bestrijding van bepaalde vormen van cybercrime bij de NR heeft schaal- en efficiëntievoordelen. Ook is er voor het buitenland één duidelijk aanspreekpunt. De toegankelijkheid voor landelijk georganiseerde aangevers is goed te regelen in een nationale variant, maar voor lokale aangevers is de grote afstand bijzonder lastig. Zij zullen behoefte blijven houden aan een lokaal aanspreekbare politie.

Balans

Wordt op basis van de zes organisatiekundige aspecten en de bovenbeschreven ontwerpvarianten de balans opgemaakt, dan zijn er diverse vormen van cybercrime die vragen om aanpak binnen de politieregio of op het niveau van gezamenlijke politieregio's, Het gaat met name om delicten waarvan de gemiddelde computergebruiker het slachtoffer is, en waarvan het op basis van het toegankelijkheidsprincipe belangrijk is dat men lokaal met een aangifte terecht kan. Zodat ook een duidelijk beeld ontstaat in welke mate juist de gemiddelde gebruiker slachtoffer wordt van cybercrime. Een beeld waarop vervolgens met maatregelen kan worden ingespeeld.

Daarnaast noodzaakt de schaal waarop cybercrime zich voordoet, de aard ervan en de wijze waarop waarop de partners in de bestrijding daarvan zijn georganiseerd, tot de behoefte aan een slagvaardige centrale voorziening. De noodzaak wordt versterkt door efficiency-argumenten.

5.6 Realisatie van gewenste functies: voorgesteld ontwerp

5.6.1 Inrichting van een landelijke voorziening

Er zijn verschillende varianten gepresenteerd, waar ook nog onderlinge combinaties van zijn te maken. Op basis van het uitgangspunt ‘zoveel mogelijk gebruik maken van bestaande structuren’, wordt een ontwerp voorgesteld dat past binnen de huidige indeling in Nederland qua rechercheniveaus.

Voor de realisatie van de gewenste opsporingsfuncties genummerd met 2, 3, 4 en 5 zal een nationale voorziening ingericht moeten worden. Op basis van de criteria schaalgrootte, moeilijkheidsgraad, slagvaardigheid en efficiency zou het beleggen van deze functies op het regionale of bovenregionale niveau onaanvaardbare nadelen met zich meebrengen. Binnen de huidige structuur van de opsporing is op nationaal niveau alleen de Nationaal Recherche actief om deze functies bij te beleggen. De kenmerken van het type opsporingsonderzoeken dat door de NR in behandeling wordt genomen en de schaal waarop de problematiek die in deze onderzoeken aan de orde is zich afspeelt, verhouden zich goed tot een groot deel van het cybercrimevraagstuk en haar verschijningsvormen. Derhalve wordt tevens voorgesteld om de daadwerkelijke opsporing van bijzondere en exclusieve vormen van cybercrime, (vallend onder opsporingsfunctie 1) te beleggen bij de Nationale Recherche. De politieregio’s blijven verantwoordelijk voor de (boven)regionale bestrijding van cybercrime en kunnen ter ondersteuning een beroep doen op de landelijke voorziening.

De toewijzing van de nationale bestrijdingstaak van cybercrime zal aan de NR moeten worden opgedragen. In eerste instantie voor een periode van drie jaar. Na verloop daarvan zal worden beschikt over een Nationaal Dreigingsbeeld voor cybercrime. Op basis van dat beeld kan definitieve besluitvorming plaatsvinden over de noodzaak tot de bestrijding van cybercrime en de plaats(en) waar die bestrijding het beste kan worden belegd. Dit advies past naadloos in de implementatiebenadering die gekozen is voor de Nationale Infrastructuur Bestrijding Cybercrime als geheel, waarin op basis van tijdelijke keuzes wordt gekomen tot een stevige onderbouwing voor permanente oplossingen.

In het verlengde van de positionering van de genoemde opsporingsfuncties bij de NR berust het gezag over de uitoefening van die functies bij het Landelijk Parket van het OM. De intake van opsporingsonderzoeken van bijzondere en exclusieve vormen van cybercrime zal onder toeleiding van informatie uit o.a. de Nationale Infrastructuur Bestrijding Cybercrime, plaatsvinden door het Landelijk Parket.

5.6.2 Feitelijke opsporing van cybercrime op alle rechercheniveaus

Voorgesteld wordt om de wijze waarop de opsporing in Nederland thans is georganiseerd, ook tot uitdrukking te brengen in de verdere organisatie van de opsporingsfunctie 1 (het verrichten van opsporingsonderzoeken naar cybercrime). Positionering bij de NR vindt alleen plaats voor die opsporingsonderzoeken met een nationaal en/of

internationaal karakter. Veel van de cybercrimevraagstukken zullen aan dit criterium voldoen, maar het laat onverlet dat zich ook op regionaal en bovenregionaal niveau cybercrimevraagstukken zullen voordoen. De aangifte- en opsporingsfunctie voor deze vormen van cybercrime blijft berusten waar die nu ook al ligt: bij de regionale politie. Zodat de toegankelijkheid van de opsporing voor de individuele gebruiker voldoende is gegarandeerd. Waar op dat niveau de vereiste deskundigheid voor het opnemen van aangiftes of het uitvoeren van een opsporingsonderzoek ontbreekt, zal voor feitelijke ondersteuning een beroep kunnen worden gedaan op de landelijke voorziening bij de NR. Wel zullen politieregio's ervoor dienen te zorgen dat zij over minimale deskundigheid terzake beschikken conform de aanbevelingen van het landelijk project digitale opsporing.

Ook wanneer politieregio's of de Bovenregionale Recherche ambtshalve onderzoeken op het terrein van cybercrime in behandeling nemen waarvoor ondersteuning is gewenst, kan men een beroep doen op de landelijke voorziening. De ondersteuning kan vervolgens variëren van het geven van advies tot en met daadwerkelijke participatie met personele capaciteit in onderzoeken. Omgekeerd zal ook personeel uit de politieregio's kunnen participeren in nationale opsporingsonderzoeken. Door de politieregio's opgenomen signalen en aangiftes vormen namelijk mede de basis voor onderzoeken van de landelijke voorziening. Uitwisseling van deze informatie in het kader van de Nationale Infrastructuur Bestrijding Cybercrime in het algemeen, en de opsporing en vervolging in het bijzonder is geen vrijblijvende aangelegenheid, en zal nadrukkelijk door de betrokken partijen worden georganiseerd. Dat impliceert dat de landelijke voorziening in voorkomende gevallen input verzorgt voor het wegingsproces dat aan de toewijzing van zaken door de Bovenregionale Recherche vooraf gaat. In het geval dat de landelijke voorziening wordt geconfronteerd met cybercrimevoorvallen waarbij het accent ligt op het regionale of bovenregionale niveau, dan zal terzake door de landelijke voorziening een pre-weegvoorstel worden opgesteld ten behoeve van de politieregio of de BR waarop het accent met name betrekking heeft. In het pre-weegvoorstel zal nadrukkelijk de mogelijke bijdrage van de landelijke voorziening zelf aan een eventueel opsporingsonderzoek worden beschreven.

Het gezag over de (boven-)regionale opsporing van cybercrime volgt de reguliere wijze waarop dat gezag is georganiseerd. Net als voor de landelijke opsporingsvoorziening, geldt ook voor de arrondissementen dat men een beroep kan doen op vervolgingsondersteuning door het Landelijk Parket.

5.6.3 De vorm van de voorziening

Naast de uitvoering van haar expertisetaken, zal de landelijk voorziening tegelijkertijd twee tot vier strafrechtelijke onderzoeken kunnen verrichten van gemiddelde grootte. Per jaar zullen minimaal twee onderzoeken van deze omvang worden afgerond. Daarnaast zullen kleinere onderzoeken worden verricht en zullen onderzoeken binnen de politieregio's worden ondersteund. Rechtshulpverzoeken zullen op de gebruikelijke manier worden afgehandeld, en niet uitsluitend door de Nationale Recherche.

Op basis van ervaringen uit het project NHTCC, uit lopende onderzoeken en een afgerond groot onderzoek, blijkt dat voor een onderzoek van gemiddelde grootte ongeveer 15 fte's noodzakelijk zijn. Om daarnaast ook nog een expertisefunctie te kunnen vervullen is uiteindelijk in totaal een teambezetting noodzakelijk van circa 36 ft (inclusief beheersmatige ondersteuning). Deze zal echter niet direct vanaf het begin zijn gerealiseerd. Op grond

van ervaringen van soortgelijke buitenlandse opsporingsteams is het niet ondenkbaar dat de voorziening op termijn zal moeten uitbreiden om het groeiende werkaanbod aan te kunnen. De totale kosten in de voorgestelde opzet, worden geraamd op 3,7 mln euro per jaar. Aan het KLPD zal moeten worden gevraagd om te komen met een nader onderbouwd voorstel.
De kosten voor de landelijke OM-voorziening zijn niet afzonderlijk begroot, maar zullen voor de voorlopige duur van de voorziening (drie jaar), door het OM zelf worden gedragen.

Bij de vorming van de nationale opsporingsvoorziening zal gebruik worden gemaakt van de opgedane kennis en ervaring die zijn verkregen tijdens het NHTCC-project en het NPAC-project. Een groot aantal activiteiten die in het project NHTCC zijn ondernomen zullen worden voorgezet in respectievelijk de nationale voorziening en de Nationale Infrastructuur Bestrijding Cybercrime. Hiermee wordt ervoor gezorgd dat kennis en ervaring worden behouden en verder worden uitgebouwd. Een belangrijk uitgangspunt bij het vormgeven van de landelijke voorziening is dat de noodzakelijke bijzondere expertise en kennis weerspiegeld wordt in de personele samenstelling van de voorziening. Dat houdt in dat het merendeel van de medewerkers die opsporingsonderzoeken naar bepaalde vormen van cybercrime uitvoert niet alleen affiniteit heeft met de specifieke thematiek, maar met name beschikt over een hoog niveau van (digitale en internet) expertise naast of aangevuld met recherchevaardigheden. Daarnaast zal in de voorziening bijvoorbeeld ook, een wetenschappelijke component herkenbaar zijn ten behoeve van (criminaliteitbeeld)analyses en informatiemedewerkers ten aanzien van het intelligence proces. Tot slot wordt in deze voorziening ook de liasonfunctie voor de Nationale Infrastructuur Bestrijding Cybercrime gerealiseerd.

Hoofdstuk 6 Implementatie

Heel snel kan op zijn minst het hart van de Nationale Infrastructuur voor de bestrijding van cybercrime worden gerealiseerd. Dit hoofdstuk beschrijft waarom niet tot directe structurele reorganisaties is geadviseerd. Met als belangrijkste argument om niet in de valkuil terecht te komen van wederom het creëren van een 'oplossing' zonder dat het probleem duidelijk is. Vandaar dat een implementatiestrategie is ontwikkeld die voorkomt dat er onomkeerbare stappen worden gezet in mogelijk de verkeerde richting, maar ondertussen de principes van een Nationale Infrastructuur wel uittest. Zodat ze alvorens daadwerkelijk structureel te worden gemaakt zich in de praktijk al dan niet hebben bewezen. Ondertussen levert de implementatiestrategie niet alleen organisatorische inzichten op, maar wordt er gelijktijdig in de praktijk al inhoud gegeven aan de bestrijding van cybercrime. Dit hoofdstuk beschrijft ook dat de twee bestaande projecten NHTCC en NPAC in dit programma bij elkaar komen. Daarmee wordt gewaarborgd dat de kennis en expertise die is opgedaan in het project NHTCC maximaal benut kan worden.

6.1 De implementatieambitie

Het woord implementatie suggereert wellicht dat de ontwerpkeuze al wordt vastgelegd en het alleen nog de vraag is hoe die in te voeren. Een onjuiste suggestie, omdat uit de implementatie ook moet blijken of het ontwerp zoals het is bedacht ook daadwerkelijk gaat brengen wat er van wordt verwacht. Met name of het een antwoord is op het juiste probleem. Aan de andere kant: het ontwerp is ook niet zomaar uit de lucht gegrepen en wel degelijk gebaseerd op noties over de omvang van cybercrime als probleem, en over het krachtenveld van actoren en belangen waarbinnen bestrijding plaatsvindt. Het essentiële van de implementatieambitie is dat de bestaande actoren die direct of indirect zijn betrokken bij de bestrijding van cybercrime zich materieel al gaan gedragen conform de gedachten achter het ontwerp voor een Nationale Infrastructuur. Dat levert twee voordelen op:

- toetsing van de noties achter de infrastructuur aan de hand van de praktijk;
- concreet resultaat in de bestrijding van cybercrime.

In plaats van traditionele implementatietrajecten waarin er eerst een tijd gebouwd wordt en er daarna pas op inhoudelijk resultaat mag worden gerekend, wordt in de implementatieambitie in relatie tot cybercrime het resultaat gebruikt als voertuig voor implementatie. Ondertussen verandert er organisatorisch niets structureel. Hooguit zullen in de vorm van projectmatige inzet medewerkers van de ene dienst eens over de schutting kijken van de andere dienst of in de keuken van een bepaald veld waarop men zich normaal gesproken niet beweegt. Het voorstel is om de gedachten achter de Nationale Infrastructuur toe te passen te toetsen binnen vier sectoren: MKB, grote industrie, financiële instellingen en decentrale overheid. Die sectoren bestrijken niet het hele spectrum van cybercrime, maar wel een belangrijk deel. Ze zijn aan de ene kant gekozen vanuit de veronderstelling dat er sprake is van een aantal witte vlekken in relatie tot de door deze sectoren ervaren

problemen. Aan de andere kant bestaat ook het vermoeden dat binnen de sectoren veel informatie over cybercrime en verschijningsvormen is af te leiden die ook dienst baar kan zijn voor de bestrijding gericht in andere branches. En tot slot is de gedachte achter de keuze voor juist deze vier sectoren dat als het concept voor hen blijkt te werken, het ook beter zal aansluiten op de in het veld ervaren cybercrime-problematiek. Als belangrijk onderdeel van de implementatie zal het concept achter de Nationale Infrastructuur toegepast worden binnen de sectoren zij het op kleine schaal middels experimenten. Bij die toepassing worden de organisaties ingeschakeld die nu al direct of indirect bij de bestrijding van cybercrime zijn betrokken. In het kader van de implementatieambitie zal parallel aan de experimenten gestart worden met het organiseren van de publiek-private informatie-uitwisseling.

Op basis hiervan wordt voor wat betreft de in hoofdstuk 4 genoemde functies bekeken waar nog witte vlekken voorkomen en wordt bepaald of deze vlekken ingevuld kunnen worden door bestaande organisaties danwel een nieuwe organisatievorm vergen. Daarmee wordt invulling gegeven aan de in de ontwerpscenario's genoemde uitgangspunten.

Waardevolle constateringen die tijdens de toepassingen worden gedaan en waarvan het onverstandig zou zijn om er pas iets mee te doen nadat het implementatietraject is afgerond, worden al tijdens het implementatietraject uitgezet en verbreed. Ook onder de sectoren waarin geen experiment plaatsvindt. Feitelijk wordt op die manier al toegewerkt naar een gewenste situatie. De praktijk profiteert al ten tijde van het implementatietraject van de uitkomsten.

Onderdeel van de implementatieambitie is ook het ontwerp voor de aanpak van cybercrime door opsporing en vervolging. Inclusief de relaties tussen opsporings- en vervolgingsinstanties en de andere actoren die in het implementatieproces zijn betrokken.

6.2 Sectoren waarop de implementatie specifiek betrekking heeft

Bij de bestrijding van cybercrime komt het MKB naar voren als een moeilijk te bereiken en sterk heterogene doelgroep met een hoog slachtofferrisico en een gering geëffectueerd en georganiseerd risicobewustzijn. Slachtoffer als gevolg van het zelf schade ondervinden door cybercrime, maar ook slachtoffer door zonder dat men het weet mee te werken aan de schade die anderen oplopen door bijvoorbeeld gegijzelde computers. In de keuze voor het MKB als basis voor toepassing van de filosofie achter de Nationale Infrastructuur is bevestiging gevonden door de algemene voorlichtende activiteiten van o.a. het programma Kwint, en de zorg bij VNO-NCW over de geringe daadwerkelijke ondersteuning van het MKB indien slachtoffer van cybercrime.

Als tweede focus is gekozen voor financiële instellingen te beginnen met banken. Recent is middels een aantal wel en niet gepubliceerde voorvallen (gestolen creditcardgegevens, phishing Postbank) gebleken hoe het consumentenvertrouwen onder druk kan komen te staan door cybercrime. Juist waar de daders zich vrijwel per definitie buiten de landsgrenzen ophouden, is samenwerking geboden om schadetoebrengende gedragingen te stoppen.

Als derde focus is gekozen voor de grote industrie. Niet zozeer op basis van de veronderstelling dat men weinig besef heeft van de risico's van cybercrime en daarop onvoldoende zou zijn ingericht (hoewel zelfs dat in brede kring wordt betwijfeld), maar vooral ook vanwege het internationale netwerk dat men vertegenwoordigt en vanwege het algemeen belang dat hiermee gemoeid is. Daardoor kan het optreden van bepaalde vormen van cybercrime mogelijk snel worden gedetecteerd, hetgeen ten goede zou kunnen komen aan andere sectoren en de daarop gerichte preventie-inspanningen. Op haar beurt zou de grote industrie kunnen profiteren van de internationale contacten van bijvoorbeeld organisatie die in de implementatie mee doen, om bepaalde gedragingen te doen stoppen. Tot slot wordt verondersteld dat de grote industrie én bron én afnemer kan zijn van kennis bij het voorkomen, signaleren en bestrijden van cybercrime of het bieden van de gelegenheid daarvoor. Bij voorkeur wordt er hier gekozen voor een sector uit de groep van de zogeheten vitale infrastructuren.

Als vierde focus is gekozen voor de decentrale overheid. Een keuze die is gebaseerd op signalen van GOVCERT en die lijken te duiden op een vergelijkbare situatie bij bijvoorbeeld kleine gemeenten als die is aangetroffen binnen het MKB.

6.3 Één verstevigd project: NPAC en NHTCC bij elkaar

In de afgelopen periode is door het project NHTCC en het project NPAC gewerkt aan verdere invulling van de bestrijding van cybercrime. In dit ontwerp komen beide ontwikkelingslijnen bij elkaar tot één ontwikkelingslijn, met als basis wat al gerealiseerd is in de afzonderlijke projecten.

1. Richt op korte termijn een programma in dat de praktijktoetsing en realisatie van de Nationale Infrastructuur tot doel heeft. Hiertoe zal een plan van aanpak worden opgesteld.
2. Het programma wordt een onderdeel van het Actieplan Veilig Ondernemen 2 en komt daarmee onder de vlag van het NPC.
3. De activiteiten gericht op het tot stand brengen van het meldpunt cybercrime worden vooralsnog onder de verantwoordelijkheid van het KLPD gebracht.
4. Het begrip NHTCC wordt exclusief gereserveerd voor de toekomstige politie-eenheid gericht op opsporing en vervolging van cybercrime. Het bouwen/toerusten van (een) opsporingsorganisatie(s) binnen het OM en de Nederlandse Politie is de eerste verantwoordelijkheid van het landelijk parket en het KLPD. Vanuit het programma worden hand- en spandiensten verricht ten behoeve van de bouw van het NHTCC. Hetzelfde geldt voor de ondersteuning van ontwikkelingen in andere sectoren.
5. Het programma wordt aangestuurd door één vanuit het NPC gemandateerde opdrachtnemer.

6.4 De implementatiefilosofie

Het implementatieprogramma heeft niet de bedoeling uit te groeien tot een zelfstandige organisatie. Het implementatieprogramma maakt op een slimme wijze gebruik van krachtenvelden bestaande uit actoren en hun belangen, waardoor dat ook niet nodig is. In plaats van die belangen te vervangen door één gemeenschappelijk

belang, worden belangenverschillen gelegitimeerd. Om er vervolgens naar te streven er zoveel mogelijk afzonderlijk aan tegemoet te komen. Een dergelijke strategie heeft alleen kans van slagen als op enige wijze de producten van het programma aansluiten op een belang van de beoogde adoptanten In de professionele omgevingen waarin zowel de slachtoffers (bijvoorbeeld bedrijven) als de bestrijders functioneren is het overnemen van elkaars plannen geen automatisme. Het ‘not invented here syndroom’ wordt als kenmerk van professionele organisaties door diverse auteurs uit de doeken gedaan. Wil desondanks een krachtenveldbenadering succes hebben, dan dient in het algemeen gesproken te worden voldaan aan vier factoren:

1. er moet bij de actor wiens medewerking is vereist een belang zijn/worden aangebracht (latent of manifest);
2. het belang moet worden getriggerd;
3. het belang moet op zijn minst enige tijd worden gediend;
4. het product of idee moet een zekere exclusiviteit kennen:
    a. omdat het nog niet eerder is vertoond en de beoogd adoptant er eer mee in kan leggen;
    b. de beoogde adoptant kan het product of idee niet elders (tegen gunstiger voorwaarden) betrekken.

6.5 Het besluitvormingsproces ten tijde van de implementatie

Een implementatieprogramma dat zowel praktijktoetsing als het invoeren van oplossingen nastreeft op basis van de toetsresultaten, vereist een actief besluitvormingsproces tijdens het verloop van het programma. De kenmerken van het vraagstuk dat onderwerp is van het programma, zullen doorwerken op het programma en op het besluitvormingsproces. Het programma moet qua uitvoering flexibel zijn en actief gebruik maken van (nieuwe) ontwikkelingen, inzichten en behaalde tussenresultaten. In die zin is het implementatietraject op zich zelf al een experiment in het ontwikkelen van en oefenen met besluitvormingsprocessen die passen bij een zich dynamisch ontwikkelend vraagstuk. Zoveel is wel duidelijk, dat de werkelijkheid van het steeds wisselende vraagstuk van cybercrime zich niet laat structuren aan de hand van vaste ambtelijke procedures. Daarmee is ook geadviseerd om niet alleen organisatorische thema’s of bedrijfsvoeringaspecten onderdeel van het besluitvormingsproces te maken, maar vooral ook de inhoud van het cybercrimevraagstuk. Een en ander conform de eerder in deze notitie geïntroduceerde uitgangspunten die niet uitsluitend van toepassing zijn op het ontwerp en daarmee af, maar ook op het beleidsproces op basis waarvan het ontwerp moet worden aangestuurd en moet opereren.

6.6 De organisatie van het implementatieprogramma

In de implementatiefase komt capaciteit beschikbaar om het programma te bemensen en te coördineren, maar het is nadrukkelijk de bedoeling dat in de uitvoering een centrale plaats wordt ingeruimd voor organisaties die al bij de bestrijding zijn betrokken. De programmacapaciteit zal bij aanvang vooral in ontwikkelactiviteiten gaan zitten en in het mobiliseren van actoren die bij de bestrijding van cybercrime zijn betrokken of kunnen worden betrokken. Tijdens de implementatiefase nemen de ontwikkelactiviteiten af en de beheeractiviteiten toe.

6.6.1 Een ontwikkelomgeving

Het implementatieprogramma wil op zichzelf al zoveel mogelijk een voorloper zijn van de gewenste structuur voor de aanpak van cybercrime. Consistent daarmee vormt de programmabezetting weliswaar de kern van de ontwikkelomgeving, maar wordt de inbreng van vertegenwoordigers van actoren uit het veld daaraan verbonden, zodat er al iets ontstaat van 'human interfaces' en een Nationale Infrastructuur. De ontwikkelomgeving valt onder de verantwoordelijkheid van een kwartiermaker, die rechtstreeks verantwoording aflegt aan de opdrachtgever. Op zijn beurt legt deze verantwoording af aan het NPC. De ontwikkelomgeving is per definitie tijdelijk. Opgeleverde en geïmplementeerde producten gaan over van de ontwikkelomgeving naar de bestaande of op te richten organisaties. Ze vallen vanaf dat moment niet meer onder de verantwoordelijkheid van het implementatieprogramma. Op deze manier wordt voorkomen dat de ontwikkelomgeving op zichzelf belang krijgt bij instandhouding, verbreding of inkleuring van het project. De ontwikkelomgeving kent maar één belang: het neerzetten van een werkende Nationale Infrastructuur. Vanuit deze positie blijft de ontwikkelomgeving gefocust op haar primaire opdracht. Bovendien kan zij die beheeromgeving voor producten zoeken die daarbij het beste past, zonder dat de eigen positie daarbij in het geding is. Zou de ontwikkelomgeving ook verantwoordelijk worden voor het beheer, dan ontstaat een eigen belang waardoor de kans groter is dat producten in eigen beheer worden genomen terwijl dat voor de bestrijding van cybercrime wellicht niet de beste oplossing is. Op deze manier kan het implementatieprogramma zich ook blijven gedragen als luis in de pels zonder daarbij last te hebben van bijbedoelingen. Dat komt het gezag van het implementatieprogramma ten goede.

Door de ontwikkelomgeving worden de volgende activiteiten uitgevoerd.

- Begeleiden en evalueren van experimenten binnen de vier sectoren, en het op basis daarvan vormen van de permanente Nationale Infrastructuur;
- Casestudy van het feitelijk verloop van bestrijdingsacties in de praktijk en de uitwerking daarvan in de opgezette Nationale Infrastructuur;
- Voorstellen voor het oplossen van positioneringvraagstukken van cybercrime ten opzichte van andere initiatieven en ontwikkelingen; Hierbij moet gedacht worden aan de positionering ten opzichte van de uitwerkingen van het programma Bescherming Vitale Infrastructuren (BVI), de initiatieven vanuit het beleidsdossier terrorismebestrijding, initiatieven van de OPTA, het programma Veilige Elektronische Communicatie van het Ministerie van EZ/ECP.nl en de Consumenten Autoriteit i.o.; de oprichting van een platform voor ICT en vitale sectoren; het operationeel Incident response team overleg (O-IRT-O); internationale ontwikkelingen;
- Voorstellen voor de (inter)nationale aanpak van cybercrime op basis van informatie aangeleverd door de bij het programma betrokken partijen;
- Voorstellen voor nadere uitwerking van de informatiefilosofie en het opzetten van de gemeenschappelijke informatie-uitwisselingstructuur;
- Monitoren of alle processtappen, functies en doelgroepen in relatie tot de bestrijding van cybercrime voldoende zijn afgedekt (witte vlekken) en het doen van voorstellen wanneer dat niet het geval is;
- Afronding van de activiteiten van het NHTCC project gericht op Schiphol als vitale structuur;
- Ondersteuning van de ontwikkeling van een digitaal crisisbeheersingsplan.

Voor alle activiteiten geldt dat ze samen met de organisaties in de Nationale Infrastructuur en de daaraan deelnemende organisaties worden uitgevoerd. De ontwikkelomgeving neemt geen verantwoordelijkheden over van bestaande organisaties.

6.6.2 Een beheeromgeving

De beheeromgeving bestaat uit de bestaande organisatie in de Nationale Infrastructuur. In de beheeromgeving worden die producten ondergebracht die voor langere periode een bijdrage kunnen leveren aan de aanpak van cybercrime. In feite is de beheeromgeving na afronding van het implementatietraject gewoon gelijk aan de Nationale Infrastructuur geworden. De producten die de ontwikkelomgeving voortbrengt krijgen een plaats in de beheeromgeving. Maar ondertussen zijn er ook anderen actief in de bestrijding van cybercrime of vinden elders ontwikkelingen plaats die daaraan raken. Ook deze krijgen een plaats in de beheeromgeving. De ontwikkelomgeving is dus geen exclusief kanaal voor de beheeromgeving. Het begrip beheeromgeving roept iets op van één organisatie, maar dat is niet de bedoeling. Per product wordt bekeken wat de beste plaats is om het product onder te brengen. In feit speelt dat keuzeproces al bij de productontwikkeling. Op die manier is de flexibiliteit van het positioneren van bepaalde producten optimaal. Omdat de ontwikkelomgeving geen eigen belang heeft, blijft dat ook zo gedurende het hele implementatietraject.

Producten die nu al in aanmerking om ergens in de beheeromgeving te worden ondergebracht zijn:

- Het vertrouwelijk informatienetwerk ccWiki. Op basis van een gedeeltelijke vaste structuur van de informatie kunnen diegenen die toegang hebben tot de ccWiki op een laagdrempelige wijze informatie krijgen over een breed scala aan aspecten op het gebied van cybercrime;
- Bestaande samenwerkingsverbanden. Hiervoor geldt dat deze op grond van de uitkomsten van één van de activiteiten in de ontwikkelomgeving kunnen leiden tot aanpassing. Te denken valt aan het operationeel Incident Response over (O-IRT-O) en de samenwerking met het Financial Institutions-Information Sharing and Analysis Center (FI-ISAC) van de Nederlandse Vereniging van Banken;
- Door middel van het ontwikkelen en uitvoeren van een jaarlijks terugkerende survey zoals voor de eerste maal uitgevoerd in het kader van het NHTCC project, komt er meer inzicht in de aard en omvang van High Tech Crime. Deze survey moet op de Nederlandse situatie zijn afgestemd en internationaal vergelijkingsmateriaal opleveren. Bovendien levert het input op ten behoeve van het Nationaal Dreigingsbeeld, een te ontwikkelen Digitaal Crisisbeheersplan en bruikbare resultaten voor andere verschillende doelgroepen, zoals openbaar bestuur, opsporing, ICT- en security management;
- De ontwikkelingen en verschijningsvormen van cybercrime worden met behulp van een trendanalyse- en volgmodel periodiek in een trendrapportage beschreven.

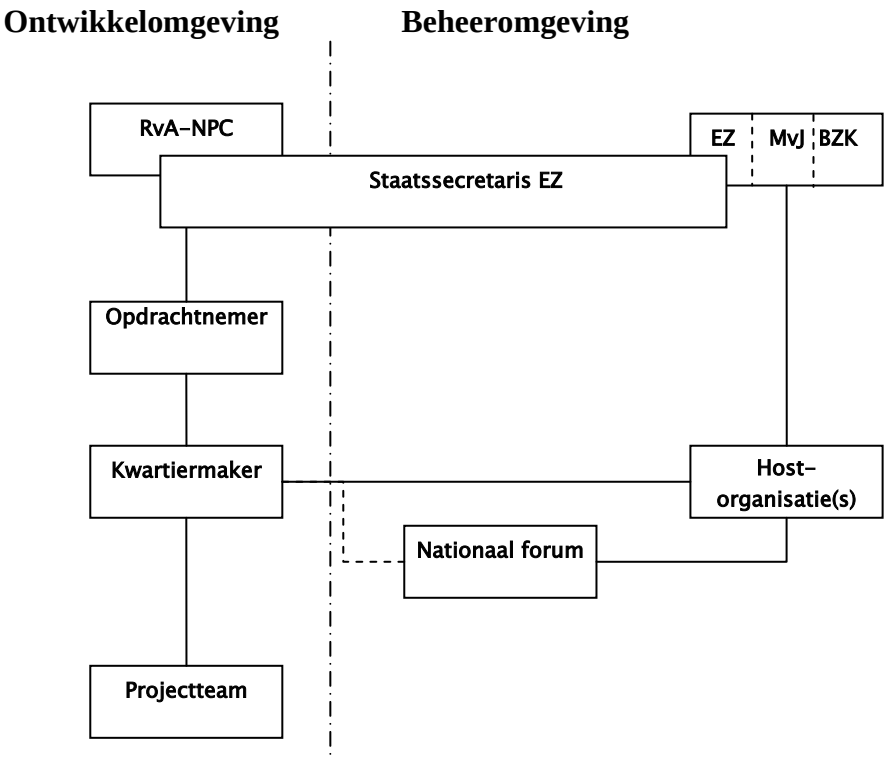
6.7 De begeleidingsstructuur

De begeleidingsstructuur van het implementatieprogramma is zo eenvoudig mogelijk gehouden. Formeel opdrachtgever is de Raad van Advies van het NPC. Namens de Raad van Advies wordt deze taak behartigd door de Staatssecretaris van Economische Zaken. Zij benoemt een opdrachtnemer met voldoende gezag naar het

betrokken veld. De opdrachtnemer stuurt actief een kwartiermaker aan die is belast met de uitvoering van het implementatietraject. Het ministerie van Economische Zaken is primair verantwoordelijk voor de afstemming met de collega-departementen van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties. Voor de coördinatie tussen de beleidsverantwoordelijke departementen zal een beleidsoverleg worden ingericht.

Er wordt als onderdeel van de beheeromgeving een nationaal forum cybercrime ingesteld. Het forum is uitsluitend bedoeld om van gedachten te wisselen over de inhoudelijke aanpak van cybercrime en de visie daarop vanuit verschillende betrokkenen. Het forum staat vooral ten dienste van de beheeromgeving. Tijdens het implementatieprogramma zal ook de kwartiermaker zich van het forum kunnen bedienen voor inhoudelijke probleemverkenning. Het forum kent een eigen voorzitter. Om haar inhoudelijke oriëntatie te benadrukken, heeft het forum heeft geen directe relatie naar de opdrachtgevende instanties.

De host-organisaties zijn organisaties die door de ontwikkelomgeving opgeleverde producten een structurele basis geven. Van de kennis, ervaring en inbreng vanuit de host-organisaties verzekert de ontwikkelomgeving zich ook tijdens het implementatietraject. Per deelproject of activiteit kan de betrokkenheid van host-organisaties wisselen.



6.8 Middelen, planning en fasering

De kosten voor het programma zijn begroot op circa vier miljoen euro. Eventueel budgettair beslag in de beheeromgeving valt buiten deze begroting. Hiervoor zal in voorkomend geval door de verantwoordelijke departementen een besluit over worden genomen.

Bij de start van een project is het gebruikelijk om de einddatum concreet vast te stellen. Bij het implementatieprogramma is dat in zoverre lastig dat er geen sprake is van een lineaire fasering maar van parallelschakeling van activiteiten. Ontwikkeling en implementatie trekken gelijktijdig met elkaar op. Zodra een oplossingsrichting zich in de praktijk voldoende heeft bewezen, vindt implementatie plaats binnen een bestaande of eventuele aan te bouwen of nieuw te bouwen organisatie. Het implementatieprogramma zal naar verwachting twee jaar duren. Dit betekent echter geenszins dat de Nationale Infrastructuur twee jaar op zich laat wachten. Vanaf de start van het programma wordt gewerkt volgens dit model. Na afloop van het programma is de Nationale Infrastructuur tegen de bestrijding van cybercrime volledig operationeel. Hetzelfde geldt voor de in te richten functies rond de opsporing en vervolging.