VERANTWOORDING

Project
High Tech Crime

februari 2006

Bijlage bij 'Ontwerp Nationale Infrastructuur Bestrijding Cybercrime', maart 2006

INHOUDSOPGAVE

1. Inleiding

Dit is de verantwoording van het project High Tech Crime met daarin een beschrijving van de activiteiten en de bevindingen in het kader van High Tech Crime. Dit document is geschreven in opdracht van de Stuurgroep High Tech Crime, bestaande uit leden van de ministeries van BZK, Justitie en EZ, een vertegenwoordiger van het OM en voorgezeten door de plv. Korpschef van het KLPD.

Speciale aandacht verdient de samenwerking met het project NPAC. Als resultaat van deze samenwerking heeft de stuurgroep in het najaar besloten geen eigen advies meer uit te brengen. De in dit project opgedane ervaringen zullen, samen met de ervaringen uit het project NPAC, leiden tot één advies aan de bewindslieden van de drie betrokken departementen. In dat advies zal onder meer worden ingegaan op de organisatorische inbedding van de aanpak van High Tech Crime. Dat is ook de reden dat er in deze verantwoording verder geen organisatorische voorstellen gedaan worden.

De inzichten die zijn verworven door het project High Tech Crime zijn verwerkt in het NPAC/NHTCC adviesontwerp 'nationale infrastructuur bestrijding cybercrime'. In de onderhavige projectverantwoording wordt door middel van omkaderde teksten aangegeven op welke wijze de inzichten en aanbevelingen van het project High Tech Crime een plek hebben gevonden in het NPAC/NHTCC advies. Deze wijze van verslaglegging geeft de lezer dan ook direct inzicht in de gezamenlijke visie van het project High Tech Crime en het NPAC ten aanzien van de nationale infrastructuur ter bestrijding van cybercrime.

Leeswijzer

Met het toenemende gebruik van ICT dienen zich steeds nieuwe vormen van High Tech Crime aan. De ICT-criminelen zoeken niet meer alleen naar de makkelijkste manier om eenvoudig geld te verdienen, maar richten zich ook op politieke motieven en van daaruit mogelijk zelfs op de ontwrichting van de informatie-infrastructuren zelf. In hoofdstuk 3 wordt hier nader op ingegaan. Dit wordt in hoofdstuk 2 voorafgegaan door een korte procesbeschrijving van het verloop van het project High Tech Crime.
In hoofdstuk 4 wordt vervolgens ingegaan op de activiteiten die het project heeft ondernomen om een beter inzicht te krijgen in de verschillende problemen van cybercriminaliteit en dat de basis van een gedegen advies kan zijn.
In hoofdstuk 6 worden de bevindingen omgezet in aanbevelingen op basis van enkele uitgangspunten en criteria die in hoofdstuk 5 worden beschreven.

In het afgelopen jaar hebben vele mensen meegedacht over en meegewerkt aan de activiteiten van het project. Het projectteam dankt iedereen hiervoor hartelijk.

2. Procesbeschrijving Project High Tech Crime

In dit hoofdstuk wordt ingegaan op de werkwijze en het verloop van het project HTC.
Centraal in het werk van het project stond de term 'learning by doing'. Aan de hand van werkzaamheden in de praktijk en vele discussies met de betrokkenen werd getracht inzicht te krijgen in de wijze waarop High Tech Crime het best kon worden aangepakt. In het project hebben in totaal circa 10 mensen deelgenomen gedurende de gehele projectperiode. Daarnaast zijn er in de periode tussen juli en november nog enkele politiefunctionarissen gedetacheerd geweest met als specifieke opdracht mee te werken aan het opsporingonderzoek High Tech Crime in opdracht van de Nationale Recherche.

2.1 Projectopdracht en aanpassing

In oktober 2004 is het project High Tech Crime gestart met als opdracht te werken aan de realisatie van een effectieve en efficiënte bestrijding van High Tech Crime. Hieraan voorafgaand is uit een verkenning gebleken dat er onvoldoende aandacht is voor de groeiende High Tech Crime problematiek.
De opdracht is als volgt verwoord:
"High Tech Crime is een internationaal fenomeen, dat middels het internet alle geledingen van de samenleving in (meer of minder) ernstige mate kan compromitteren/hinderen, belemmeren en er misbruik van kan maken. Het kan daarbij zowel als middel voor de uitvoering van bestaande vormen van criminaliteit en als doel voor nieuwe vormen van criminaliteit worden gehanteerd. Er is nog onvoldoende kennis, expertise en ervaring in de samenleving aanwezig, zowel privaat als publiek (inclusief opsporing), om de aanpak en bestrijding van High Tech Crime effectief en efficiënt te kunnen realiseren. De voortdurend snelle doorontwikkeling van High Tech Crime is een extra complicerende factor, terwijl het ontbreken van een integraal inzicht en optreden dit nog versterkt.
De opdracht heeft dan ook primair als doel de proactieve taak van de overheid en meer specifiek van de politie op het gebied van de bestrijding van ICT criminaliteit vorm te geven. Het project moet aantonen op welke wijze dreigingen en criminele activiteiten op dit gebied niet alleen kunnen worden opgespoord, maar vooral ook kunnen worden voorkomen of tegen gehouden.
Randvoorwaardelijk is gesteld dat deze proactieve taak in een internationaal en multi-agency verband wordt uitgevoerd en zal leiden tot publiekprivate samenwerking.
Nader uitgewerkt behelst de opdracht van het project High Tech Crime de volgende doelstellingen:

a. *het realiseren van een goed intakeproces en (inter-)nationale loketfunctie voor High Tech Crime;*
b. *inzicht te verkrijgen in aard, omvang en impact van de diverse uitingsvormen van High Tech Crime en de mogelijke consequenties voor vitale knooppunten en sectoren;*
c. *dreigingen door High Tech Crime proactief te signaleren, erover te adviseren en de adviezen in een brede context weg te zetten;*
d. *(inter-)nationale multidisciplinaire en multi-agency samenwerking te realiseren ten behoeve van de bestrijding van High Tech Crime."*

Het project High Tech Crime kreeg één jaar om deze opdracht te verwezenlijken.

In de periode mei-juni zijn er enige aanpassingen aangebracht in de projectopzet, die vooral betrekking hebben gehad op de betere positionering van het project en op de aanscherping van de te verrichten activiteiten. Als hoofdbestanddeel van de projectresultaten werd verzocht om het uitbrengen van een advies met betrekking tot de inhoudelijke én organisatorische aanpak van zware cybercriminaliteit in, dan wel via Nederland. Onderhavige projectverantwoording heeft vooral betrekking op de informatievergaring en analyse fase die ten grondslag heeft gelegen aan de advisering. Het uiteindelijke advies heeft een plek gekregen in (gezamenlijke) NPAC/NHTCC adviesontwerp 'nationale infrastructuur bestrijding cybercrime'.

2.2 Werkconferenties

Eén van de belangrijkste aspecten bij de aanpak van cybercrime is samenwerking. Samenwerking zowel met publieke als met private partijen. Dit werd opgepakt, niet alleen met diverse bilaterale contacten, maar ook met behulp van discussie met de meest betrokken organisaties en personen in dit werkveld. Daartoe zijn twee werkconferenties georganiseerd, één op 20 juni en één op 16 september van dit jaar.
Op de eerste conferentie, waaraan door circa 60 mensen werd deelgenomen, stond de open discussie over een drietal thema's centraal. In werkgroepverband werd gesproken over:

- de wijze waarop publiekprivate samenwerking voor de aanpak van HTC het best kan worden vormgegeven;
- de wijze waarop informatie-uitwisseling en opsporing bij elkaar gebracht kunnen worden;
- de verbanden tussen vitale infrastructuren en High Tech Crime.

Ook de tweede bijeenkomst op 16 september werd goed bezocht. In deze sessie werd meer naar de invulling van de informatie-uitwisseling gekeken en de naar de manier waarop het NHTCC gepositioneerd zou kunnen worden.
De uitkomsten van beide werkconferenties hebben veel invloed gehad op het vervolg van het project en op het uiteindelijke resultaat van dit document. Zo is het model voor de informatie-uitwisseling dat is gepresenteerd in de laatste bijeen-

komst in bijgestelde vorm in dit document opgenomen. Daarnaast heeft na de laatste werkconferentie de discussie over de organisatorische inbedding van de geconstateerde aanpak van High Tech Crime zowel binnen de stuurgroep als met het project NPAC, tot een aanpassing van de projectwerkzaamheden geleid.

2.3 Afronding project

Het resultaat van de hierboven gevoerde discussie na de laatste werkconferentie resulteerde in een besluit om te komen tot één advies op basis van de bevindingen van het project HTC én van de bevindingen van het project NPAC.
Het project HTC heeft drie van haar vier doelstellingen volledig kunnen realiseren, te weten:

- Het verkrijgen van inzicht in de aard omvang en impact van diverse uitingsvormen van High Tech Crime;
- Dreigingen door High Tech Crime te signaleren, erover te adviseren en de adviezen in een brede context weg te zetten;
- (Inter-)nationale multidisciplinaire en multi-agency samenwerking te realiseren ten behoeve van de bestrijding van High Tech Crime.

De vierde doelstelling, het realiseren van een goed intake proces en (inter-)nationale loketfunctie, is op het moment van beëindiging van het Project High Tech Crime nog niet gerealiseerd. De inzichten opgedaan in het NPAC project hebben echter laten zien dat, mede met het oog op de publiekprivate informatie-uitwisseling, een enkelvoudige loketfunctie niet de gewenste oplossingsrichting is. Vooral voor de participatie van het bedrijfsleven bij de bestijding van cybercrime is een scheiding tussen preventie en herstel enerzijds en opsporing en vervolging anderzijds van cruciaal belang. In het NPAC/NHTCC adviesontwerp 'nationale infrastructuur bestrijding cybercrime' wordt dan ook geadviseerd de loketfunctie op een gedifferentieerde wijze in te vullen zodat deze scheiding gerealiseerd wordt.

Het project is met de oplevering van deze eindverantwoording en het gezamenlijke en NPAC/NHTCC advies formeel afgesloten.

3. Aanleiding

In dit hoofdstuk wordt ingegaan op de inhoud van de problematiek rondom High Tech Crime en worden analyses gemaakt van de inhoudelijke en organisatorische knelpunten bij de aanpak van HTC.

3.1 Problematiek

3.1.1 High Tech Crime: criminaliteit in de moderne tijd

High Tech Crime (HTC) is een relatief nieuw 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. De criminelen zijn vaak anoniem of wisselen vaak van identiteit. Zij maken gebruik van de mogelijkheden van ICT om zich te verhullen en switchen erg snel van methodes en gedragingen. Zij zijn in hoge mate supra-nationaal bezig en zoeken altijd naar de zwakste schakels bij veel verschillende organisaties, hetzij publiek, hetzij van private origine. Steeds meer zijn zij zich aan het organiseren.

High Tech Crime kan worden gedefinieerd als *misdaden met behulp van (of gericht tegen) Informatie en Communicatie Technologie (ICT)*. Met nadruk 'misdaden' omdat veel ongewenste High Tech Crime verschijningsvormen en activiteiten nog niet wettelijk zijn omschreven, laat staan dat deze strafbaar zijn gesteld ofwel 'misdrijf' zijn te noemen.

De term 'Cybercrime' wordt ook door experts veelvuldig gebezigd voor deze materie. Internationaal kiezen politiële instanties in de externe communicatie echter meer en meer voor de term High Tech Crime om te voorkomen dat bij leken de indruk ontstaat dat het uitsluitend criminaliteit in 'virtuele' computeromgevingen zou betreffen en niet ook om fysieke criminaliteit waarbij crimineel ICT gebruik een belangrijke rol speelt. In Nederland worden daarnaast de termen cybercriminaliteit en computercriminaliteit veelvuldig gebruikt.

In het NPAC/NHTCC adviesontwerp 'nationale infrastructuur bestrijding cybercrime' wordt gemakshalve in de aandacht van de opsporing en vervolging, geen onderscheid gemaakt tussen cybercrime en High Tech Crime. Dit betekent dat de security of high tech oriëntatie die losstaat van publieke netwerken en in algemene zin betrekking heeft op de fysieke veiligheid van ICT-infrastructuren ook als onderwerp wordt genomen van de opsporing en vervolging. Uitgangspunt van het advies is dat voor wat de bestrijding van deze dreigingen het wenselijk is aan te sluiten bij bijvoorbeeld terrorismebestrijding en de daarvoor in het leven geroepen opsporingsaandacht of in de sfeer van het project bescherming vitale infrastructuren.

In 2002 is door de Dienst Nationale Recherche Informatie van het KLPD een onderzoek gedaan naar het fenomeen. In dat onderzoek zijn twee hoofdcategorieën van High Tech Crime onderscheiden:

a. Moderne en digitale vormen van criminaliteit die verricht zijn met (of gericht zijn tegen) computers of communicatiesystemen.
b. Klassieke criminaliteit in een nieuw – technologisch – jasje.

Wanneer is een dergelijke criminaliteitsvorm een vorm van High Tech Crime? Als bij het begaan van deze vormen van criminaliteit het gebruik van de ICT-toepassing of het Internet het overwegende middel of doelwit is, kan worden gesproken van een vorm van High Tech Crime. De criminele activiteit zou zonder deze toepassing of zonder het gebruik van Internet niet hebben kunnen plaatsvinden.

High Tech Crime wil overigens niet per definitie zeggen dat de criminelen die al dan niet bewust deze vorm van criminaliteit bedrijven universitaire studies Informatica hebben gevolgd.
Wel duidt het erop dat de criminaliteitsvorm in ieder geval doorspekt is met allerhande technische elementen waardoor het voor zowel de slachtoffers alsook politie en justitie erg problematisch is erachter te komen wat er precies is gebeurd en wie er achter een bepaald misdrijf zit.

Eenvoudig of complex, de ICT component in de criminele activiteit veroorzaakt de problemen bij bijvoorbeeld de opsporing of bij de preventie.

In de Nederlandse wetgeving vinden we diverse bepalingen die zich richten op computercriminaliteit (uit http://www.ejure.nl/):
Er zijn diverse artikelen in het Wetboek van Strafrecht te vinden die specifiek gericht zijn op computercriminaliteit: 138a (computervredebreuk en strafverzwarende varianten daarvan als het overnemen van gegevens), 350a en b (waaronder bijvoorbeeld defacing van een website, het verspreiden van virussen, wormen en Trojaanse paarden valt), 161 sexies en septies (dDos attack). In maart 2005 werd het wetsvoorstel Computercriminaliteit II in gewijzigde vorm toegezonden aan de Tweede Kamer. Het wetsvoorstel "aanpassing aan het Cybercrimeverdrag" is in de wijzigingen meegenomen en zal dus niet zelfstandig door de kamer worden behandeld.

Belangrijke onderdelen van het wetsvoorstel zijn:

- uitbreiden van de strafbaarstelling van hacking;
- ophogen van het strafmaximum voor delicten als virusverspreiding en (d)DoS-en;
- strafbaar stellen van voorbereidingshandelingen;
- invoeren van de bevoegdheid bepaalde gegevens een tijd vast te houden (bevriezingsbevel);

- invoeren van bevoegdheid af te tappen zonder medewerking van de beheerder van het te tappen netwerk.

Zie bijlage 4: Wet Computercriminaliteit I en Wetsvoorstel Wet Computercriminaliteit II op hoofdlijnen.

Met het toenemende gebruik van ICT dienen zich steeds nieuwe vormen van High Tech Crime aan. Deze zijn niet alleen gericht op het verdienen van geld, maar ook gericht op ontwrichting van computernetwerken en informatie-infrastructuren zelf en daarmee op de ontwrichting van de samenleving. Onderstaand overzicht geeft enkele ontwikkelingen aan.

3.1.2 Het recente verleden

Meer en meer dienstverlening en transacties vinden plaats in of met behulp van ICT-omgevingen en die ICT-omgevingen zijn gemakkelijker en sneller toegankelijk geworden in de afgelopen jaren. Dit heeft geleid tot een sterke roep om een betere beveiliging van die diensten en de computernetwerken waarlangs zij worden geserveerd. Deze roep kwam in beginsel van de zijde van de gebruikers van die diensten en ICT-voorzieningen. Zij kregen namelijk meer en meer te maken met diverse vormen van criminaliteit gerelateerd aan het gebruik van computers, netwerken en ICT-diensten.

Al snel probeerde de ICT-industrie gehoor te geven aan deze wens en vele beveiligingsmaatregelen volgden. Op hardwarematig en softwarematig terrein, maar ook werd het menselijk (gebruikers) aspect onder de loep genomen. Dit in achtnemend is een brug te slaan van de introductie en het gebruik van ICT naar de ontwikkeling van de op ICT gerichte of door ICT gefaciliteerde criminaliteit. Die ontwikkeling kan – sterk vereenvoudigd - worden gekenmerkt door drie fasen:

Fase 1: 'Mama, kijk eens wat ik kan!'.
Periode: 1980-1995
In deze fase wordt in zeer rap tempo duidelijk dat men computers en computernetwerken voor meer doeleinden kan gebruiken dan alleen communicatie of het maken van rekensommetjes. In hoog tempo worden nieuwe diensten en toepassingen geïntroduceerd die gebruikmaken van ICT. De gevallen waarbij de politie te maken krijgt met computercriminaliteit, High Tech Crime of ICT criminaliteit leidt dan ook vaak tot daders die zich van geen kwaad bewust zijn. In deze gevallen gaat het vaak om eenlingen of kleine groepen die, hoewel zich welbewust van hun technisch handelen, geen oogmerk hebben om in georganiseerd verband zware vormen van criminaliteit te begaan. Uitgangspunt voor hen blijft de technische uitdaging.

Redenerend vanuit de op dat moment bekende en actieve criminele organisaties kan men stellen dat deze personen ICT zeer zeker gebruikten als communicatiemiddel, maar op dat moment nog veel minder als informatiebron of als infrastructurele basis voor hun organisatie en de van daar uit verrichte activiteiten.

Fase 2: 'Meneer, weet u wel hoeveel die 'downtime' kost?'.

Periode: 1996-2002

Deze fase kenmerkt zich door bewustwording. ICT heeft de samenleving overrompeld. Er zijn drie kampen: mensen die alles weten van ICT en nog meer willen weten; mensen die er wars van zijn en voor wie al dat nieuwerwetse technogedoe maar een hoop blabla en aanstellerij is; en de groep mensen die zeer bewust gebruik maakt van ICT, maar geen idee heeft hoe de technologie (zoals elektronische zakagenda's, 'computergestuurde' automobielen, GPS systemen, mobiele telefoons, e-mail, www) nu eigenlijk precies in elkaar zit.

Er is een nieuwe groep 'ICT misbruikers' aangetreden. Of eigenlijk twee nieuwe groepen:

1. De nieuwe lichting technologisch goed onderlegde computercriminelen die in dit tijdperk verduveld goed weten wat de consequenties zijn of kunnen zijn van hun gedragingen in de virtuele wereld, en tevens weten 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 andere ICT gebruikers geld afhandig te maken. Als zij het niet zelf kunnen verzinnen dan kijken ze het desnoods wel 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 gingen ICT niet meer alleen als communicatiemiddel gebruiken, maar ook als 'tool' om extra financiën te genereren voor hun core business. Voorbeelden: 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 Rusland en Korea- bleken deze vormen van criminaliteit te benutten als exogene financiering voor de meer traditionele en klassieke criminaliteitsvormen. Ook werd in zijn algemeenheid de computer door criminelen ingezet als werktuig (bijvoorbeeld hacking, keylogging en interceptievormen) waarbij meer dan eens verwacht werd dat opsporende instanties de criminele gebruiker ervan niet of nauwelijks zouden kunnen achterhalen (Campina zaak, fraude met vliegtickets, bommeldingen, bedreigingen van politici).

Eindresultaat: ICT vormde steeds meer de basisinfrastructuur voor velerlei soorten activiteiten in de samenleving, ook voor criminaliteit en criminali-

teitsbestrijding. Punt van aandacht was wel het feit dat criminelen zich veel meer bewust leken te zijn van de voordelen van het gebruik van ICT voor hun criminele business, dan dat de politie zich bewust was van de nadelen van crimineel ICT gebruik voor de politiële business. De politie was daarin niet alleen, ook elders binnen overheid en bedrijfsleven werden de gevaren van crimineel ICT gebruik weinig tot niet onderkend.

Fase 3: 'Echt waar? U heeft nog geen Intrusion Detection System (IDS)?' Periode 2003 e.v.
Fase 3 is feitelijk het heden, waarbij een toenemende professionalisering valt waar te nemen.

Alle ICT-gebruikers (groot en klein) 'horen te weten' wat de gevaren zijn, 'horen te weten' dat ICT misbruikt kan worden en 'horen te weten' wat de gevolgen daarvan kunnen zijn. Waren bedrijven als slachtoffer van ICT gebruik vroeger met name geïnteresseerd in de 'businesscontinuïteit', nu willen ze maar wat graag weten wie dat misbruik heeft gepleegd. ICT is zoals eerder vermeld nu niet meer 'de infrastructuur voor', het is de 'aorta van' geworden. We kunnen echt niet meer zonder.
ICT stuurt op dit moment kernprocessen in de samenleving aan, nationaal en internationaal. Het belang van de continuïteit van die processen is mede daarom enorm groot. De tijd van 'op goed geluk' en 'uitproberen' is voorbij. 'IT is serious business'. Dit maakt dat telecom providers en de ICT industrie ook meer verantwoordelijkheid nemen voor hun rol bij het leveren van diensten of produceren van ICT-systemen, netwerken en componenten.

Misbruik van ICT wordt daarom in het buitenland al strenger gestraft. Ook in Nederland roept de samenleving hier om. Incidenten worden sneller gemeld en kwetsbare onderdelen van een ICT-infrastructuur worden door slachtoffers onverwijld aangepakt. De criminelen of criminele organisaties gaan echter dikwijls vrijuit. Niet alleen de roep om opsporing van de misbruiker(s) is belangrijker geworden, ook het voorkomen van incidenten. Hierbij zien we de ontwikkeling van virusscanner en firewall naar netwerkbrede Intrusion Detection Systemen en filter technologieën.
Tenslotte willen we ook graag de gegevens die we uitwisselen en de communicatie die we voeren zoveel mogelijk afschermen van luistervinkjes: Virtual Private Networks, PGP Universal en CryptoGSMs doen hun intrede.

3.1.3 De nabije toekomst

Deze professionalisering op verschillende fronten kan leiden tot de volgende ontwikkelingen ten aanzien van crimineel ICT-gebruik:
Criminelen zonder technische kennis richten zich op 'de beschikking krijgen over' in plaats van 'het binnendringen van'. Het is makkelijker belangrijke onderdelen van de ICT infrastructuur fysiek in bezit te hebben en te beheren en dan pas de gegevens te benaderen of de criminele activiteit te faciliteren, dan ze virtueel te moeten benaderen langs ingewikkelde technische wegen om ze daarna voor het criminele doel in te kunnen zetten;
meer creatief gebruik (lees faciliterend aan oplichtingpraktijken, fraude, spionage, diefstal e.d.) van ICT-middelen door criminelen in plaats van hard- of softwarematige manipulatie.

Hoewel beter beveiligd, biedt ICT ook in de toekomst meer mogelijkheden voor gebruikers, welk doel ze dan ook nastreven, en van die mogelijkheden zijn de consequenties vaak niet meteen bekend doordat soms nog steeds primair de functie van het ICT product belangrijk wordt gevonden en pas secundair de mogelijk vervelende neveneffecten.

In het land der blinden is Eenoog koning: toename van het aantal ICT gebruikers die geen technische kennis hebben en niet anders kunnen dan op de veiligheid van hun systemen en de betrouwbaarheid van hun systeembeheerder te vertrouwen. In zo'n omgeving kan High Tech criminaliteit welig tieren en technisch goed onderlegde criminelen hebben in dezen redelijk vrij spel.

Voor de criminelen en criminele organisaties is de inzet van vele facetten van ICT bij hun bedrijfsvoering nu reeds 'gangbaar'. Voor de Nederlandse politie als geheel is dit nog in ontwikkeling. Denk hierbij bijvoorbeeld aan het binnen de recherchepraktijk breedbandig en versleuteld e-mailen, chatten, bestanden uitwisselen of met PC's en draadloze communicatie toegang verwerven tot de interne politie databases vanuit welke locatie dan ook. Kennis van dergelijke basistechnologieën en het gebruik daarvan ontbreekt in veel gevallen.

Al eerder is bij de politie geconstateerd dat er op dit punt onvoldoende kennis en capaciteit is om in het algemeen snel en adequaat op te treden tegen High Tech Crime[1]. Naast het inmiddels gestarte opleidingsprogramma bij de politie om rechercheurs meer vertrouwd te maken met digitale opsporing (als uitvloeisel van het Landelijk project Digitale Opsporing) is dit project een uitkomst van die constatering.

3.2 Knelpunten

3.2.1 Inhoudelijk

Wanneer we de opsomming in het kader van de volgende pagina goed bestuderen, dan zien we dat de criminele activiteiten in het overzicht in de kern niet verschillen van wat we noemen 'traditionele criminaliteit'. Diefstal blijft diefstal, fraude blijft fraude en drugshandel blijft drugshandel, ook al gebruiken criminelen ICT meer en meer voor dit soort activiteiten. Oude wijn in nieuwe zakken dus.

Desondanks lijken politie en justitie erg veel moeite te hebben met het oppakken of bestrijden van met ICT doorspekte zaken. Slachtoffers van High Tech Crime merken dit maar al te goed. Zij ervaren bij het doen van

[1] Zie hiervoor ook het rapport van het Landelijk Project Digitale Opsporing (in bijlage 2)

aangifte dat de politie veel moeite heeft met bijvoorbeeld het opnemen en verwerken van de technische aspecten van het incident.
Ook is het voor politie en justitie nog steeds moeilijk High Tech Crime op de juiste waarde te bepalen waar het gaat om impact op slachtoffers en samenleving of de precieze omvang van de schade.

Het wordt nog ingewikkelder als het incident zich over de landsgrenzen heen afspeelt. Dan blijkt vaak dat er weinig coördinatie is en onduidelijkheid bestaat over de rolverdeling bij de internationale bestrijding van deze vorm van misdaad. Ook hier is een goed verloop van het opsporingsproces afhankelijk van de goede informele contacten tussen politiemensen in die landen. Zowel voor politie als slachtoffers is het moeilijk de juiste wegen te vinden bij de aanpak van dit probleem.

De slachtoffers zijn niet alleen de thuisgebruikers. Ook zijn er aanwijzingen dat belangrijke sectoren als de luchtvaartsector, de financiële sector, de overheid, de chemische industrie, de transportsector, de gezondheidszorg en het MKB (Midden- en Kleinbedrijf) zich geconfronteerd zien met een toename van HTC-incidenten, die hun oorsprong kennen in de meest afgelegen contreien.

Het lijkt er dus op dat de combinatie van technische complexiteit, het internationale karakter, de snelheid, de diversiteit en de veelvuldigheid van sommige vormen van High Tech Crime maakt dat het opsporings- en vervolgingsapparaat minder adequaat kan reageren als het eigenlijk zou willen of - volgens delen van onze samenleving - zou moeten.

Er is geprobeerd te onderzoeken hoe groot het probleem van High Tech Crime precies is. In welke mate is er mogelijk een lacune in de criminaliteitsbestrijding doordat er bewust of onbewust - geen aandacht aan wordt besteed of kan worden besteed, door bijvoorbeeld gebrek aan kennis en kunde? Deze pogingen waren tevergeefs, omdat er binnen het opsporingsapparaat niet of nauwelijks registratiesystemen blijken te zijn die de mogelijkheid bieden relevante ICT-aspecten bij een crimineel incident vast te leggen - als High Tech Crime al wordt vastgelegd.

We weten niet goed wat de omvang van het probleem is, of veel criminelen dankzij ICT de dans ontspringen en wat de rol en invloed van ICT op criminaliteit nu precies is. Op deze manier is het tevens erg moeilijk te bepalen hoe de criminaliteitsbestrijders zich het beste zouden kunnen voorbereiden en uitrusten bij de bestrijding van High Tech Crime.

Misdaad en ICT

Hieronder is een lijst met vormen van High Tech Crime. Onder deze criminaliteit verstaan we misdaden die zijn verricht met, of gericht tegen informatie en communicatietechnologie (ICT).

Categorie A - Misdaden met ICT als doelwit:

1. **Aanvallen op computer- of informatiesystemen (*denial of service*-aanvallen) of op vitale informatie-infrastructuren van logistieke knooppunten. Deze aanvallen kunnen leiden tot uitschakeling van de voorzieningen die gebruik maken van de computer- of informatiesystemen;**
2. **Inbraak in computer- of informatiesystemen of in computerprogramma's (*hacking/cracking*);**
3. **Vernieling/wijziging/verwijdering van informatie in computersystemen (*virussen en Trojans*) of informatie op internet (*defacing*).**

Categorie B – Misdaden verricht met behulp van ICT:

4. **Terrorisme - voorbeelden: *online* verdachte financiële transacties, propaganda, rekrutering, communicatie, bedreigingen, *online* beschikbaar zijn van gevoelige of vertrouwelijke informatie; eventueel bruikbaar voor terreuractiviteiten;**
5. **Spionageactiviteiten – gegevens van computergebruikers onderscheppen met behulp van ogenschijnlijk onschuldige softwareapplicaties (*spyware*) waarmee men de gebruiker ongemerkt kan afluisteren of bespioneren;**
6. **Fraude op internetwinkels, veiling- of verkoopsites;**
7. **Fraude met internetwinkels, veiling- of verkoopsites;**
8. **Fraude met internetbetalingen (bancaire transacties, '*phishing*');**
9. **Fraude met inbelnummers (0900-fraude, *autodailers*);**
10. **Handelen met voorkennis door afspraken te maken met gebruik van besloten *online chatsites*, discussieruimten. Gebruik van (*online*) discussieruimten voor criminele activiteiten/communicatie door criminele organisaties;**
11. **Verzoeke tot het verrichten van dubieuze investeringen of betalingen (*advance fee fraud, Nigerian scams, lottery scams*);**
12. **Merkvervalsing op het internet, software piraterij; kopiëren en illegaal uitwisselen en verkopen van films, muziek etc.;**
13. **Bedreiging, chantage, afpersing en *stalking* via het internet of met behulp van GPS-systemen;**
14. **Drugshandel op of via het internet (*online*-verkooppunten);**
15. **Illegale handel in geneesmiddelen op of via het Internet;**
16. **Illegale kansspelen op het Internet;**
17. **Kinderpornografische afbeeldingen op het Internet of het lokken van kinderen via chatsites (*grooming*);**
18. **Racisme, discriminatie, smaad en laster op of via het internet;**
19. **Diefstal en misbruik van (*online*) persoonsgegevens of profielen;**
20. **Illegaal kopiëren van betaalpassen, toegangspassen of *online*-betaalkaartgegevens (*skimming*).**

Bron: NHTCC

3.2.2 Organisatorisch

Het is niet altijd makkelijk voor aangevers van High Tech Crime om met hun cybercrime-probleem een goede ingang te vinden. Hierdoor is bij aangevers en melders het idee ontstaan dat - als het aangifteproces al niet goed verloopt - de politie vast niet in staat is om High Tech Crime afdoende te bestrijden.
Dit ontmoedigt het doen van aangifte. Is er wel een aangifte gedaan dan moet een zaak eerst gewogen kunnen worden, alvorens een besluit valt om tot actie over te gaan. De opsporingscapaciteit is immers schaars.

De weging van een zaak gebeurt in overleg met het Openbaar Ministerie (OM). Helaas passeren High Tech Crime-zaken vaker niet dan wel een dergelijke case screening. Hiervoor zijn verschillende redenen aan te voeren. Het kan zijn dat de beoordelaars niet over ICT-kennis beschikken. Tevens is gebleken dat het niet direct voorhanden hebben van een pasklare oplossing eveneens een factor kan zijn. In het laatste geval bestaat de vrees voor een langdurig en ingewikkeld technisch onderzoek naar een vaak evenzo ingewikkeld ICT-incident - waarbij uitkomst en rendement dikwijls onzeker zijn.

De kans op behandeling van de aangifte wordt ook verkleind door de vaak lage individuele schadeposten, bijvoorbeeld in het geval van het ontfutselen van gegevens van internetbankieren door internetcriminelen of andere vormen van internetfraude waar in beginsel slechts individuele burgers door getroffen worden. De kans is dan groot dat aan deze vorm van misdaad geen prioriteit wordt gegeven. Wanneer men onderzoekt wat hiervoor de argumenten zijn, doemt vaak de vraag op of High Tech Crime wel zo'n groot probleem vormt, dat er reden is om er prioriteit aan te geven.

Hier ontstaat een vicieuze cirkel: zolang er niet of niet op de juiste wijze aangiften worden opgenomen van High Tech Crime kan nooit precies aangegeven worden wat, hoe groot en hoe nijpend de problematiek is. En dus zal het ook geen prioriteit krijgen. Daardoor kan er weer geen diepgaand onderzoek naar worden gedaan.

Ook laat High Tech Crime zich soms moeilijk etiketteren. Een crimineel kan zich vandaag bezighouden met online neploterijen, hij kan morgen aan het vissen zijn naar iemands gegevens bij het internetbankieren en volgende week een illegaal online casino runnen. 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 vanuit dezelfde locatie (waar ook ter wereld en relatief afgeschermd voor politie en justitie), bijvoorbeeld door snel en continu te wisselen van virtuele identiteit.

Aangevers kunnen soms verschillende verwachtingen hebben van de effectiviteit of de mogelijke resultaten van een politieoptreden. Zo is er lang niet altijd de wens dat de high tech crimineel wordt opgepakt. Even belangrijk is dat de criminele activiteit wordt gestaakt. Dankzij ICT zijn dat tegenwoordig verschillende zaken: de veroorzaker kan namelijk achter slot en grendel worden gezet, terwijl de criminele activiteit in de digitale omgeving gewoon doorgang vindt. In die gevallen is er de verwachting dat - zoals dit ook in de fysieke omgevingen het geval is - de politie kan bijdragen aan een permanente verhoogde veiligheid van digitale omgevingen.

3.3 Overzicht van aandachtspunten

High Tech Crime is een probleem waar te weinig aandacht voor is door het gebrek aan inzicht in de problemen en er dus te weinig wordt gedaan door politie en justitie in Nederland, terwijl de effecten van High Tech Crime wereldwijd vaak zeer (snel) merkbaar zijn en in andere landen inmiddels meer gegevens beschikbaar komen die aantonen dat de schade die door High Tech Crime wordt veroorzaakt, gestaag toeneemt.

De reden dat er nauwelijks iets aan High Tech Crime wordt gedaan, wordt veroorzaakt door onder meer de volgende factoren:

Het gebrek aan specialistische kennis en expertise bij politie en justitie. Politie en justitie (overall) beschikken over onvoldoende kennis en capaciteit voor het op een kwalitatief goede wijze opnemen van aangiften, wegen van zaken en naspeuren van misdrijven. Hierdoor is het enerzijds weinig aantrekkelijk om aan zo'n High Tech Crime zaak te beginnen, en anderzijds heeft men er soms gewoon geen capaciteit of expertise (meer) voor in huis.

De snelheid van ICT ontwikkelingen. De omgeving die door ICT wordt gecreeerd laat zich kenmerken door snelheid, flexibiliteit, mobiliteit en gebruiksvriendelijkheid. Die omloopsnelheid van het gebruik van nieuwe middelen en methoden kan niet worden gehaald door politie en justitie.

De schade en impact van High Tech Crime is onduidelijk en wordt mede daardoor mogelijk onderschat. De schade door en impact van High Tech Crime 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'. Ook leeft bij velen die niet thuis zijn in de materie de gedachte dat High Tech Crime in veel gevallen te etiketteren valt als 'aangiftecriminaliteit'. En 'aangiftecriminaliteit' wordt zelden 'zwaar' of 'ernstig' geacht.

De horizontale werking van High Tech Crime. High Tech Crime kan geen apart resultaatgebied genoemd worden zoals drugshandel, mensenhandel, fraude etc. High Tech Crime heeft 'overal' wat mee te maken en de inherente complexe ICT component loopt als een rode draad door alle resultaatgebieden heen. Dit levert momenteel niet alleen een probleem op bij de registratie van High Tech Crime 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. Dit kost tijd en geld, en niet altijd is hiervoor bij politie en justitie voldoende aandacht.

Het gebrek aan onderzoek naar de rol van 'High Tech' bij criminaliteit en criminaliteitsbestrijding. Naast het feit dat ICT als rode draad door alle criminaliteitsvormen die we kennen heen schiet en steeds weer de belemmerende of hinderende factor in opsporingsonderzoeken blijkt te zijn (of zelfs voorkomt dat opsporingsonderzoeken worden gestart) wordt momenteel in Nederland NIET breed en gecoördineerd onderzocht in hoeverre ICT de politie, veiligheids- en inlichtingendiensten in staat stelt, om efficiënter en effectiever reactief, proactief of zelfs realtime op te treden. Of het nu gaat om de rol van ICT bij het verrichten van criminaliteit of bij het bestrijden van criminaliteit.

Het gebrek aan een loket voor High Tech Crime issues. Er is geen kundig, laagdrempelig en eventueel online en (inter-)nationaal aanspreekpunt voor:

a. probleemhouders die misdaden met of tegen ICT - High Tech Crime - hebben ervaren of ze juist willen (helpen) bestrijden;

b. probleemhouders met meldingen, verdenkingen of concrete informatie inzake terroristische activiteiten die gerelateerd zijn aan of gefaciliteerd worden door ICT;
c. probleemhouders van onderdelen van een vitale infrastructuur waarvan een uitval als gevolg van een High Tech Crime activiteit tot grote maatschappelijke gevolgen kan leiden;
d. de uitwisseling van kennis en expertise op het gebied van High Tech Crime als 'High Tech' criminaliteitsbestrijding;
e. voorlichting en advisering op het gebied van zowel High Tech Crime als 'High Tech' criminaliteitsbestrijding;
f. verzoeken tot een (inter-)nationaal gecoördineerde bestrijding van zware en georganiseerde vormen van criminaliteit die technisch complex (lijken te) zijn en/of een grensoverschrijdend karakter hebben;
g. innovatieve en multidisciplinaire (inter-)nationale (technische) onderzoeken die kunnen worden geïnitieerd in relatie tot High Tech Crime.

Het gebrek aan communicatie en informatie-uitwisseling over High Tech Crime. Met behulp van communicatie, informatie-uitwisseling over daders, doelwitten en tools kan men bevorderen dat bestaande initiatieven ter bestrijding van cyber crime worden gecoördineerd en gestroomlijnd. Het is met name van belang dat informatie wordt uitgewisseld tussen partijen in de publieke én de private sector. Of het nu gaat om slachtoffers, onderzoekers of bestrijders van High Tech Crime.

Het gebrek aan afspraken over rolverdeling en procedures bij High Tech Crime incidenten. Het is dringend noodzakelijk dat de beschikbare kennis en opsporingscapaciteit binnen het opsporingsapparaat transparant wordt gemaakt. Denk hierbij ook aan de bijzondere opsporingsdiensten zoals FIOD/ECD en SIOD, of aan de expertise bij een GOVCERT.NL. Ook de toezichthouders in diverse sectoren kunnen gespecialiseerde kennis en middelen aandragen, denk aan AFM, OPTA en NMA. Duidelijk moet worden wat de behoefte, rol(len) en eigen verantwoordelijkheden zijn van overheidsinstellingen en het bedrijfsleven in relatie tot de bestrijding van High Tech Crime.

Geen publiekprivate samenwerking bij de bestrijding van High Tech Crime. Bevorderd dient te worden dat een koppeling wordt gemaakt tussen de behoefte en verantwoordelijkheden van de overheid en die van het bedrijfsleven. Ook is een goede vertrouwensrelatie tussen opsporingsdiensten en (geselecteerd) bedrijfsleven van het uiterste belang voor de verbetering van samenwerking en informatie-uitwisseling. Verder beschikken veel private partijen over een schat aan expertise en kennis die de publieke organisaties kunnen helpen bij de oplossing van HTC-problemen.

Geen zicht op mogelijkheid van preventieve maatregelen tegen cybercrime; De digitalisering van de samenleving, de misdaad en dus ook het werk van politie en justitie, is onomkeerbaar. De inzet van digitale expertise in reactieve

zin en enkel ter ondersteuning van het tactisch proces is niet meer voldoende. Van de politie wordt in toenemende mate verwacht dat ze structureel en proactief zorg draagt voor openbare orde en veiligheid in virtuele omgevingen, omdat het disfunctioneren van die omgevingen een directe negatieve impact heeft op de fysieke omgevingen.

In diverse andere projecten, studies en beleidstukken is aandacht voor High Tech Crime. In bijlage 1 worden enkele daarvan nader beschreven, teneinde een goed overzicht van de initiatieven op dit gebied te krijgen.

Daarnaast zijn er in het afgelopen jaar diverse keren Kamervragen gesteld over deze materie. In het rapport dat PriceWaterhouseCoopers voor het ministerie van Economische Zaken maakte over de 10 doorbraken in de ICT werd over de noodzaak van optreden tegen High Tech Crime ten behoeve van gebruik en ontwikkeling van commerciële ICT innovaties en diensten zelfs het volgende geschreven:

"A crucial condition for a broad deployment and use of ICT by business and consumers is user confidence. Therefore the EU needs to enforce structural solutions for viruses and spam by creating liabilities, give priority to cybercrime within law enforcement and ensure the availability of critical infrastructures. The crucial questions for the EU are: 1. How much time the EU is willing to give to the market to (collectively) come up with structural solutions concerning internet security? 2. Is the EU prepared to create liabilities to enforce market players to find real solutions for 'the darker side' of the internet? 3. Is the EU prepared to give priority to cyber crime (over and above other tasks) within law enforcement?"

4. Uitwerking van de opdracht

Aan de opdracht, het werken aan een effectieve en efficiënte bestrijding van High Tech Crime, is uitvoering gegeven door gedurende de projecttermijn een aantal concrete activiteiten te ondernemen.

4.1 Survey High Tech Crime

Uit periodieke berichtgevingen, onderzoeken en meldingen is op te maken dat de digitale criminaliteit snel toeneemt in omvang en verscheidenheid. Zo zou het aantal Nederlandse bedrijven en instellingen dat geconfronteerd wordt met IT- of High Tech Crime incidenten variëren van 16% tot 50% en de schatting van de schade als gevolg van de incidenten uiteenlopen van € 185 miljoen tot € 1 miljard. Hoewel uit deze informatie kan worden geconcludeerd dat High Tech Crime toeneemt en zelfs voor aanzienlijke schade zorgt in de Nederlandse samenleving, ontbreekt het aan een betrouwbaar kwalitatief overzicht en inzicht in de aard en omvang van High Tech Crime. Daardoor kunnen geen valide en voldoende maatregelen op beleidsterreinen en opsporingsgebied genomen worden om High Tech Crime tegen te gaan en op te sporen. Door middel van het ontwikkelen en uitvoeren van een jaarlijks terugkerende survey 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. Daarvoor is het noodzakelijk dat de survey, zowel een kwalitatief als kwantitatief beeld geeft van High Tech Crime binnen een brede vertegenwoordiging van overheid en bedrijfsleven, van klein- tot grootbedrijf en van waterschap tot ministerie. Om de medewerking van geselecteerde bedrijven en instanties te vergroten is nauwe samenwerking met vertegenwoordigende instanties wenselijk en noodzakelijk. De survey wordt bij voorkeur in samenwerking met partners als VNO/NCW, GOVCERT.NL en ECP.NL uitgevoerd.

Tijdens de projectperiode werd de eerste High Tech Crime & Security Survey in juli 2005 gestart waarbij 711 bedrijven en instellingen werden aangeschreven. Deze survey wordt beschouwd als een 0-meting en naast concrete informatie is deze survey tevens bedoeld bedrijven en instellingen (meer) bewust en bekend te maken met het onderwerp.
Naast overheidsinstellingen werden vooral bedrijven in de vitale infrastructuur, zoals de energiesector, financiële sector, waterkwantiteit en transport aangeschreven. De survey kon zowel handmatig als via het Internet worden ingevuld. 50 Respondenten vulden de survey in; dit is 7%.

Dit aantal respondenten is te weinig om uit de resultaten verantwoorde conclusies te kunnen trekken.

Uit een eerste globale analyse van de resultaten blijkt dat:

- Er werden reacties ontvangen van bedrijven uit 11 van de 17 benoemde sectoren. Bedrijven in de sectoren drinkwatervoorziening, voedselvoorziening, bouwnijverheid en civiele techniek, retail en groothandel en de horeca leverden geen reacties. De bedrijfsgrootte van de respondenten varieerden van 18% kleinbedrijf tot 55% grootbedrijf en de omvang van de omzet van 30% met een omzet van < € 5 miljoen en 13% met een omzet van > € 1 miljard;
- Ruim 57% van de respondenten hanteren een beveiligingsbeleid, terwijl 36% dat niet kennen;
- 54% gaf aan geconfronteerd te zijn met een vorm van High Tech Crime, waarvan ongeveer 1/3 deel hacking, dDos, phishing en bedrijfsspionage betrof; 37,5% bleek geen slachtoffer te zijn geweest;
- 43 bedrijven hadden schade, variërend van imagoschade tot productiviteitsschade en financiële schade, tengevolge van enige vorm van High Tech Crime. De omvang van de financiële schade liep uiteen van minder dan € 1.000,- (8%) tot meer dan € 100.000,- (16%), waarvan 4% zelfs meer dan € 500.000,-;
- Slechts 8 respondenten hadden aangifte gedaan bij het Openbaar Ministerie of Politie. De redenen om geen aangifte te doen varieerden van negatieve publiciteit tot onbekendheid met het gegeven dat aangifte gedaan kon worden. Twijfels over een goede afloop van een justitieel opsporingsonderzoek en onbekendheid met het gegeven dat politie en justitie interesse in deze incidenten zouden hebben, werden het meest opgegeven;
- Ongeveer de helft van de respondenten gaf aan, dat het investeringsbudget om de beveiliging te verbeteren verhoogd werd.

De resultaten worden nog nader uitgewerkt en in samenwerking met VNO-NCW en ECP.NL bekendgemaakt.

Het project High Tech Crime van mening dat dit een goed middel is om meer te weten te komen over de aard en omvang van het probleem. Een internationale vergelijking leert ons dat deze respons niet onder doet voor de eerste surveys in andere landen.

4.2 Informatie-uitwisselingsproces

Het inrichten van een proces van informatieverzameling en analyse, teneinde hieruit maatregelen voor de bestrijding van High Tech Crime te kunnen voorstellen, is het fundament voor een goed werkende bestrijding van High Tech Crime. Onderstaand proces is gemaakt met de bedoeling te fungeren als model dat door het vervolgtraject kan worden toegepast. De volgende procesfuncties worden onderscheiden:

4.2.1 Informatievergaring

Voor een effectieve en efficiënte bestrijding van High Tech Crime is het verkrijgen van inzicht een eerste vereiste. Deze doelstelling kan gerealiseerd worden door een adequate en betrouwbare informatieverzameling en –uitwisseling met en tussen verschillende (inter-)nationale partijen zoals het bedrijfsleven, internationale zusterorganisaties, inlichtingendiensten, voor ICT verantwoordelijke ministeries en opsporingsorganisaties. Deze informatie is afkomstig van publieke[2] en private[3] partijen. Veel van deze informatie heeft een vertrouwelijk karakter en moet onder bepaalde condities worden behandeld en afgeschermd zijn van de openbaarheid.

Private en publieke partijen zijn een belangrijke bron van informatie over High Tech Crime en willen de informatie delen als deze maar niet direct en vanzelfsprekend in 'de opsporing' verdwijnt. Door het realiseren van bijvoorbeeld overeenkomsten kunnen bepaalde waarborgen worden gesteld, zodat partijen de zekerheid en het vertrouwen hebben in een betrouwbare en integere informatieverwerking. Onderdeel van een dergelijke overeenkomst is onder andere de bepaling, dat de oorspronkelijke informatieverstrekker vooraf nadrukkelijk toestemming moet geven wanneer 'zijn' herleidbare informatie ter beschikking van de opsporing wordt gesteld. In een algemeen vertrouwensdocument worden de algemene kaders en werkwijze met betrekking tot de informatievoorziening inzichtelijk en openbaar.

Er wordt ook relevante nationale en internationale opsporings- en politieinformatie verzameld om daarmee onder andere te kunnen zoeken naar dwarsverbanden en fenomenen in de verschillende verschijningsvormen van High Tech Crime.

De toegevoegde waarde van dit model is dat informatie die wordt verkregen vanuit de opsporing wordt gebruikt ter invulling van proactief getinte werkzaamheden, dan wel dat informatie vanuit openbare en private bronnen aanleiding is voor repressieve activiteiten. De tweezijdigheid in deze informatie-uitwisseling is daarbij cruciaal. Daarmee wordt bedoeld dat alle partijen die met elkaar een afspraak over informatie-uitwisseling maken, van elkaar weten wat ze kunnen verwachten aan informatie, maar ook wat niet wordt uitgewisseld.

Zo gebeurt het verkrijgen van de opsporingsinformatie, het bewerken en analyseren daarvan onder verantwoordelijkheid van het OM, conform de heersende wet- en regelgeving. Dit betekent dat hiervoor ook restricties in acht moeten worden genomen met betrekking tot de soort informatie die met anderen kan worden gedeeld en wanneer dat kan.

[2] landelijke, regionale en lokale overheidsinstellingen, wetenschap en onderwijs, zorginstellingen

[3] bedrijven in de vitale sector, financiële sector, energiesector etc. midden en klein bedrijf.

Er worden drie informatiestromen en vier soorten informatie onderscheiden.
De drie informatiestromen zijn:

- Publiek (overheidsinstellingen, wetenschap en zorg);
- Opsporing (OM/Politie);
- Privaat (bedrijfsleven, belangenorganisaties en consument).

De vier soorten informatie zijn:

a. statistische informatie;
b. informatie met verzoek om advies;
c. informatie om een incident tegen te houden of op te heffen;
d. informatie met verzoek om opsporingshandelingen te laten verrichten c.q. opsporing in gang te zetten.

Ad a. Statistische informatie
Dit is niet naar personen of concrete zaken te herleiden informatie. Deze informatie kan tevens worden gebruikt om fenomeenonderzoek (onderzoek naar vormen van High Tech Crime), verschillende soorten van en eventuele overeenkomsten in werkwijzen uit te voeren en vast te stellen.

Ad b. Informatie met verzoek om advies
Hierbij wordt informatie uitgewisseld of om advies gevraagd, zonder dat direct sprake is van een in te stellen strafrechtelijk onderzoek of het tegenhouden van een incident.

Ad c. Informatie om een incident tegen te houden of op te heffen
Deze informatie wordt uitgewisseld om een incident te melden. Prioriteit ligt daarbij bij het voorkomen of stoppen van de handelingen.

Ad d. Het aanleveren van deze informatie is bedoeld voor het doen uitvoeren van opsporingshandelingen en/of het initiëren van een opsporingsonderzoek.

De informatie kan op verschillende manieren worden verstrekt, zoals schriftelijk, telefonisch, e-mail, per fax en, afhankelijk van de mate van betrouwbaarheid en veiligheid, open of encrypt bij digitale melding. Een specifieke bron van informatie kan het te ontwikkelen Nationaal Meldpunt Cybercriminaliteit (NMC) zijn.

4.2.2 Informatieanalyse

Na ontvangst van de informatie wordt deze in eerste instantie ingevoerd en opgeslagen in een centrale database binnen het 'eigen' (publieke of private) domein. Deze informatie wordt naar soort en inhoud gekwalificeerd zoals melding, mutatie, verzoek, algemene info etc.

Binnen het eigen domein wordt de informatie geanalyseerd en verwerkt. Afhankelijk van de soort informatie en het eventuele specifieke verzoek wordt deze informatie verder verwerkt.
In beginsel wordt de informatie die via het meldpunt binnenkomt geaggregeerd tot niet-herleidbare informatie, waarna deze naast de overige informatie wordt gelegd, afkomstig van publieke en private partijen. Op deze manier wordt goed inzicht verkregen in fenomenen, de verschillende soorten van incidenten en toegepaste werkwijzen. Ook kan daarmee bijvoorbeeld worden vastgesteld of een incident eenmalig voorkomt, alleen bij de meldende partij, dan wel bij meerdere instellingen of bedrijven. Wanneer de meldende partij een voorbehoud heeft gemaakt met betrekking tot het gebruik van de geleverde informatie (anders dan statistisch gebruik) wordt in een dergelijk geval met de oorspronkelijke melder overleg gepleegd om overeenstemming te verkrijgen over de te nemen stappen, zoals het doen stoppen of tegenhouden, het nemen van concrete preventieve maatregelen om herhaling te voorkomen of het initiëren van een onderzoek naar een nieuw HTC-fenomeen.

Wanneer na een grondige analyse van verkregen informatie blijkt dat deze informatie van toegevoegde waarde is voor ondersteuning in de opsporing of het initiëren van opsporingsonderzoeken van High Tech Crime door opsporingsdiensten, wordt de publieke en private informatie met inachtneming van de vastgestelde kaders en afspraken gematcht met opsporingsinformatie.
Omgekeerd wordt deze gematcht met de publieke en private informatie wanneer uit verkregen opsporingsinformatie relevante informatie wordt gedistilleerd en geanalyseerd en ten behoeve van producten, zoals adviezen en/of waarschuwingen voor publieke en/of private partijen kan worden gebruikt. Dit zal door de aanwezige politiefunctionarissen worden verricht. Zo'n vermenging van de publieke en private informatie met de opsporingsinformatie wordt aangeduid als informatietransformatie.
Dit specifieke informatietransformatieproces vindt plaats onder verantwoordelijkheid van het Openbaar Ministerie als bevoegd gezag.[4]

De opslag, analyse en verwerking van informatie en ook informatietransformatie is een proces dat zich binnen het model afspeelt. De uitvoering hiervan gebeurt met de eigen beschikbare expertise in de staande organisaties, waarmee vervolgens de verschillende producten worden geleverd. Daarnaast kan meer specifieke expertise benodigd zijn.
Na overleg met de betreffende partij wordt hierin voorzien. Uiteraard zijn daar in een vooraf afgesloten overeenkomst afspraken over gemaakt.

Het informatieproces wordt bewaakt en begeleid onder verantwoordelijkheid van de informatiemanagement functionaris die daarmee tevens aan-

[4] Zie ook informatieprocesschema

spreekbaar is voor de verschillende partijen. Hij vervult daarmee een vertrouwensfunctie naar deze externe partijen en rapporteert zowel langs de reguliere lijn binnen de eigen organisatie als direct of indirect aan betrokken derde partijen.

De verschillende activiteiten, die voortkomen uit het informatieproces worden onder andere onderscheiden in:
- voorbereiden opsporing;
- tegenhouden van illegale content;
- advies geven;
- ontwikkelen van maatregelen en procedures;
- (sectorale) vergelijkingsoverzichten produceren.

Deze activiteiten resulteren onder andere in de volgende producten:
- preweegdocument ten behoeve van de opsporing (conform het OMP-proces[5]);
- tegenhoudacties, zoals het doen verwijderen door een ISP van illegale content van het internet al dan niet op last van justitie;
- advies over het doen voorkomen van HTC of te nemen acties naar aanleiding van actuele HTC;
- ontwikkeling van maatregelen en aanpassing van procedures;
- doorgeleiden van informatie naar andere diensten en instellingen in het binnen- en buitenland;
- voorstellen tot (aanpassing van) beleid en/of voorstellen tot wijziging van de wet op basis van de witte vlekken die worden ervaren bij de bestrijding van High Tech Crime.

Indien vanuit dit model een verzoek tot (ondersteuning bij) opsporing wordt gedaan, voldoet de politie in afstemming met het OM aan dit verzoek, mits het verzoek past binnen de kaders van capaciteit en gestelde criteria van HTC. Dit geschiedt op basis van maatwerkconstructies. Een goede communicatie is hiervoor randvoorwaardelijk.

Goede afspraken met de politieorganisatie en het OM als bevoegd gezag over het opvolging geven aan een preweegdocument dan wel een opsporingsonderzoek en vervolging inzake High Tech Crime is noodzakelijk om een effectieve bestrijding van High Tech Crime te bewerkstelligen. Daarbij worden de eigen verantwoordelijkheden van de betrokken partijen in acht genomen.

4.2.3 Informatieverspreiding

Er wordt een actieve en passieve informatieverspreiding gehanteerd. Bij de passieve informatieverspreiding worden algemene adviezen, te nemen

[5] OMP Informatie Gestuurde Opsporing, een pre-weeg-document is een onderdeel in de aanvangsfase van de opsporing, meer concreet de 1e fase in de 'voorbereiding van de opsporing'

maatregelen in standaard situaties, statistische informatie en overzichten ter beschikking gesteld. Dit gebeurt door deze bijvoorbeeld te plaatsen op de website of te publiceren in (vak)bladen.
Met de actieve informatieverspreiding worden resultaten van geanalyseerde informatie aan de diverse belanghebbenden verstuurd of ter beschikking gesteld.
Deze resultaten kunnen een algemeen karakter hebben, maar ook specifiek zijn ontwikkeld op basis van een specifieke vraagstelling of afspraak in een overeenkomst. Bij actieve informatieverspreiding gebeurt de uitwisseling door beveiligde methoden en kanalen. Daarnaast wordt er jaarlijks een rapportage uitgebracht met trends en ontwikkelingen.

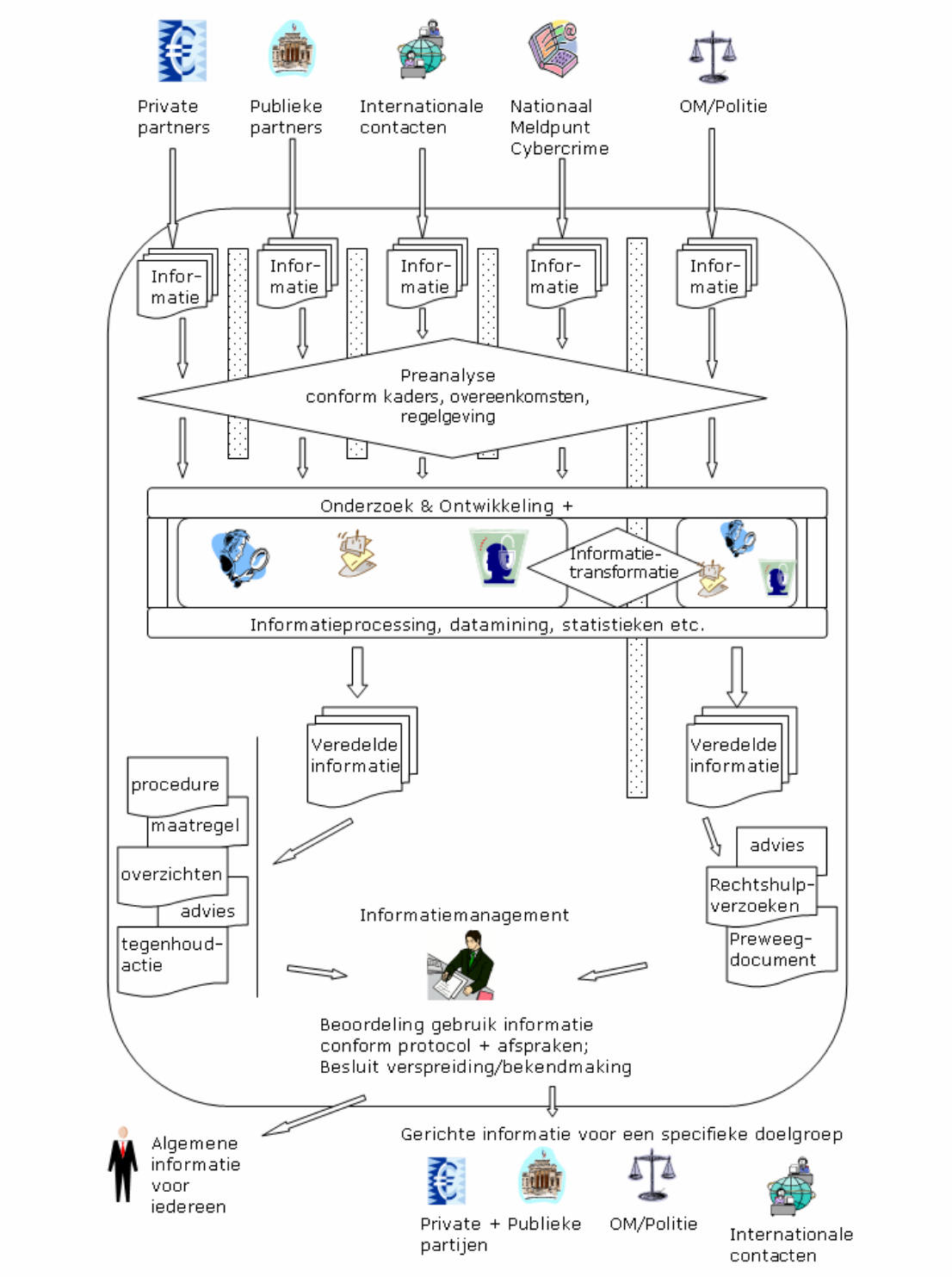
4.2.4 Informatie-uitwisselingsproces schematisch weergegeven

De voorgaande beschrijving van informatievergaring, -analyse en –verspreiding is in het volgende informatieproces samen te vatten:
De informatie over High Tech Crime komt op grofweg twee manieren binnen. Het eerste kanaal is het Nationaal Meldpunt Cybercrime (NMC), de tweede manier is rechtstreeks van publieke en private partijen, waarmee al dan niet nadere procedureafspraken zijn gemaakt en eventueel vastgelegd in overeenkomsten.
Deze informatie wordt conform de gemaakte afspraken en daarvoor geldende wet- en regelgeving behandeld en wordt in de volgende 'preanalyse' fase nader onderzocht en beoordeeld. Nadat de informatie 'niet-herleidbaar' is gemaakt, komt ze in de fase van 'Onderzoek & Ontwikkeling'. Door middel van technieken en methodieken, zoals datamining, wordt de informatie nader onderzocht op eventuele overeenkomsten in werkwijzen, op meerdere malen voorkomen van gelijksoortige incidenten etc. Eventueel wordt de informatie gematcht met concrete opsporingsinformatie in het deelproces van informatietransformatie. Dit gebeurt dan specifiek onder verantwoordelijkheid van het OM.

Na deze fase wordt de informatie verder veredeld naar producten zoals statistische overzichten, adviezen, te nemen maatregelen om kwetsbaarheden te verhelpen, preweegdocumenten etc.
Vervolgens worden deze resultaten beoordeeld op toe te passen waarde en nut en ter beschikking gesteld en verspreid naar de respectievelijke doelgroepen. Dit informatiemanagement is ook verantwoordelijk voor een juist gebruik en beheer van de verkregen informatie in dit informatieproces.

Het informatie-uitwisselingsproces is hierna visueel weergegeven.

Informatie-uitwisselingsproces



Het boven beschreven informatie-uitwisselingsproces heeft een nadrukkelijke oriëntatie op de opsporing en vervolging van cybercrime. In het NPAC/NHTCC advies wordt wat betreft de informatie-uitwisseling een veel breder perspectief gehanteerd, waarbij informatie uit publieke en private bronnen op elkaar worden betrokken. Dientengevolge is het boven gepresenteerde informatie-uitwisselingsproces dan ook niet een op een toepasbaar. Wel geldt ook voor de nationale infrastructuur cybercrime, dat de door het project HTC onderscheidde functies zoals informatievergaring, informatieanalyse en informatieverspreiding geadresseerd zullen worden.

4.3 Juridische randvoorwaarden informatie-uitwisseling High Tech Crime

De essentie van de werkzaamheden bij de bestrijding van High Tech Crime bestaat uit informatievergaring en informatie-uitwisseling over High Tech Crime tussen en/of met private partijen en/of overheidsorganisaties.
Een informatie-uitwisselingsproces brengt aansprakelijkheidsrisico's met zich mee. Aansprakelijkheidsrisico's kunnen worden beheerst door de inrichting en de naleving van zorgvuldige procedures. Zorgvuldige procedures ontstaan doordat de juridische randvoorwaarden van de toepasselijke wet- en regelgeving worden ingebed in de werk- en/of uitwisselingsprocessen. Deze juridische randvoorwaarden voor informatie-uitwisseling worden bepaald door de verantwoordelijkheden, de taken en bevoegdheden van de betrokken partijen.

Met het oog op een zorgvuldige informatie-uitwisselingprocedure is door het project een informatie-uitwisselingbeleid opgesteld. In paragraaf 4.2 is zowel een schematische weergave als een toelichting op dit informatie-uitwisselingbeleid opgenomen. De volgende concrete producten maken onderdeel uit van het informatie-uitwisselingbeleid:

- een informatie-uitwisselingbeleid politie-informatie;
- een informatie-uitwisselingbeleid/privacybeleid voor uitvoering van de Wet bescherming persoonsgegevens en het algemene aansprakelijkheidsrecht;
- de mogelijkheid tot de zogenaamde informatietransformatie.
- een conceptprocedure afhandeling WOB-verzoeken voor uitvoering van de Wet openbaarheid bestuur;
- een model samenwerkingsovereenkomst ten behoeve van een publiek private samenwerking;
- een intentieverklaring met de banken ten behoeve van de gezamenlijke bestrijding van High Tech Crime.

4.4 Bescherming Vitale Infrastructuren

Er bestaat grote zorg dat kwetsbaarheden in informatiesystemen of ongeautoriseerd gebruik van belangrijke digitale (informatie-)infrastructuren op enig moment een grote bedreiging kunnen vormen voor de Nederlandse samenleving en economie; of het nu gaat om slecht beveiligde of ingerichte computersystemen, grootschalige virtuele aanvallen, cybervandalisme of andersoortig ongewenst optreden in de digitale omgeving. Die zorg bestaat met name rondom zogenoemde vitale sectoren of knooppunten. Een van de taken van het project is te bekijken of de dreigingen in kaart gebracht kunnen worden en aan de hand daarvan een generieke set maatregelen te ontwikkelen waarmee die vitale sectoren of knooppunten beter beschermd kunnen worden.

Vitaal Knooppunt Schiphol

In het deelproject Vitaal Knooppunt Schiphol is Amsterdam Airport Schiphol als pilot-omgeving gekozen om te experimenteren met het opstellen van een digitaal dreigingsbeeld en zodoende ervaring op te doen met de bescherming van vitale informatie infrastructuren tegen zware georganiseerde criminaliteit en terrorisme. Daarbij wordt specifiek gekeken naar kwetsbaarheden voor crimineel misbruik van de informatie-infrastructuur en/of het verstoren of platleggen van vitale computersystemen en netwerken door digitale aanvallen van terroristische aard (zogenaamd 'bewust menselijk handelen').

De resultaten van verschillende activiteiten (WiFi scan, Digitaal Dreigingsbeeld Vrachtafhandeling, table top en model Stormcenter Luchthaven) leiden tot inzicht in de (mogelijke) digitale handelswijze van een crimineel en terrorist. Dit resulteert in enerzijds beschermende maatregelen en anderzijds een verbeterde informatiepositie indien een incident zich voordoet (proactieve aanpak). Het uiteindelijke doel is een generieke set maatregelen die leidt tot een blauwdruk van een 'cybersecure' regio, die eveneens toe te passen is op andere vitale knooppunten. Bij generieke maatregelen wordt gedacht aan een 'Stormcenter', CERT Luchthaven, digitaal crisisbeheersplan luchthaven, triage cyber incidenten.

Om een totale blauwdruk van de 'cybersecure'; regio Schiphol te genereren is de huidige projectduur te kort gebleken. Een aantal onderdelen hiervan is echter al wel uitgevoerd of in voorbereiding:

- Zo heeft het 'WiFi onderzoek Schiphol' een overzicht opgeleverd van alle (toegestane en niet toegestane) draadloze computer netwerken op de luchthaven op een bepaald moment in het eerste kwartaal van 2005. Daarnaast zijn aan de hand van bekende kwetsbaarheden in de WiFi protocollen de dreigingen en risico's op de luchthaven inzichtelijk gemaakt. Het resultaat is dat vanuit het perspectief van een persoon met een crimineel oogmerk bekeken wordt welke mogelijkheden deze ziet om, via draadloze netwerken, toegang te krijgen tot vitale systemen op de luchthaven. Hierbij worden de in theorie bekende kwetsbaarheden in de praktijk getoetst. Aan de hand van het verkregen over-

zicht zijn mogelijke zwakke plekken op de luchthaven gelokaliseerd.

Nader onderzoek zal moeten aantonen of deze punten ook echt door criminelen gecompromitteerd kunnen worden.
Een tweetal bevindingen zijn nu al noemenswaardig. Ten eerste blijkt dat de beveiligingsgraad van WiFi netwerken op de luchthaven gemiddeld hoger ligt dan in andere delen in het land. Ten tweede zijn WiFi netwerken eenvoudig en tegen lage kosten te implementeren waardoor gemakkelijk wildgroei kan ontstaan. Het is dus aan raden om op de luchthaven een faciliteit in te richten om de draadloze netwerken te kunnen monitoren.
Voordeel daarvan is dat de beheerder van de luchthaven wildgroei kan voorkomen en dat de overheid op haar beurt inzicht kan krijgen op welke wijze getracht wordt informatie-infrastructuur te compromitteren (informatiepositie).

- Naar analogie van het Internet Stormcenter dat waarschuwingen afgeeft als op het Internet gevaarlijke virussen rondwaren, domeinen onder vuur liggen door hackers of netwerken 'platgelegd' worden door 'denial of service' (dDos) aanvallen is een concept Stormcenter[6] uitgewerkt voor de luchthaven.
  Dat Stormcenter houdt de meest vitale computersystemen en netwerken op de luchthaven in de gaten en waarschuwt als er verdacht dataverkeer op deze netwerken plaats vindt, of als er serieuze hackpogingen gedaan worden. Aan de hand van de geleverde gegevens worden passende maatregelen genomen door in eerste instantie individuele actoren op de luchthaven en in een latere fase door een nog in te stellen digitaal crisisoverleg. In het crisisoverleg zijn de betrokken publieke en private partijen vertegenwoordigd. De volgende stap is aan de hand van dit concept Stormcenter Luchthaven een pilot netwerk van sensoren te implementeren op een aantal vitale netwerken op de luchthaven en daarmee een lokaal Stormcenter te creëren.

- De vrachtafhandeling geldt als één van de vitale processen op de luchthaven. Ook hier is de afhankelijkheid van ICT groeiende. Dat betekent dat ook criminelen misbruik maken van de informatie-infrastructuur of dat het vrachtafhandelingsproces verstoord of platgelegd kan worden door digitale aanslagen. Het lopende project Digitaal Dreigingsbeeld Vrachtafhandeling legt de kwetsbaarheden voor crimineel misbruik en digitale aanvallen vast in een dreigingsbeeld. Waar nodig worden tegenmaatregelen geadviseerd om de informatie-infrastructuur beter te beschermen. De voordelen voor de opsporings- en inlichtingendiensten zijn een verbeterde informatiepositie en de mogelijkheid om proactief te kunnen werken.

- Daar waar de noodplannen in traditionele zin op de luchthaven gemeengoed zijn, mist een plan als onverhoopt een computersysteem of netwerk verstoord wordt en daarmee een vitale functie van de luchthaven uitvalt. Een table top

[6] De kern van een Stormcenter is een centrale database waarin gegevens worden verzameld die afkomstig zijn van digitale systemen en netwerken van een bepaalde sector of knooppunt, bijvoorbeeld de financiële sector of de luchthaven schiphol. Op basis van deze data kunnen aanvallen op computersystemen worden gedetecteerd, geanalyseerd en eventueel voorkomen.

bijeenkomst, waarin een digitale ramp door (publieke en private) sleutelpartijen op Schiphol nagespeeld wordt levert de nodige input voor het digitaal crisisbeheersplan.

Het is duidelijk dat de hiervoor genoemde activiteiten een bijdrage leveren aan de blauwdruk van de 'cybersecure' regio Schiphol, maar dat voor een complete en hanteerbare blauwdruk het project ook na oktober 2005 doorgang moet vinden.

4.5 Digitaal crisisbeheersingsplan

In oktober/november 2004 is een aantal websites van de overheid dagenlang platgelegd door een dDos aanval. Een snelle en adequate reactie van de betrokken partijen om de aanval te stoppen en de aanvaller(s) op te sporen bleef uit omdat een aantal zaken ontbrak. Zo was er nauwelijks coördinatie en verliep de communicatie tussen partijen ad hoc. Het blijkt dat er bij een dergelijke digitale aanval een protocol ontbreekt dat er voor zorgt dat de betrokken partijen bij elkaar komen om de situatie in te schatten en adequate acties uit te zetten.
Op initiatief van het project High Tech Crime zijn de betrokken partijen bij elkaar gebracht en de dDos aanvallen in gezamenlijkheid geëvalueerd.
Het resultaat hiervan is het voorstel een digitaal crisisbeheersingsplan te maken in het geval dat vitale sectoren of knooppunten te maken krijgen met grootschalige digitale aanvallen. Een afgeleide hiervan is het voornemen eerst voor Schiphol een dergelijk plan te maken (zie ook het Deelproject Vitaal Knooppunt Schiphol).

4.6 Samenwerking

In de projectperiode is veel energie gestoken in het aangaan van goede samenwerkingsafspraken met zowel publieke als private partijen. Met name in de laatste maanden begint dit zijn vruchten af te werpen. Zo zijn inmiddels partijen als Shell, KLM, Cisco, Microsoft, Schiphol Group, KPN en andere meer dan bereid om te komen tot intensieve vormen van informatie-uitwisseling. Ook met organisaties uit de publieke sector zijn inmiddels goede contacten gelegd of worden deze in gang gezet, te denken valt hierbij aan GOVCERT.NL, de AIVD, OPTA, Agentschap Telecom en natuurlijk diverse onderdelen binnen de politie- en justitieketen. In het bijzonder is veel aandacht geschonken aan de samenwerking met de banken, waarover meer in de volgende paragraaf.

<u>Samenwerking en informatie-uitwisseling project High Tech Crime & Banken</u>
De opkomst van de digitale dienstverlening maakt dat banken en hun klanten kwetsbaar worden voor criminaliteitsvormen die zich manifesteren op het Inter-

net. Phishing[7], denial of service attacks en online identity theft zijn daarvan voorbeelden. Een eenzijdige bestrijding door de overheid of het bedrijfsleven levert onvoldoende resultaat op.
In het deelproject Internet Banking Fraud heeft het project HTC samen met de Nederlandse Vereniging van Banken (NVB) onderzocht in hoeverre nauwere samenwerking kan leiden tot betere resultaten in de bestrijding van High Tech Crime. Doel van deze samenwerking is om met name Phishing aan te pakken en de problematiek van High Tech Crime bij de banken inzichtelijk te maken. Daarvoor wordt een veilig en betrouwbaar informatiekanaal gerealiseerd om informatie uit te wisselen met de banken. De samenwerking en informatie-uitwisseling moeten er ook toe leiden dat flexibel en snel gereageerd wordt op nieuwe bedreigingen en soorten van digitale criminaliteit, die een bedreiging vormen voor e-banking. Dit heeft in juli 2005 nader vorm gekregen door het afsluiten van een intentieverklaring tussen het project HTC en de NVB die namens negen grote banken tekende. Daarbij werd afgesproken een wederzijdse loketfunctie in te richten, waardoor een veilige informatie-uitwisseling kan plaatsvinden.
Als directe uitkomsten van de samenwerking behoren ook het ontwikkelen van procedures en maatregelen om frauduleuze websites en andere of nieuwe verschijningsvormen van High Tech Crime tegen te houden en aan te pakken.

De samenwerking leidt er ook toe dat flexibel en snel gereageerd kan worden op nieuwe bedreigingen en soorten van digitale criminaliteit, die een bedreiging vormen voor e-banking. Bovendien is ook afgesproken dat de haalbaarheid en wenselijkheid van een digitaal crisisbeheersplan en een Stormcenter voor de financiële sector onderzocht wordt.
Gedurende de projectperiode van het HTC is er al een regelmatige stroom van informatie-uitwisseling op gang gekomen, waarbij inmiddels ook al diverse kleinere en enkele grotere resultaten konden worden geboekt, conform de geformuleerde doelstellingen (het doen verwijderen van frauduleuze websites, adviezen, informatie over nieuwe dreigingen etc.).

Aangezien het project dit jaar haar werkzaamheden stopzet zal de intentieverklaring als zodanig niet worden voortgezet. Het is de verwachting dat tussen de beoogde opvolgorganisaties en de banken nieuwe afspraken worden gemaakt over structurele vormen van samenwerking.

4.7 Opsporingsonderzoek High Tech Crime

High Tech Crime opsporingsonderzoeken zijn vaak complex, innovatief, internationaal en staan zelden op de prioriteringslijsten van de opsporingsdiensten. Zowel

[7] Phishing is een vorm van oplichting waarbij criminelen door gebruikmaking van geraffineerde, veelal digitale technieken consumenten misleiden om hen vertrouwelijke informatie te ontlokken. De term Phishing is ontstaan uit een combinatie van het woord 'Fishing' (hengelen) en 'Phreaking'. Laatstgenoemde term wordt binnen de hackersgemeenschap gebruikt voor het kraken van telefoonsystemen. Identiteitsdiefstal staat centraal bij Phishing. Vaak is sprake van een combinatie van misleiding door social engineering en het gebruik van kwetsbaarheden in webapplicaties.

ten behoeve van het verkrijgen van (kwalitatief) inzicht in High Tech Crime alsmede om vanuit een praktisch perspectief ervaring en kennis op te doen, is in de projectperiode door projectleden deelgenomen aan een opsporingsonderzoek van de Nationale Recherche dat in al zijn facetten een High Tech Crime zaak was.

Dit onderzoek is gericht op een groep cybercriminelen en loopt nog op het moment van schrijven. Zonder in detail te treden valt een aantal, voor High Tech Crime, karakteristieke zaken op:

- Al snel na de start van het onderzoek is te zien dat de groep cybercriminelen geen kans onbenut laat om het internet te compromitteren.
  De groep heeft controle over een omvangrijk botnet en een veelheid aan gehackte internetdomeinen en netwerken. Naast de noodzaak om de criminelen op te sporen, laat het onderzoek zien dat er verschillende momenten zijn om tegenhoudacties te ondernemen en daarmee het botnet onschadelijk te maken en de gehackte netwerken te schonen. Karakteristiek aan het gebruik van botnets is dat het hacken en infecteren van computers grotendeels automatisch verloopt.
  Het is dus niet voldoende om de criminelen vast te zetten, omdat het botnet niet altijd afhankelijk is van de crimineel om te kunnen groeien en de illegale activiteiten uit te voeren. Het is eveneens noodzakelijk om naast het oppakken van de verdachten ook het botnet te ontmantelen. Daarmee wordt het instrumentarium van de crimineel onbruikbaar en wordt de illegale activiteit gestopt.
- In deze zaak worden de criminelen én opgepakt wegens strafbare feiten én tegengehouden door het ontmantelen van het botnet. Dat is een ideale combinatie. De verwachting is echter dat er niet voldoende capaciteit is (ook niet in de toekomst) om in alle gevallen de daders op te sporen en te vervolgen. In die gevallen is het ontmantelen van het botnet op zichzelf ook een nuttige activiteit waarmee in ieder geval de criminele activiteit gestopt wordt. Ervaring uit deze zaak is ook dat dergelijke tegenhoudacties niet kunnen plaatsvinden zonder internationale samenwerking met de CERT's (Computer Emergency Response Team) en de internet providers.
- Ook komt misbruik van internetdiensten en betaalmethodes aan het licht. Er worden innovatieve en deels nieuwe vormen van financiële en frauduleuze transacties bedacht om digitaal geld (bijvoorbeeld in de vorm van PayPal of eGold) te stelen en om te zetten in traditioneel geld.
- Hoewel de zaak begint met de aangifte van een enkele hack, blijkt dat door het snelle karakter van het Internet niet één keer computervredebreuk wordt gepleegd, maar dat dit bijna constant het geval is (naast de andere strafbare activiteiten zoals bijvoorbeeld het schrijven van virussen en phishing).
- Opvallend is dat de modus operandi nogal eens wisselt en evolueert omdat de cybercriminelen zich steeds voor nieuwe situaties gesteld zien. Een voorbeeld daarvan is dat de groep genoodzaakt wordt nieuwe Trojans te schrijven omdat het gebruikte Trojaanse paard op een gegeven moment door antivirus makers in viruslijsten wordt opgenomen. De werkwijze van de groep boet dan snel aan effectiviteit in en moet vernieuwd worden.

- In dit onderzoek wordt ook het vermoeden bevestigd dat de georganiseerde criminaliteit zich ook inlaat met High Tech Crime en de daarvoor benodigde kennis inhuurt. Een voorbeeld hiervan is dat de betrokken cybercriminelen in opdracht van criminelen uit het Oostblok zogenaamde Trojans maken met Phishing als doel.
- De omvang van het ontmantelde botnet en het innovatieve karakter van de zaak heeft geresulteerd in internationale bekendheid van de zaak en de naamsbekendheid van het NHTCC in haar projectfase. Het ontmantelen van het botnet en de samenwerking tussen politie, CERT's en internet providers wordt ook internationaal gezien als een belangrijke ontwikkeling in de bestrijding van High Tech Crime.
- De aandacht in de media heeft ook als resultaat dat het plegen van High Tech Crime als een ernstige aangelegenheid beschouwd wordt. Naast het feit dat blijkbaar noodzakelijk is om goed beveiligd het Internet op te gaan, gaat van het oppakken van de hackers ook een afschrikkend effect uit.
- Doordat de activiteiten van de groep cybercriminelen feitelijk wereldwijd plaatsvinden, blijkt dat er op allerlei plaatsen informatie verzameld is over de groep of individuele leden daarvan. Het bekend worden van de aanhoudingen in de zaak heeft die informatie-uitwisseling extra aangejaagd met als gevolg dat extra aangiften en informatie uit het buitenland is binnengekomen. Markant is dat het niet alleen politie-informatie betreft, maar dat ook de antivirusmaatschappijen en de grote bedrijven uit de internetindustrie beschikken over nuttige informatie over de cybercriminelen en hun werkwijze. Samenwerking met deze partijen versterkt de informatiepositie van het onderzoeksteam.

Het opsporingsonderzoek van oudsher aan het eind van de keten en het oppakken van de criminelen is hetgeen wat vaak een grote impact heeft. Toch laat deze zaak zien dat bestrijding van High Tech Crime, meer nog dan andere criminaliteit, gebaat is bij ten eerste een meer proactieve werkwijze door bijvoorbeeld High Tech Crime tegen te houden en ten tweede gebaat is bij (internationale) samenwerking; met de rest van de ketenpartners, maar ook daarbuiten met bijvoorbeeld de internetindustrie.

Naast de boven beschreven zaak heeft zich gedurende de projectperiode een aantal grotere en kleinere High Tech Crime zaken aangediend die niet opgepakt zijn. Dergelijke onderzoeken leveren een schat aan informatie op over modus operandi van cybercriminelen én over de meest effectieve werkwijze van de speurder die ze najaagt. De opgedane kennis en ervaring leveren bewijs en leerzaam materiaal voor adviezen over High Tech Crime; zowel voor de werkwijze met betrekking tot toekomstige onderzoeken als voor tegenhoudacties, proactief handelen of preventieve maatregelen.

4.8 Uitwisseling van kennis en expertise

Op het zich snel ontwikkelend en kennisintensieve terrein van High Tech Crime is het onontbeerlijk om goed geïnformeerd te zijn over methoden en technieken die cybercriminelen gebruiken en om goed geëquipeerd te zijn teneinde de verschillende vormen van High Tech Crime te bestrijden. Daarvoor heeft het project HTC een aantal specifieke verschijningsvormen van High Tech Crime onderzocht. De analyses daarvan zijn gedeeld met de direct betrokkenen. Enkele voorbeelden hiervan zijn:

- De eerder beschreven WiFi scan, die niet alleen een overzicht van de gebruikte draadloze netwerken op de luchthaven geeft maar ook inzicht biedt in de kwetsbaarheden die het gebruik van de technologie met zich meebrengt.

- De evaluatiebijeenkomst van de dDos aanvallen op de websites van de overheid in oktober 2004. Deze bijeenkomst leverde naast een dialoog tussen betrokken partijen nuttige informatie op over de kwetsbaarheid van internetdiensten voor digitale aanvallen, de werkwijze van de daders en de gebruikte technieken.
  Kennis die gebruikt kan worden bij het voorkomen en oplossen van toekomstige security incidenten met een wellicht nog vitaler functie in de samenleving.
- Onderzoek naar het fenomeen phishing. Het project heeft een studie verricht om te achterhalen welke technieken gebruikt worden en hoe de modus operandi van de 'Phishers' zich ontwikkeld heeft.
  De resultaten zijn gedeeld met onder meer de banksector zelf en in een specifiek geval is een oplossing aangedragen om een daadwerkelijke aanval te verijdelen.
  Zowel op het gebied van spam, botnets en Trojans (allemaal aspecten van Phishing) heeft het project HTC informatie verzameld en uitgedragen naar direct betrokken partijen en grotere en kleinere werkgroepen in binnen- en buitenland.
- Per brief zijn betrokken partijen geïnformeerd over de internet telefoniedienst Skype en met name over criminele gebruiksmogelijkheden ervan. Doordat de telefoniedienst gebruik maakt van internetprotocollen, standaard encryptie heeft en overal gebruikt kan worden waar een internetverbinding is, wordt het erg moeilijk gesprekken te onderscheppen of abonnees te achterhalen. Met de brief heeft het project deze problemen willen agenderen om in samenwerking oplossingen te kunnen bedenken.

4.9 Internationale samenwerking

Het gegeven dat High Tech Crime zich voornamelijk afspeelt in de digitale omgeving en dat daardoor traditionele grenzen nauwelijks betekenis hebben en afstanden heel anders ervaren worden, betekent dat High Tech Crime per definitie een internationaal karakter heeft.
De internationale uitwisseling van kennis, ervaring en informatie is cruciaal bij het goed functioneren van een High Tech Crime Center bij de politie.
Er is hierbij een aantal aspecten te noemen:

- Voor het opzetten van een opsporingsteam High Tech Crime bij de politie is het van belang om met zusterorganisaties die al enige tijd bestaan zoals de National High Tech Crime Unit (NHTCU) en het Australian High Tech Crime Centre (AHTCC) van gedachten te wisselen over de missie, de taken en organisatie van een dergelijk team. Uit verschillende bezoeken over en weer is gebleken dat het gevoerde informatie regime, het multidisciplinaire ('multi-agency') karakter, het internationale netwerk en goede 'backoffices' belangrijke aspecten zijn voor het succesvol opereren van een High Tech Crime Center bij de politie.
- Een goed internationaal netwerk is belangrijk om op operationeel niveau zaaksgerelateerde informatie te kunnen uitwisselen met zusterorganisaties in het buitenland. Daarvoor is enerzijds een vertrouwensbasis nodig en ander-

zijds de mogelijkheid om met vertrouwelijke (politie) informatie om te kunnen gaan.
In dit netwerk zijn naast contacten met de directe zusterorganisaties (NHTCU, AHTCC etc.), ook de contacten met buitenlandse en internationale politieorganisaties (Interpol, Europol) van belang.
Steeds meer blijkt dat contacten met de (internet-)industrie waardevol zijn bij het speuren naar internationaal opererende cybercriminelen.

- Ook internationale rechtshulp en de formele informatie-uitwisseling is een factor van betekenis, eenvoudigweg omdat er veel naspeuringen in het buitenland gedaan moeten worden om een High Tech Crimezaak tot een goed einde te brengen.
  Door het project is kennis verworven die kan worden ingezet om specifieke vragen met betrekking tot High Tech Crime te kunnen beantwoorden. Daarmee kan het LIRc of één van de IRC's ondersteuning geboden worden indien er internationale rechtshulp verzocht wordt op het gebied van High Tech Crime.
  Voor een degelijke internationale positie is het eveneens noodzakelijk aan te haken bij de andere officiële kanalen voor informatie-uitwisseling, zoals het Interpol, Europol of Schengen kanaal.
- Naast operationele informatie-uitwisseling is ook het uitwisselen van kennis, ervaringen en best practices zeer nuttig. Zeker omdat High Tech Crime een innovatieve en kennisintensieve tak van sport is. Kennis die toegepast kan worden bij het speuren naar criminelen, maar ook bij het onschadelijk maken van criminele acties. Zo is een uit Duitsland afkomstig software script door bemiddeling van het project HTC, gebruikt bij het verijdelen van een grootschalige Phishing zaak bij een Nederlandse bank.
- Bij de verspreiding van kennis en expertise spelen internationale politieorganisaties zoals Europol en Interpol ook een grote rol. Met name door het bijeenbrengen van experts en het organiseren van inhoudelijke werkgroepen en expertbijeenkomsten met als doel de bestrijding van High Tech Crime te faciliteren. Leden van het project nemen deel aan de Europol expert meetings en de intentie bestaat om Nederland te vertegenwoordigen op de European Working Party on Information Technology and Crime van Interpol.
  Specifiek voor de bescherming vitale infrastructuur is het project HTC actief als 'point of contact' voor Politie (naast PoC's voor CERT's en vitale informatie infrastructuur) voor het International Watch, Warning and Incident Response Network.
  Een uitstekend voorbeeld van internationale publiekprivate samenwerking is de Taskforce Botnets, waar leden van het project HTC aan deelnemen en waar grote bedrijven met politie en justitie kennis uitwisselen over de zich snel ontwikkelende botnets.

Al deze activiteiten tonen aan dat één aanspreekpunt voor de internationale activiteiten op dit terrein onontbeerlijk is. Hierbij worden, indien van toepassing, de formele kanalen voor informatie-uitwisseling gebruikt. Onderwerpen die in internationaal verband nader uitgewerkt zullen worden, zijn onder meer procesgang

bij internationale rechtshulpverzoeken, deelname aan internationale taskforces en het bevorderen van joint investigation teams in het High Tech Crime-veld.

4.10 Conclusies

Uit de werkzaamheden zijn een aantal conclusies te trekken. Zij zijn gerubriceerd in onderwerpen die essentieel geacht worden bij de efficiënte en effectieve bestrijding van High Tech Crime.

Informatie
Informatie vergaren, analyseren, bewerken en vervolgens delen is een zeer belangrijke activiteit van het project High Tech Crime gebleken. De informatie heeft één grote gemene deler en dat is High Tech Crime.
De informatie is echter afkomstig uit geheel verschillende bronnen met diverse informatie regimes en wordt op verschillende abstractieniveaus (operationeel, kennis en expertise, strategisch) gebruikt. Informatie is afkomstig van bijvoorbeeld CERT's, bedrijven of zusterorganisaties in het buitenland.
De uitdaging zit in de bewerking van informatie uit de verschillende bronnen tot specifieke informatieproducten zoals inlichtingen, preweegdocumenten, kennisdocumenten of advies, zonder daarbij bepaalde regimes geweld aan te doen. Inzicht in complexe materie zoals High Tech Crime staat of valt met een degelijke informatiehuishouding. Bestrijding van High Tech Crime is in grote mate afhankelijk van de beschikbaarheid van informatie en de snelheid waarmee deze geleverd kan worden.

Aard en omvang
Het ontbreekt nog aan voldoende inzicht in de aard en omvang van High Tech Crime. Dit heeft tot gevolg dat deze vorm van criminaliteit weliswaar veel besproken is, maar niet voorkomt op de prioriteitenlijsten van de opsporingsinstanties en er geen bruikbare cijfers zijn die aangeven hoe groot het probleem nu werkelijk is. De survey verschaft op termijn het inzicht in de aard en omvang in kwantitatieve zin.

In kwalitatieve zin geeft initiëren of ondersteunen van daadwerkelijke opsporingsonderzoeken inzicht in de bestrijding van High Tech Crime. Deze onderzoeken leveren kennis op over de innovatieve aanpak van cybercriminelen én over de beste aanpak van de speurders. Daarnaast blijkt uit deze High Tech Crime onderzoeken dat naast de opsporing ook tegenhoudacties of preventieve maatregelen heel goed mogelijk zijn. Sterker nog dat een effectieve bestrijding van High Tech Crime een integrale aanpak is, waarbij preventie, pro-actie, tegenhouden en opsporing alle onderdeel zijn van het proces.

Expertise
High Tech Crime is een kennisintensieve tak van sport die gedreven wordt door snelle technologische ontwikkelingen. De bestrijding van High Tech Crime leunt

voor een groot deel op de kennis van de technologische ontwikkelingen en de wijze waarop de crimineel van die ontwikkelingen gebruik maakt. Voor de effectieve bestrijding van High Tech Crime is het nodig dat de expertise op peil gehouden wordt en belangrijker nog op een centrale plaats toegankelijk is. Het betreft overigens niet alleen technische expertise, het betreft bijvoorbeeld ook kennis over best practices, gebruikte modus operandi en dadergroepen.

Samenwerking en afstemming

In de projectfase is de noodzaak tot samenwerking met publieke én private partijen duidelijk geworden. High Tech Crime kent een groot aantal betrokkenen die allen een stuk van de puzzel hebben als het gaat om het oplossen van zaken.

Het is dus noodzakelijk om samen te werken om op operationeel en strategisch niveau High Tech Crime aan te pakken. Voor de hand liggend is dat het samenwerking met zusterorganisaties in het binnen en buitenland betreft. Steeds meer betreft het echter ook samenwerking met private partijen die 'slachtoffer' zijn of op andere wijze betrokken zijn bij de High Tech Crime, bijvoorbeeld als leverancier van de informatie-infrastructuur of softwareontwikkelaar.

Met name daar waar het gaat om vitale informatie-infrastructuur is publiekprivate samenwerking nodig. Dat blijkt onder meer uit de samenwerking met de bancaire sector en die op de luchthaven schiphol. Eveneens is in het geval van High Tech Crime het niet de politie alleen die een bepaalde verantwoordelijkheid draagt. Ook andere overheidsorganen spelen ieder een specifieke rol bij de bestrijding van High Tech Crime dan wel de bevordering van IT-security of hebben een bepaald belang bij een ernstig ICT security incident. De evaluatie van de dDos aanvallen laat zien dat in dergelijke gevallen de afstemming ontbreekt en het belangrijk is om spoedig na het incident de verschillende partijen aan tafel te hebben en gezamenlijk beslissingen te kunnen nemen. Het is evident dat de uitgangspunten van het werken in een 'multi-agency' verband en publiekprivate samenwerking een belangrijke rol spelen.

Internationale positie

Gebleken is dat High Tech Crime een internationaal karakter heeft. Dit impliceert dat ook de oriëntatie van een High Tech Crime Center internationaal is. Zowel de formele als ook de informele kanalen van informatie-uitwisseling zijn belangrijk om snel te kunnen reageren op incidenten. Daarnaast is een internationaal netwerk belangrijk om kennis en ervaringen te delen. Het LIRc of één van de IRC's .kan ondersteuning geboden worden indien er internationale rechtshulp verzocht wordt op het gebied van High Tech Crime. Verdere uitwerking van onderwerpen zoals de procesgang bij internationale rechtshulpverzoeken, deelname aan internationale taskforces en het bevorderen van joint investigation teams leveren een constructieve bijdrage aan de internationale bestrijding van High Tech Crime.

Ook uit het pilot-opsporingsonderzoek waarin het project een groot aandeel heeft gehad, blijkt het internationale karakter van High Tech Crime en de noodzaak tot internationale samenwerking; met zusterorganisaties in het buitenland, met an-

dere ketenpartners zoals GOVCERT maar ook daarbuiten met bijvoorbeeld de internet industrie. Deze samenwerking verbetert de informatiepositie van het onderzoeksteam en is eveneens noodzakelijk om invulling te kunnen geven aan de proactieve aanpak door (wereldwijde) tegenhoudacties. Daarvan is het ontmantelen van een omvangrijk botnet een goed voorbeeld.

Door deelname aan internationale werkgroepen en samenwerking met internationale partners binnen en buiten de keten, maar vooral ook door het oppakken van een High Tech Crime zaak is het project High Tech Crime internationaal goed zichtbaar geweest. De naamsbekendheid van het NHTCC is dan ook zeer goed te noemen; evenzo geldt dat het project HTC gezien wordt als een betrouwbare partij om informatie mee uit te wisselen.

<u>Bescherming vitale informatie-infrastructuur</u>
Het project Vitaal Knooppunt Schiphol heeft tot nu toe laten zien dat High Tech Crime wel degelijk invloed kan hebben op vitale informatie-infrastructuur. Het in kaart brengen van digitale dreigingen vanuit crimineel of terroristisch perspectief, ofwel vanuit het perspectief van bewust menselijk handelen, kent een drietal belangrijke aspecten.
Ten eerste levert het maatregelen op tegen crimineel misbruik van de vitale computersystemen en netwerken en tegen verstoring van vitale processen. Ten tweede levert het de overheidsdiensten op de luchthaven een verbeterde informatiepositie op zodat in geval van dreigend digitaal onheil, proactief te werk gegaan wordt. Als derde punt wordt publiekprivate samenwerking als onontbeerlijk gezien omdat zonder medewerking van de partijen op de luchthaven er geen toegang is tot de vitale infrastructuur.

De voorlopige resultaten van het project Vitaal Knooppunt Schiphol laten gedeelten zien van het digitale dreigingsbeeld van de luchthaven. Eveneens wordt duidelijk dat bij de verschillende partijen op de luchthaven de behoefte bestaat aan een duidelijk dreigingsbeeld.

De projectactiviteiten zullen echter ook na oktober 2005 doorgang moeten vinden alvorens gesproken kan worden van een generieke set maatregelen voor het maken 'cybersecure regio's'.
Ten slotte staat vast dat dergelijke onderzoeken ook voor andere vitale sectoren gedaan zouden moeten worden.

<u>Vormgeving en integrale aanpak</u>
Gedurende de projectfase is nog eens duidelijk geworden dat diverse partijen uit verschillende geledingen van de Nederlandse maatschappij, zowel publiek als privaat, opsporing, vervolging en wetgeving etc. een rol hebben in de bestrijding van High Tech Crime. Voor zover kennis over dit onderwerp al aanwezig is, is deze sterk versnipperd en gefragmenteerd. Elke partij heeft haar eigen specifieke

taken en verantwoordelijkheden, maar deze zijn voor de specifieke bestrijding van High Tech Crime niet altijd duidelijk, afgebakend, of met elkaar afgestemd. Is bijvoorbeeld de aanpak en bestrijding van HTC een verantwoordelijkheid van ICT-expertise en ICT-organisatie of van OM en politie? Is beveiliging van IT in de vitale infrastructuur een aangelegenheid voor CERT's en overheid of van bedrijfsleven? Tijdens het project is nog eens bevestigd en de vorige bevindingen tonen dat ook aan, dat een effectieve bestrijding van High Tech Crime alleen kans van slagen heeft wanneer bestaande taken en verantwoordelijkheden goed op elkaar worden afgestemd en een multidisciplinaire aanpak wordt gerealiseerd.

In de multidisciplinaire aanpak is het mogelijk om in zeer korte tijd direct een afgewogen oordeel te vormen welke maatregel het grootste effect zal sorteren, voorkomen door preventieve maatregelen of procedures, tegenhouden en opsporen. Een combinatie van deze drie maakt een effectieve bestrijding mogelijk. Het project HTC heeft aangetoond, onder andere in de (deels) uitgevoerde deelprojecten, dat een integrale en gecoördineerde aanpak noodzakelijk is om dat inzichtelijk te maken en een daarbij passende vormgeving in structuur wenselijk is om de vereiste taken en verantwoordelijkheden te bundelen om deze aanpak de komende jaren effectief en efficiënt te realiseren.

<u>Witte vlekken</u>
Uiteindelijk kan worden vastgesteld dat er op het gebied van een meer doelgerichte bestrijding van High Tech Crime er nog de nodige witte vlekken zijn. Deze witte vlekken zijn er op de volgende onderdelen van High Tech Crime:

1. Het ontbreken van hoogwaardige kennis en expertise op het terrein van High Tech Crime;
2. Onvoldoende nationale en internationale afstemming en informatie-uitwisseling van High Tech Crime, zowel met private als met publieke partijen;
3. Onduidelijkheid bij het tegenhouden of verstoren van vormen van High Tech Crime;
4. Geen ondersteuning van en de voorbereiding op opsporingshandelingen tegen cybercriminelen;
5. Te weinig capaciteit bij de opsporing en vervolging van cybercriminelen.

In het vervolgtraject dienen deze te worden aangepakt.

5. Uitgangspunten en criteria bij de aanpak van HTC

5.1 Uitgangspunten

Op basis van de inzichten die zijn vergaard door middel van het project High Tech Crime en die beschreven zijn in de vorige hoofdstukken is een aantal uitgangspunten geformuleerd. Deze uitgangspunten bepalen mede door wie de te verrichten taken het best kunnen worden uitgevoerd.

a. <u>De bestrijding van HTC vergt een integrale aanpak</u>
Een integrale aanpak is nodig omdat een effectieve bestrijding van High Tech Crime niet tot stand komt als alleen wordt gefocusseerd op één van bovengenoemde witte vlekken (zie 4.10). Het is juist de combinatie van de aanpak van deze lacunes die een effectieve bestrijding mogelijk maakt. High Tech Crime is niet een specifiek politie- of bedrijfsprobleem. Wanneer criminelen of terroristen gebruik maken van de digitale snelweg doorkruisen zij ontzettend veel meer fysieke en virtuele territoria dan ooit tevoren. Wil de aanpak van deze criminelen succesvol zijn dan:
   - zal snel relevante informatie moeten kunnen worden uitgewisseld tussen politie en het bedrijfsleven over zaken als internetdiensten, logging en registratiegegevens, gebruiks- en verbruiksgegevens en gebruikte software en hardware etc.;
   - zal snel met andere overheidsinstanties moeten worden samengewerkt door middel van het uitwisselen van inlichtingen en informatie over verdachte(n), activiteiten, doelwit en de mogelijke consequenties van het handelen van de verdachte(n);
   - zal in voorkomende gevallen zo snel mogelijk 'grensoverschrijdend' informatie uitgewisseld moeten kunnen worden;
   - zullen de geleerde lessen met alle betrokkenen/belanghebbenden, mogelijk ter voorkoming van toekomstige incidenten, gedeeld moeten kunnen worden.

b. <u>De bestrijding van HTC vergt een publiekprivate samenwerking</u>
Voor die integrale aanpak is het vanzelfsprekend dat nauw wordt samengewerkt met diverse partijen van zowel de publieke als private sector, inclusief opsporing.
   - *Samenwerking met publieke partijen*
     Diverse instellingen en organisaties hebben taken en verantwoordelijkheden op het gebied van het identificeren, voorkomen, tegenhouden en opsporen van High Tech Crime. Al die partijen beschikken daarbij over eigen bevoegdheden en verantwoordelijkheden. Zonder in die bevoegdheden te

willen treden, moet er wel worden zorggedragen voor een goede informatie-uitwisseling.

- *Samenwerking met private partijen*
  Private partijen zijn een belangrijke bron van informatie ten aanzien van de vormen van High Tech Crime die vanuit de optiek van het bedrijfsleven prioriteit hebben om te worden aangepakt. Tegelijkertijd heeft het bedrijfsleven een duidelijke behoefte aan deskundige adviezen en ondersteuning bij het voorkomen van High Tech Crime en wil daarin ook betrokken worden.
  Daarnaast beschikken private partijen over kennis, ervaring en informatie over HTC omdat zij bijvoorbeeld onderdeel zijn van de infrastructuur, eigenaar, beheerder of gebruiker zijn van een vitale structuur die van belang is voor de vergroting van de weerbaarheid van de samenleving. -Voor informatie-uitwisseling is vertrouwen een noodzakelijke voorwaarde. Private partijen willen informatie delen als deze maar niet direct en vanzelfsprekend in 'de opsporing' verdwijnt. Hiertoe moeten waarborgen, zoals overeenkomsten, gerealiseerd worden, waarbij deze private partijen als oorspronkelijke eigenaar van de informatie nadrukkelijk toestemming geven hoe om te gaan met hun informatie.

c. <u>Vraaggericht werken</u>
Het is van belang zoveel als mogelijk vraaggericht te werken in plaats van aanbodgericht. Het ene slachtoffer van High Tech Crime zal bij een vergelijkbaar misdrijf en andere oplossing willen dan een volgend slachtoffer.

d. <u>Geen overlap</u>
Doe geen zaken die elders ook al gedaan worden en maak zoveel als mogelijk gebruik van die maatregelen die al in de goede richting gaan of van die organisaties die al op hetzelfde onderdeel van het takenpakket actief zijn.

e. <u>Neem geen bevoegdheden over en creëer geen nieuwe organisaties waar dat niet strikt noodzakelijk is</u>
Laat de verantwoordelijkheden en bevoegdheden daar liggen waar zo op grond van wet- en regelgeving, via andere formele afspraken, of op grond van het soort organisatie thuishoren.

f. <u>Werk praktijkgericht</u>
Zorg dat je leert van de praktijk en ga met behulp van experimenten na waar een taak of maatregel het best kan worden uitgevoerd.

g. <u>Er moeten voldoende mogelijkheden voor een betrouwbare informatie-uitwisseling zijn</u>
Informatie is de basis voor het realiseren van de doelstellingen. Deze informatie is, zoals eerder beschreven, afkomstig van publieke en private partijen. Veel van deze informatie heeft een vertrouwelijk karakter, moet onder bepaalde condities worden behandeld en afgeschermd zijn van de openbaarheid.

Dit is een absolute basisvoorwaarde wil er een vertrouwenwekkende werkomgeving ontstaan.

h. Vitale infrastructuren
De overheid beziet een aantal processen in Nederland met bijzondere aandacht. Vanuit het algemeen maatschappelijk belang zal de overheid extra eisen willen stellen aan een categorie bedrijven en instellingen in Nederland die een zogeheten vitale functie vervullen bij het ongestoord functioneren van de Nederlandse (soms zelfs wereldwijde) samenleving. In het project van de overheid met de naam Bescherming Vitale Infrastructuren is al enige tijd gewerkt aan het inzichtelijk maken van deze processen en de wijze waarop deze minder kwetsbaar kunnen worden gemaakt tegen inbreuken van verschillende aard en omvang. Door het toenemende gebruik van ICT en Internet wordt het steeds belangrijker om van deze bedrijven te weten in hoeverre zij vormen van digitale criminaliteit kunnen voorkomen, en indien zij hier toch mee in aanraking zijn gekomen, dit kunnen stoppen en de schade kunnen herstellen. Het project Schiphol is hiervoor mede opgezet.

5.2 Criteria

Het aanpakken van High Tech Crime laat zich op twee wijzen beschouwen. Namelijk enerzijds door het bestuderen van een verschijningsvorm van HTC om zodoende bekend te raken met de onderliggende technieken en methodieken, zoals dat bijvoorbeeld bij Phishing is gebeurd. Anderzijds in het oppakken van concrete activiteiten zoals tegenhouden en het adviseren bij een opsporing. Voorbeelden daarvan zijn het naspeuren van de dader(s) van de denial of service aanvallen op de overheidswebsites (2004) en het onschadelijk maken van de Postbank Phishing scam.

Aangezien High Tech Crime zich in allerlei vormen manifesteert; eenvoudig of complex, individueel of georganiseerd, zal de bestrijding van High Tech Crime eveneens verweven moeten zitten in het huidige politiebestel. Van de basispolitiezorg tot en met de landelijk opererende opsporingsorganisaties. Dat is momenteel nog niet het geval. De constructies waarmee bijvoorbeeld het gros van de traditionele rechercheonderzoeken gewogen worden, zijn niet geschikt voor High Tech Crime.
Daarnaast geldt dat bij High Tech Crime meer partijen betrokken zijn dan alleen slachtoffer en politie. Andere partijen zoals internet providers, de antivirus industrie of grote technologische bedrijven beschikken ook over belangrijke kennis met betrekking tot het strafbare feit, de gebruikte veelal nieuwe methodes of zelfs met betrekking tot de dader(s).

Het is verstandig een kader vast te stellen waarbinnen de betrokken organisaties hun taken en verantwoordelijkheden zullen moeten uitvoeren. Vanzelfsprekend dienen meer criteria tegelijkertijd van toepassing te zijn. De concrete invulling en aanscherping van deze criteria gebeurt in nauw overleg en in- en afstemming met de verschillende partijen.

Criteria voor het oppakken van een verschijningsvorm van HTC:

- Internationaal: in hoeverre betreft het een internationaal of mondiaal probleem?
- Internationale positie: in hoeverre is Nederland betrokken?
- Innovatiegraad: in hoeverre gaat het over een verschijningsvorm waarin nieuwe technologie, techniek of methodes gebruikt worden?
- Infectiegraad: in hoeverre zijn computersystemen en netwerken geïnfecteerd of gemanipuleerd?
- Bereik: hoe groot is het aantal potentiële slachtoffers?
- Schade: in hoeverre gaat het om grote financiële of maatschappelijke schade
- Vitaal: heeft het te maken met vitale sectoren of knooppunten?
- Nationaal belang: heeft het te maken met de Staatsveiligheid, met Openbare orde (verstoring van) en veiligheid of democratische rechtsorde?
- Snel en daadkrachtig optreden: in hoeverre is direct handelen en optreden noodzakelijk om bedreigende situaties te voorkomen?
- Landelijke coördinatie: is direct landelijke coördinatie noodzakelijk (bijvoorbeeld dDos op vitaal systeem ten behoeve van de samenleving?

Criteria voor het oppakken van een (opsporings-)onderzoek of tegenhoudactie, waarbij opsporingsbevoegdheden moeten worden toegepast:

- Organisatiegraad: in hoeverre gaat het om crimineel samenwerkingsverband (CSV)?
- Innovatiegraad: in hoeverre worden er nieuwe technologieën, technieken en methodes gebruikt?
- Infectiegraad: in hoeverre zijn computersystemen en netwerken geïnfecteerd of gemanipuleerd?
- Complexiteit.
- Multi-jurisdictie: in hoeverre heeft het strafbare feit linken naar het buitenland?
- Vitaal: heeft het te maken met vitale sectoren of knooppunten?
- Nationaal belang: heeft het te maken met de Staatsveiligheid, openbare orde of democratische rechtsorde?

Toetsing aan bovenstaande criteria zal uitmaken waar en op welk niveau (basispolitiezorg, bovenregionaal, landelijk) een onderzoek opgepakt kan worden. Dergelijke toetsing vindt momenteel niet plaats.
Wanneer onderzoeken complex, innovatief en internationaal zijn of als het de vitale infrastructuur betreft, zijn naast de uitvoering van een opsporingsonderzoek met name de leereffecten belangrijk.

In het NPAC/NHTCC adviesontwerp 'nationale infrastructuur bestrijding cybercrime' is opgenomen op welk politieniveau (landelijk, bovenregionaal, regionaal) bepaalde opsporingsonderzoeken dienen plaats te vinden.

6. Aanbevelingen

Op basis van de werkzaamheden zijn enkele aanbevelingen te verwoorden die gebruikt kunnen worden bij de opstelling van het eindadvies aan de Tweede Kamer.

6.1 Integrale aanpak High Tech Crime

Informatie-uitwisseling tussen alle betrokken partijen, zowel publiek als privaat, in een betrouwbare én vertrouwelijke omgeving wordt als cruciaal element gezien voor het succes bij de aanpak van High Tech Crime. Dit kan het best als deze partijen nauw met elkaar in contact kunnen treden op zowel strategisch als operationeel niveau.
Aanbevolen wordt derhalve de aanpak van cybercrime integraal vorm te geven en zodanig te organiseren dat de preventieve en repressieve aspecten bij de bestrijding ervan bijeengebracht kunnen worden.

De integrale aanpak van Cybercrime komt in het NPAC/NHTCC adviesontwerp 'nationale infrastructuur bestrijding cybercrime' zowel in de ontwikkelomgeving als in de beheersomgeving tot uitdrukking.

Ontwikkelomgeving: het implementatieprogramma Nationale Infrastructuur Cybercrime:
In de ontwikkelomgeving worden als onderdeel van het Actieplan Veilig Ondernemen II (AVO II) van het Nationaal Platform Criminaliteitsbeheersing (een publiekprivaat verband dat tot doel heeft de criminaliteit waarvan het bedrijfsleven slachtoffer is in gezamenlijkheid te bestrijden[8]) drie experimenten ter hand genomen die direct aansluiten bij de door het bedrijfsleven ervaren cybercrime:

- Een Notice and Take Down (NTD) experiment waarbij GOVCERT.nl in samenwerking met de Nederlandse Vereniging van Banken en de bancaire sector een NTD faciliteit ontwikkelt. Het toepassingsbereik van deze NTD faciliteit beperkt zich echter niet tot de bancaire sector. Ook voor niet bancaire incidenten waarbij behoefte is aan NTD, zoals bij haat-zaai sites en kinderporno is deze faciliteit na afloop van het experiment inzetbaar.
- Een MKB-experiment waarbij ECP.nl en Syntens in samenwerking met MKB Nederland daadwerkelijk bij een aantal geselecteerde MKB-bedrijven onderzoeken in welke mate deze bedrijven geconfronteerd worden met cybercrime, wat het beschermingsniveau is, in hoeverre systemen geïnfecteerd zijn en de maatregelen die in het kader van herstel nodig zijn. Daarnaast wordt het herstel ook ter hand genomen zodat de deelnemers aan het experiment ook op weg worden geholpen.

[8] Zie bijlage 1.

- Een experiment met de grote industrie dat tot doel heeft de kennisuitwisseling tussen deze bedrijfstak en de overige deelnemers aan de Nationale Infrastructuur Cybercrime op gang te brengen en te faciliteren. Achtergrond van dit experiment is het binnen het project High Tech Crime ontwikkelde inzicht 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. Het voornemen is het industrie experiment uit te voeren met een sector uit de groep van de zogeheten vitale infrastructuren zodat ook het raakvlak van cybercrime met de vitale infrastructuur aan bod kan komen.

Deze drie experimenten laten zien dat juist de publiekprivate samenwerking één van de belangrijkste pijlers is bij de experimenten die bij moeten dragen aan de Nationale Infrastructuur Cybercrime. Het vierde experiment, een met het MKB experiment vergelijkbaar onderzoek bij kleine gemeenten, laat zien dat de integrale benadering ook de publieke sector omvat en dat de aandacht bij de ontwikkeling van een Nationale Infrastructuur Cybercrime zich dus niet uitsluitend beperkt tot de private sector. Tot slot komt de integrale benadering in de ontwikkelomgeving tot uitdrukking in relatie tot het primaire doel van de ontwikkelomgeving: het neerzetten van een werkende nationale infrastructuur. De kiem voor de nationale infrastructuur wordt in het programma gelegd door de ontwikkeling van een informatieknooppunt. Kern van dit knooppunt is nu juist de betrokkenheid van zowel publieke als private partijen.

Beheersomgeving
De integrale benadering in de beheersomgeving blijkt met name uit het uitgangspunt bestaande organisaties die betrokken zijn bij de bestrijding van cybercrime meer op elkaar te betrekken. Er wordt als het ware een ringleiding gelegd tussen deze organisaties en de publieke en private partijen die slachtoffer zijn van cybercrime. In de ontwikkelomgeving wordt hier in het kader van het informatieknooppunt mee geëxperimenteerd. Het informatieknooppunt zal echter een vast onderdeel worden van de beheeromgeving. Ook bij het beleggen van nieuwe taken wordt zoveel mogelijk aansluiting gezocht bij bestaande instituties hetgeen een voorbeeld is van de integrale benadering.

6.2 Kennis en expertise

Cruciaal bij de aanpak van High Tech Crime is het hebben van afdoende kennis en expertise, met name omdat het werkterrein zo nieuw en innovatief is en telkens weer verder ontwikkeld. Derhalve wordt aanbevolen de kennis en expertise op het terrein van HTC verder te ontwikkelen en verspreiden. Dit kan door het:

- ontwikkelen van nieuwe methodes voor de bestrijding van High Tech Crime;

- verrichten van onderzoek naar bestaande en nieuwe vormen van High Tech Crime;
- uitvoeren van een jaarlijkse survey op het gebied van High Tech Crime;
- geven van gerichte adviezen aan de partners over nieuwe vormen van High Tech Crime en de manier waarop nieuwe methoden en technieken door cybercriminelen worden toegepast;
- aanleveren van informatie ten behoeve van Nationaal Dreigingsbeeld;
- verspreiden van kennis en expertise via congressen en symposia;
- verstrekken van informatie ten behoeve van trainingen en opleidingen;
- geven van adviezen voor de aanpassing van beleid en wetgeving.

De ontwikkeling van kennis en expertise is een andere pijler in het NPAC/NHTCC adviesontwerp 'Nationale Infrastructuur Bestrijding Cybercrime'. Ook dit is, vanuit het uitgangspunt aan te sluiten bij bestaande instituties, op verschillende plekken belegd.

Als eerste kan genoemd worden het implementatieprogramma Nationale Infrastructuur Cybercrime. De experimenten die in het kader van dit programma binnen de ontwikkelomgeving worden uitgevoerd dragen door hun opzet bij aan de ontwikkeling van kennis en expertise. Kennis zal worden verkregen omtrent de daadwerkelijke dreiging van cybercrime voor de bancaire sector, het MKB, de kleine gemeenten en, zij het in beperkte mate, de grote industrie. Daarnaast zal door deze experimenten expertise ontwikkeld worden. Bijvoorbeeld over het uitvoeren van Quick Scans om de mate van bedreiging en besmetting te kunnen beoordelen. Het NTD experiment zal expertise genereren aangaande het in samenwerking met de ISP's, CERT's en de getroffen bedrijven stoppen van de cybercrime aanval.

Ook in de beheersomgeving is veel aandacht voor de ontwikkeling van kennis en expertise. Zo zal bij het KLPD een expertisecentrum worden ingericht dat kennis en expertise verzameld om cybercrime-onderzoeken te kunnen uitvoeren en de partners in de strafvorderlijke keten over de aanpak, ontwikkeling en gevolgen van cybercrime te kunnen adviseren. Hierdoor wordt de opsporing op zowel het regionale, het bovenregionale en het nationale niveau ondersteund. Taken van het KLPD expertisecentrum zijn onder meer:

- Ontwikkelen van strategieën op het gebied van tegenhouden van cybercrime en het ontwikkelen van nieuwe opsporingsmethodieken.
- Uitwisselen van informatie, kennis en expertise met (inter-)nationale partners.
- Het gebruiken van informatie verkregen vanuit opsporingsactiviteiten en open bronnen voor de invulling van de expertisetaak en het selecteren van nieuwe onderzoeken.
- Het ondersteunen van andere onderdelen binnen de politie bij de opname van aangiftes.
- Ontwikkelen en implementeren van kengetallen omtrent opsporingsonderzoeken naar cybercrime.
- Het aanleveren van informatie ten behoeve van het Nationaal Dreigings-

beeld.
- Het signaleren van ontwikkelingen ten behoeve van aanpassing van beleid en wetgeving.
- Het leveren van input ten behoeve van training en opleiding binnen de politie.

Uitgaande van de bestaande instituties ter bestrijding van cybercrime is in de beheersomgeving voor de ontwikkeling van kennis en expertise een belangrijke taak belegd bij GOVCERT.NL. Nu reeds is het voor overheidsdiensten *het* aanspreekpunt voor kennis en expertise voor de bestrijding en voorkoming van cybercrime. De oriëntatie op de overheid wordt als eerste in het kader van de experimenten van het implementatieprogramma losgelaten. Op basis van de ervaringen met deze experimenten zal onderzocht worden of deze ruimere oriëntatie tot uitgangspunt kan worden gemaakt.

6.3 Aanspreekpunt

Veel betrokkenen in Nederland en daarbuiten, individuen en organisaties, zoeken een aanspreekpunt voor vragen rondom High Tech Crime of om een partner bij de bestrijding ervan. Het is derhalve van het grootste belang deze partijen een landelijk aanspreekpunt voor HTC te bieden.

Hierin dient te worden bezien:
- Hoe en door wie het best High Tech Crime kan worden tegengehouden en verstoord, door onder meer de ontwikkeling en realisatie van een notice and take down systeem.
- Hoe en met wie het best kan worden gekomen tot nationale en internationale samenwerking. Dit kan door middel van:
  - het voorzien in een makelaarsfunctie tussen verschillende partijen op basis van afspraken en protocollen;
  - sluiten van samenwerkingsovereenkomsten met partners, zowel publiek als privaat;
  - optreden als contactpunt voor internationale zusterorganisaties.
- Hoe en met wie het best kan worden gekomen tot een proces van informatie-uitwisseling. Door middel van:
  - een proces van informatie-uitwisseling;
  - ontwikkeling van een digitaal crisisbeheersplan;
  - inrichting Nationaal Meldpunt Cybercriminaliteit.
- Hoe en door wie het best detectering en monitoring kan plaatsvinden van nieuwe methoden van High Tech Crime. Te denken valt hierbij aan de implementatie van zogeheten Stormcenters bij ICT-knooppunten van vitale infrastructuren;
- Hoe en met wie het best kan worden gewerkt aan de ondersteuning en de voorbereiding van de opsporing. Hiervoor zijn de volgende producten voorzien:

- ontwikkelen en implementeren van kengetallen omtrent High Tech Crime opsporingsonderzoeken bij de politie;
- het gericht helpen van een slachtoffer van High Tech Crime bij het doen van een aangifte;
- het ondersteunen van een onderdeel van de politie bij het analyseren van een aangifte van High Tech Crime;

- het in samenwerking met andere partijen in een beschermde omgeving een specifieke zaak analyseren en hierover een gericht advies geven. Dit kan onder meer in de vorm van een algemeen advies, een zogeheten pre-weegdocument, een tegenhoudactie e.d.

Zoals ook al in hoofdstuk 2 aangegeven hebben de inzichten opgedaan in het NPAC project laten zien dat, mede met het oog op het op gang brengen en in-standhouden van de publiekprivate informatie-uitwisseling, een enkelvoudige loketfunctie niet de gewenste oplossingsrichting is. Vooral voor de participatie van het bedrijfsleven bij de bestrijding van cybercrime is een scheiding tussen preventie en herstel enerzijds en opsporing en vervolging anderzijds van cruciaal belang. In het gezamenlijke NPAC/NHTCC adviesontwerp 'nationale infrastructuur bestrijding cybercrime' wordt dan ook geadviseerd de loketfunctie op een gedifferentieerde wijze in te vullen zodat deze scheiding gerealiseerd wordt.

Voor wat betreft de opsporing van cybercrime zal het door het KLPD en het Landelijk Parket van het OM gezamenlijk in stand te houden expertisecentrum fungeren als aanspreekpunt voor regionale en bovenregionale opsporingsdiensten. Bovendien zal het expertisecentrum fungeren als aanspreekpunt voor buitenlandse opsporingsdiensten. Door deze twee taken vormt het expertisecentrum een belangrijke schakel in zowel de nationale als de internationale informatie-uitwisseling. Andere taken van het expertisecentrum zijn het ontwikkelen en implementeren van kengetallen omtrent High Tech Crime opsporingsonderzoeken bij de politie, het ondersteunen van onderdelen van de politie bij het analyseren van een aangifte van High Tech Crime en het in samenwerking met andere partijen analyseren van zaken en het hierover adviseren. Een taak van het expertisecentrum is ook het uitwisselen van informatie met andere partijen (visa versa) binnen de nationale infrastructuur cybercrime.

Een ander belangrijk aanspreekpunt, het Nationaal Meldpunt Cybercriminaliteit wordt op korte termijn gerealiseerd. Vooralsnog wordt dit ondergebracht bij het KLPD maar als onderdeel van het programma om te komen tot een nationale infrastructuur ter bestrijding van cybercrime zal worden onderzocht wat de meest wenselijke positionering is. Dit meldpunt zal een centrale rol spelen bij het verwerken van meldingen van burgers ten aanzien van kinderporno, aan terrorisme gerelateerde internet-uitingen (bijvoorbeeld haat-zaai sites), oplichting sites, e.d. Onderzocht zal worden of dit meldpunt ook een functie kan hebben ten aanzien van meldingen vanuit het bedrijfsleven of dat hier voor andere kanalen meer ge-

eigend zijn.

Een derde reeds bestaand aanspreekpunt is GOVCERT. Dit 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 die overheidsorganisaties ondersteund bij het invullen van hun informatiebeveiligingsverantwoordelijkheid. Daarnaast informeert en waarschuwt GOVCERT burgers en bedrijven over ICT-security en informatiebeveiliging (Waarschuwingsdienst).
Als onderdeel van het programma om te komen tot een nationale infrastructuur ter bestrijding van cybercrime zal worden onderzocht of de beperking van de taakstelling tot informatiebeveiliging door overheidsinstellingen niet moet worden losgelaten. Een eerste stap in die richting wordt gezet door het NTD-experiment dat in samenwerking met de Nederlandse Vereniging van Banken en de bancaire sector zal worden uitgevoerd.

6.4 Capaciteit opsporing

Realiseer voldoende capaciteit voor de opsporing en vervolging van High Tech criminelen. Aanbevolen wordt het onderwerp High Tech Crime als aandachtsgebied of resultaatsgebied te bestempelen bij de Nederlandse politie op landelijk niveau. Het is als zodanig te bezien als een integraal onderdeel van het pakket van maatregelen inzake High Tech Crime.

Naast het doen van opsporingsonderzoeken dient de daarbij ontwikkelde kennis en expertise ingebracht te worden voor de informatie-uitwisseling met andere partijen. Verder is het van belang een herkenbaar aanspreekpunt te hebben bij de politie voor deze problematiek.

Er komt een nieuw op te richten nationale opsporingsvoorziening. Deze opsporingsvoorziening zal zich gaan bezighouden met de opsporing van bijzondere en exclusieve vormen van cybercrime. Daarnaast zal het ook als een (politieel) expertisecentrum op het terrein van cybercrime gaan dienen. Het onderzoeksteam moet tegelijkertijd twee strafrechtelijke onderzoeken van gemiddelde grootte kunnen doen en daarnaast ook kleine rechtshulpverzoeken moeten kunnen afhandelen. Het regionaal en bovenregionaal niveau blijft verantwoordelijk voor de opsporing van (boven-)regionale vormen van cybercrime.

6.5 Naam National High Tech Crime Center

Aanbevolen wordt de naam National High Tech Crime Center terug te laten komen als naam bij de opvolgorganisaties. Deze naam heeft zowel bij de nationale als bij de internationale partners met name in het opsporingsveld inmiddels de

nodige bekendheid gekregen. Teneinde de continuïteit te waarborgen wordt aanbevolen deze naam hiervoor te blijven gebruiken.

In het gezamenlijke NPAC/NHTCC advies wordt voorgesteld het begrip NHTCC exclusief te reserveren voor de toekomstige nationale opsporingsvoorziening voor cybercrime binnen het KLPD. Deze voorziening is mede belast met de taak van informatie-uitwisseling met nationale en international partners.

Bijlage 1

Andere ontwikkelingen en projecten in relatie tot High Tech Crime

G8

Bron: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-243494&als[theme]=CC%20Home%20Page

The G8 (or "Group of Eight") is a multilateral group consisting of the world's major industrial democracies: Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States. The European Commission attends G8 meetings as an observer. The G8 address a wide range of international economic, political, and security issues.

Work on Transnational Organised Crime.
After the 1995 Summit in Halifax, Nova Scotia, a group of experts was brought together to look for better ways to fight international crime. In 1996, this group (later known as the "Lyon Group") produced Forty Recommendations to combat international crime that were endorsed by the G8 Heads of State at their Summit Meeting in Lyon in June 1996. "Subgroups" of the Lyon Group thereafter were formed to address specific crime-related issues (e.g., legal processes for evidence-sharing, high-tech crime, and immigrations fraud and human trafficking). In December 1997, U.S. Attorney General Janet Reno hosted the first-ever meeting of her counterparts from the G8 countries and the Ministers issued their first joint Communiqué which endorsed the work of the Lyon group. The last three Presidencies of the G8 have hosted meetings of Justice and Home Affairs ministers. The Home Secretary will host a Justice and Home Affairs Ministerial meeting in Sheffield 15-17 June.

G8 Transnational crime and Counter-terror objectives in 2005
The 2005 objectives combine work on the inherited agenda and a number of new initiatives. There are nearly 100 separate projects. The key areas of work are:

- As lead country for counter-narcotics work in Afghanistan, the UK will continue to seek co-ordination of the G8 support for this work.
- The completion of several initiatives to enhance international travel security.
- International co-operation in combating immigration crime, with an emphasis on document fraud.
- International law enforcement co-operation, focusing on child protection, the expanded use of DNA and the international illegal trade in firearms.
- International co-operation in combating high-tech crime.

- Shared assessment of the threat from international terrorism and co-operation to counter the treat.
- The reinforcement of the principles of judicial co-operation and mutual legal assistance in the investigation and prosecution of transnational organized crime and terrorism.

EU

Bron: http://www.euractiv.com/Article?tcmuri=tcm:29-117465-16&type=LinksDossier

Electronic communication networks and information systems are now an essential part of the daily lives of EU citizens and are fundamental to the success of the EU economy. Networks and information systems are converging and becoming increasingly interconnected. Despite the many and obvious benefits of this development, it has also brought with it the worrying threat of intentional attacks against information systems.

At the Lisbon European Council of March 2000, the European Council stressed the importance of the transition to a competitive, dynamic and knowledge-based economy. The eEurope Action Plan which came out of this, includes actions to enhance network security and the establishment of a coordinated and coherent approach to cybercrime. As part of the Commission's contribution to this mandate on cybercrime, it published the Communication 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime' on 26 January 2001.

On 23 April 2002, the Commission adopted a draft Council framework Decision on "attacks against information systems". The proposal addresses new forms of criminal activity against information systems, such as hacking, viruses and denial of service attacks (DoS). Approval is still pending on this proposal which has to be in line with the Council of Europe's Convention on Cybercrime .

On year on, the Commission proposed to set up a European Network Security Agency which will be fully staffed and operational in the course of 2005. ENISA has a budget of ¬ 34.3 million for five years and will mainly collect and analyze data on security incidents in Europe and report to the Commission.

Issues:
Types of attacks could be:
- Unauthorized access to information systems;
- Disruption of information systems (denial of service attack);
- Execution of malicious software that modifies or destroys data;
- Interception of communications;
- Malicious misrepresentation ('identity theft').

Cyber criminals can launch an attack from anywhere in the world, to anywhere in the world, at any time. This means new, unexpected forms of attacks could occur. This makes the need for effective action to deal with threats to the authenticity, integrity, confidentiality and availability of information systems and networks all the more urgent and at the same time all the more complex.

The ultimate challenge is to find the right policy mix to find the best balance between cybercrime and cyber surveillance, two phenomena capable of hindering the free flow of information.

Positions:
The Union of Industrial and Employers' Confederations of Europe (UNICE) welcomes initiatives aiming at the creation of a safer information society by improving the security of information infrastructures and combating computer-related crime. UNICE states the Commission's proposal on cybercrime will help the Member States criminal laws to provide a "common response in an area of criminal activity which, by nature, knows no borders." It adds that "harmonization of laws should improve police and judicial cooperation: if the same activity is considered an offence in all 15 Member States, criminals will no longer be able to find safe havens in EU Member States."

The International Chamber of Commerce (ICC) states that business "needs effective law enforcement and judicial networks to ensure that cyberspace does not become a criminal's charter."

Raad van Europa

Bron: http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/Cybercrime/_Summary.asp#TopOfPage

The rapid growth of the new information technologies and their use for criminal purposes have created serious problems, which cannot easily be solved, using traditional international co-operation methods. The Committee of Experts on Crime in Cyberspace (PC-CY) was set up to deal with cybercrime (computer crime) and criminal procedure problems linked with information technology. It was given the task of preparing a legally binding instrument.

The Committee has completed its work at the end of the year 2000 and worked in close coordination with the G-8 and other international bodies on a final draft Convention on Cybercrime.

The Convention on cybercrime was opened for signature on 23 November 2001 in Budapest, on the occasion of an international conference organized in Budapest on 22 and 23 November 2001. 30 states signed the Convention : 26 Council of

Europe member States and 4 non-member States which had helped with the drafting.

ENISA

Bron: http://europa.eu.int/agencies/enisa/index_en.htm

The Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 (OJ L 77, 13 March 2004) establishing the European Network and Information Security Agency sets the frame and paves the way for the work of the Agency.

In this context, ENISA's mission is to assist the Community in ensuring particularly high levels of network and information security. The Agency will therefore contribute to the development of a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organizations of the European Union, consequently contributing to the smooth functioning of the internal market.

The Agency will assist the Commission, the Member States and the business community in meeting the requirements of network and information security, including those of present and future Community legislation.

ENISA will ultimately serve as a centre of expertise for both Member States and EU Institutions to seek advice on matters related to network and information security.

In order to ensure the fulfillment of its objectives, the Agency's tasks will be focused on:
- Collecting and analyzing data on security incidents and emerging risks;
- Cooperating with different players notably through the establishment of public / private partnerships with industry operating at EU and / or global levels;
- Raising awareness and promoting risk assessment methods and best practices for interoperable risk management solutions;
- Tracking the development of standards for products and services on Network and Information Society.

ENISA will have its seat in Heraklion (Greece).

Ministerie van Economische Zaken - Nederland

KWINT

Bron: http://www.ez.nl/content.jsp?objectid=31303

Internetgebruik is een integraal onderdeel van ons maatschappelijk en economisch verkeer geworden en speelt een nog steeds groeiende rol. Met het goed functioneren van internet zijn daarom grote maatschappelijke en economische

belangen gemoeid. Incidenten als het "I love you"-virus en het saboteren van websites (door platleggen of wijzigen van de inhoud) laten zien dat de veiligheid en betrouwbaarheid van dit medium de nodige zwakke plekken vertonen. De gevolgen van dergelijke incidenten worden steeds groter. In 2001 is de kabinetsnota Kwetsbaarheid op Internet (KWINT) aangeboden aan de Tweede Kamer, waarin een aantal actielijnen is benoemd om de betrouwbaarheid van internet te vergroten. In 2002 is in een aantal publiek-private werkgroepen gewerkt aan deze actielijnen.

ECP.nl

Bron: http://www.ecp.nl/bestuur.php

De ontwikkeling van Nederland als informatiemaatschappij is cruciaal voor zowel de arbeidsproductiviteit als de sociale cohesie in de maatschappij. De toepassing van ICT biedt vele mogelijkheden en kansen voor bedrijfsleven en overheid maar ook voor de consument, de burger, en de patiënt. Toch worden deze mogelijkheden nog onvoldoende benut om als Nederland hiermee voorop te kunnen lopen. ECP.NL wil hier iets aan doen en zet zich als onafhankelijk platform in voor de ontwikkeling van Nederland als informatiemaatschappij: eNederland.

Binnen ECP.NL werken publieke en private instellingen samen door kennis op het gebied van de ontwikkeling en toepassing van ICT te bundelen en te delen. Zij doen dit in de vorm van projecten en werkgroepen waarin actuele thema's worden opgepakt. Door deze sectoroverschrijdende samenwerking helpt ECP.NL de (internationale) concurrentiepositie van Nederland te behouden en te verbeteren.

ECP.NL is in januari 1998 opgericht door het Ministerie van Economische Zaken en VNO-NCW. In zeven jaar tijd is ECP.NL uitgegroeid tot het platform voor eNederland met 150 deelnemende bedrijven en instellingen (overheid, intermediairen, bedrijfsleven, onderwijs).

Activiteiten:
Onder begeleiding van de medewerkers van ECP.NL (14 in totaal) wordt kennis gebundeld in kennisgroepen waarin deelnemers aan het platform (kunnen) participeren. Zo wordt er gewerkt aan projecten op het gebied van consumentenvertrouwen, wet- en regelgeving (maar ook zelfregulering), veiligheid van ICT-toepassingen, standaarden en (internationale) trends en ontwikkelingen. De onderwerpen die binnen ECP.NL worden opgepakt passen binnen deze gebieden en lopen uiteen van elektronisch betalen en spam, naar ebXML, veilig internetten voor kinderen en opkomende nieuwe technologieën als RFID en ambient intelligence.

Rapport: Rethinking the European ICT agenda - Ten ICT-breakthroughs for reaching Lisbon goals

Bron: http://www.pwc.com/Extweb/pwcpublications.nsf/docid/EC6DE73A846581CE80256EFD002E41FB

Het ministerie van Economische Zaken heeft op 25 augustus 2004 het door PricewaterhouseCoopers opgestelde rapport 'Rethinking the European ICT Agenda' openbaar gemaakt. In het rapport worden tien doorbraken voor vernieuwing van het Europese ICT-beleid gepresenteerd. Deze doorbraken moeten een nieuwe impuls geven aan de Lissabon-doelstelling van de Europese Unie om in 2010 de meest concurrerende economie ter wereld te zijn. Minister Brinkhorst heeft het rapport naar de voorzitter van de Tweede Kamer gestuurd.

De conclusies van het onderzoek zijn gebaseerd op een uitvoerige deskresearch en bijna 100 interviews met thought leaders in het ICT-veld, waaronder veel PwC-cliënten. Tevens is de Europese ICT-sector en het Europese ICT-beleid vergeleken met die van vijf referentielanden: de Verenigde Staten, India, China, Zuid Korea en Japan.

Bron: http://www.pwc.com/Extweb/pwcpublications.nsf/docid/EC6DE73A846581CE80256EFD002E41FB/$file/pwc_rethinking_european_ict_agenda.pdf

Breakthrough 9: Enforce real solutions for consumer confidence and security:

365 The great benefits of the Internet also entail a 'darker side', e.g. the ability to spread viruses, spam, pornography, privacy violation and cybercrime. These threats affect consumer (private-business-public) trust and confidence and hence form a barrier to the development of the Information Society in general and the content market specifically (see also breakthrough 4). Moreover, they seriously can threaten the proper functioning of the economy. consumer trust and confidence are severely affected and need to be addressed.

A crucial condition for a broad deployment and use of ICT by business and consumers is user confidence. Therefore the EU needs to enforce structural solutions for viruses and spam by creating liabilities, give priority to cybercrime within law enforcement and ensure the availability of critical infrastructures.

Bescherming vitale infrastructuur:

Bron: http://www.ez.nl/content.jsp?objectid=31279

De Tweede Kamer heeft in mei 2001 de regering verzocht een sectoroverschrijdend plan van aanpak inzake de bescherming van vitale (informatie-)infrastructuur op te stellen. Voordat tot uitvoering van deze motie kon worden overgegaan, volgden de dramatische gebeurtenissen op 11 september 2001 in de Verenigde Staten. Deze gebeurtenissen waren mede na de aanname van de Motie Wijn, aanleiding voor de Nederlandse Overheid om de bescherming van de vitale infrastructuur breed aan te pakken en dit in te bedden in het Actieplan Terrorismebestrijding en Veiligheid. Actiepunt 10 van dit plan betreft de bescherming van vitale infrastructuren.

Voor de aanpak en uitvoering van dit actiepunt is in april 2002 het project Bescherming Vitale Infrastructuur (BVI) ingesteld. Het betreft een grootschalig project waarbinnen onder coördinatie van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) nauw wordt samengewerkt met alle departementen, het bedrijfsleven en de medeoverheden. Het project BVI zal alle maatschappelijke vitale sectoren bezien en de onderlinge afhankelijkheden en ketens in kaart brengen, de kwetsbaarheden en de beschermingsmaatregelen inventariseren, om zo eventueel te kunnen besluiten tot het treffen van (aanvullende) maatregelen ter minimalisering van risico's.

Ministerie van Binnenlandse Zaken - Nederland

GOVCERT.NL

Bron: http://www.govcert.nl/render.html?it=36

Veiligheid is voor de overheid een belangrijk thema. Dat beperkt zich niet tot de fysieke ruimte. Het vergroten van de veiligheid in de virtuele wereld is evenzeer een verantwoordelijkheid van de overheid. GOVCERT.NL komt daaruit voort.

In het "Plan van aanpak virusproblematiek en informatiebeveiliging overheid" en de beleidsnota "Kwetsbaarheid op Internet" kreeg het oprichten van een Computer Emergency Response Team van de Nederlandse overheid hoge prioriteit.

GOVCERT.NL is een initiatief van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en sinds 5 juni 2002 officieel actief, toen nog onder de naam CERT-RO. Omdat zij inmiddels niet alleen de rijksoverheid (waar 'RO' voor stond) meer bedienen, is de naam veranderd.

GOVCERT.NL is ondergebracht bij ICTU, de ICT-uitvoeringsorganisatie van de overheid.

Ook burgers en het kleinbedrijf maken tegenwoordig gebruik van de Waarschuwingsdienst. De Waarschuwingsdienst waarschuwt computergebruikers thuis en het kleinbedrijf tegen virusuitbraken en lekken in software via www.waarschuwingsdienst.nl en gratis e-mail en SMS alerts.

Bescherming vitale infrastructuur

Bron: http://www.minbzk.nl/veiligheid/nationaal/inspringthema_s/bescherming_vitale

De dramatische gebeurtenissen van 11 september 2001 in de Verenigde Staten bevestigden nadrukkelijk hoe afhankelijk en kwetsbaar de infrastructuur van overheid, bedrijfsleven en (internationale) samenleving is. Niet alleen de aanslagen in de VS, maar ook andere gebeurtenissen zoals de millenniumovergang illustreren deze kwetsbaarheid.

Bij de bescherming van vitale belangen in Nederland gaat het niet alleen om de bescherming tegen terroristische aanslagen, maar ook tegen bijvoorbeeld natuurgeweld, organisatorische en technische gebreken. Deze brede benadering doet recht aan de inspanningen die het bedrijfsleven en de overheden al ver voor de 11de september 2001 hebben geleverd.

Doelstelling:
De regering heeft op verzoek van de Tweede Kamer in april 2002 het project Bescherming Vitale Infrastructuur ingesteld. Binnen dit project werken departementen, het bedrijfsleven en de medeoverheden nauw samen. De doelstelling van dit project is het behalen van de volgende eindresultaten:

2. De ontwikkeling en instandhouding van een samenhangend pakket van maatregelen ter bescherming van de vitale infrastructuur van overheid en bedrijfsleven, waaronder ICT, en;
3. De verankering van deze maatregelen in de normale bedrijfsvoering .

Deze opdracht is vermeld als actiepunt 10 van het Actieplan Terrorismebestrijding en Veiligheid en houdt verband met de motie Wijn (TK, 2000-2001, 26 643, nr. 20). In deze motie wordt de regering verzocht een sectoroverschrijdend plan van aanpak voor de bescherming van vitale infrastructuur op te stellen.

In juli 2004 is de laatste projectmatige rapportage aan de Tweede Kamer aangeboden. Hierin wordt een overzicht gegeven van de gehanteerde aanpak en de tot nu toe behaalde resultaten. Ook geeft de rapportage aan welke resultaten nog niet zijn behaald en via welke weg deze in de nabije toekomst alsnog worden bereikt.

Per september 2004 is de projectorganisatie van vitaal ontbonden. Dit betekent overigens niet dat alle beleidsactiviteiten worden stopgezet. Het monitoren en actualiseren van de inzichten in de kwetsbaarheid en in de effectiviteit van de maatregelen blijft ook na september noodzakelijk. Met alle betrokkenen binnen de overheid en bedrijfsleven zijn daarom afspraken gemaakt om de bescherming van de vitale infrastructuur structureel voort te zetten. Per september zal het beleidsdossier Vitaal structureel zijn belegd bij alle deelnemende ministeries.

Nationaal Platform Criminaliteitsbeheersing

Bron: http://www.justitie.nl/themas/meer/NPC/index.asp

Het Nationaal Platform Criminaliteitsbeheersing (NPC) is een publiekprivaat samenwerkingsverband. Overheid en bedrijfsleven richten zich in het NPC samen op de aanpak van criminaliteitvormen waarvan het bedrijfsleven slachtoffer is.

Het Platform, onder voorzitterschap van de minister van Justitie, komt 2 à 3 keer per jaar bijeen. Tijdens deze bijeenkomsten wisselen vertegenwoordigers van de overheid en het bedrijfsleven op strategisch niveau van gedachten. Daarbij staat zowel de aanpak van huidige criminaliteitsproblemen als de koers voor de langere termijn centraal.

Alle relevante departementen, de politie, het openbaar ministerie en de VNG zijn in het platform vertegenwoordigd. Namens het bedrijfsleven maken werkgeversorganisaties deel uit van het Platform en is een aantal branches vertegenwoordigd.

Bron: http://www.ez.nl/content.jsp?objectid=31308

Op 15 november 2004 heeft de Raad van Advies van het Nationaal Platform Criminaliteitsbeheersing ingestemd met het plan van aanpak van het NPC-project Aanpak Cybercrime (NPAC). In dit project werken vele publieke en private partijen uit het bedrijfsleven gezamenlijk aan:

- het verminderen van de kwetsbaarheid van overheid en bedrijfsleven voor cybercrime;
- het verhogen van het bewustzijn voor de gevolgen van cybcercrime;
- het organiseren van preventieve maatregelen;
- het verbeteren van het collectieve reactievermogen.

Het project loopt tot november 2006. Al tijdens de looptijd van het project zullen producten worden opgeleverd die bijdragen aan bovenstaande doelstellingen. Bij de uitvoering van het project zullen (naast de partijen die zitting hebben in de projectgroep) ook vele experts worden betrokken.

De activiteiten van het NPAC zijn onderdeel van het actieplan veilig ondernemen (deel 2)

Bron: http://www.veiligheidsprogramma.nl/default.asp?projectID=15&groepID=11&template=overig/detailProject.htm

Het Actieplan veilig ondernemen is tot stand gekomen onder de vlag van het Nationaal Platform Criminaliteitsbeheersing (NPC).

Dit actieplan bevat concrete maatregelen en acties om in vier jaar tijd de criminaliteit tegen het bedrijfsleven met 20% terug te dringen.
In het actieplan zijn voor de periode 2004-2008 tien projecten vastgelegd met acties voor het tegengaan van criminaliteit gericht tegen het bedrijfsleven. Zo zijn er onder andere projecten gestart voor de:

- verbetering van aangifte-, meldings- en terugkoppelingsprocedures;
- verbetering van het protocol voor het doorgeven van alarmmeldingen door Particuliere Alarmcentrales aan politiemeldkamers, zodat efficiënter kan worden opgetreden tegen criminaliteit;
- aanpak van freeriders;

- verbetering van beveiliging van diefstalstalgevoelige producten.

Daarnaast zijn er projecten voor de transportsector, de uitgaansbranche, de detailhandel, de juweliersbranche, de interne criminaliteit en de aanpak van urgente bedrijvenlocaties.

Actieplan veilig ondernemen - deel 2

De overheid en het bedrijfsleven geven een extra impuls aan de veiligheid van het bedrijfsleven. Daarom werd op donderdag 12 mei 2005 het Actieplan Veilig Ondernemen deel 2 ondertekend.
Het nieuwe actieplan bevat, ten opzichte van het eerste plan, vijf nieuwe projecten en drie versterkingen van eerdere projecten voor de periode 2005-2008. Met het actieplan deel 2 wordt tegemoet gekomen aan een aantal lang gekoesterde wensen van het bedrijfsleven. Zo wordt in het project 'Tegenhouden van Georganiseerde Criminaliteit' ingezet op de aanpak van mobiele bendes waar vooral de detailhandel slachtoffer van is. Daarnaast komt het project 'Heling' tegemoet aan de signalen van het bedrijfsleven over de vrije verkrijgbaarheid van bij hen gestolen goederen.

Bron: http://www.veiligheidsprogramma.nl/bestand.asp?id=389

PROJECT 13 : CYBER CRIME

Steeds meer transacties en onderdelen van het economische en maatschappelijke leven vinden plaats via het internet en andere vormen van online dienstverlening. Steeds vaker krijgt deze virtuele wereld te maken met criminaliteit en schade als gevolg daarvan. Voor een deel valt deze criminaliteit te voorkomen door goede beveiligingsmaatregelen. Om dit bekend te maken en de beveiliging te verbeteren, en zo cyber crime preventief aan te pakken, bestaan al diverse initiatieven zoals het publiekprivate samenwerkingsprogramma Kwetsbaarheid op Internet (KWINT) en de campagne Surf op Safe. Hierin worden kennis, methoden en hulpmiddelen ontwikkeld en verspreid. Daarnaast is de Waarschuwingsdienst ingesteld om onder andere het bedrijfsleven te informeren over actuele kwetsbaarheden en dreigingen op het internet. Ook lopen er verschillende initiatieven om cyber crime repressief aan te pakken. Ondanks al deze initiatieven kent de aanpak van cyber crime diverse obstakels, namelijk: - door onduidelijke statistieken en een geringe aangiftebereidheid is de omvang van het probleem onhelder - vaak wordt cyber crime niet als zodanig geregistreerd maar als diefstal van gegevens, fraude, afpersing of een ander 'traditioneel' vergrijp; - het opsporen van cyber crime vereist kennis die soms onvoldoende beschikbaar is in het opsporingsapparaat; - er bestaat onduidelijkheid in het opsporingsapparaat met betrekking tot het niveau waarop de verschillende verschijningsvormen van cyber crime moeten worden aangepakt - regionaal, bovenregionaal of landelijk; - er is sprake van een versnippering van initiatieven ter bestrijding van cyber crime; - alle bovenstaande aspecten gezamenlijk beperken de mogelijkheid tot juiste prio-

riteitstelling binnen het opsporingsapparaat. Dit belemmert een daadkrachtige en gecoördineerde aanpak van cyber crime.

Door de projectgroep cyber crime is al een begrippenlijst en een overzicht van betrokken partijen samengesteld. In aanvulling daarop worden de volgende acties ter hand genomen: Inventariseren krachtenveld Actie 1 op 1 juni 2005 is een overzicht gereed van 'wie doet wat, waarom, waartoe en met wie in relatie tot cyber crime'. Actie 2 op 1 juni 2005 is een 'virtuele organisatie' gereed om bij te dragen aan de preventie en bestrijding van cyber crime. Inventariseren trends Actie 3 op 1 november 2005 is een typologie/classificatie van verschijningsvormen van cyber crime gereed. Actie 4 op 1 november 2005 is een overzicht van trends en ontwikkelingen gereed. Actie 5 op 1 november 2005 is een model gereed hoe om te gaan met (nieuwe) verschijningsvormen. Bevorderen van proactie en preventie Actie 6 uiterlijk op 1 april 2006 is een experiment afgerond met een dienst die bij ondernemers en overheden de informatiebeveiliging toetst en adviseert in ruil voor het gebruik van verkregen informatie. Actie 7 met ingang van 1 juli 2006 worden handleidingen en protocollen voor ondernemingen en overheden beschikbaar gesteld. Bevorderen van preparatie en repressie Actie 8 uiterlijk 1 oktober 2006 is er een handhavingarrangement opgesteld met daarin de inspanningen van alle betrokken partijen op het gebied van bijvoorbeeld melding en aangifte, verzamelen en delen van informatie, preventieve inspanningen, repressieve inspanningen.

Landelijk Project Digitale Opsporing

Bron: http://www.ejure.nl/mode=display/downloads/dossier_id=65/id=201/KVR22675.pdf

De Raad van Hoofdcommissarissen is een Landelijk Project Digitaal Opsporen gestart dat verbetering in de situatie van het digitaal opsporen moet brengen. Uitgangspunt daarbij is een onderscheid tussen tactisch uitvoerend en technisch ondersteunend opsporingswerk.
Het uitvoeren van werkzaamheden op het gebied van digitaal rechercheren dient in de visie van de Raad generiek te zijn: iedere opsporingsambtenaar (recherche of anderszins) moet worden toegerust om zijn of haar werk te kunnen doen, gegeven de digitalisering van de samenleving. Dat betekent een verbreding van de competenties van alle opsporingsambtenaren. Daarnaast is naar de mening van de Raad op het gebied van de technische ondersteuning een professionaliseringsslag nodig.
Bovenstaande visie heeft tot gevolg dat een aantal maatregelen zal moeten worden genomen, waarvan de belangrijkste zijn: het heroverwegen van het opleidingsaanbod en het heroverwegen van de gehanteerde structuur waarbinnen deskundigheid is georganiseerd. Er is voorzien in een opleidingstraject van alle zittende rechercheurs. Dit zal worden gerealiseerd in een periode van 4 jaar: van 2005 tot en met 2008. Tegelijkertijd zal de organisatie van de digitale recherche worden gewijzigd. De technische kennis wordt verdiept en samengevoegd met de

forensisch technische expertise binnen de politie. De tactische kennis wordt door middel van de eerdergenoemde opleidingen verbreed en ingebed in de bestaande tactische opsporingsteams op regionaal, bovenregionaal en landelijk niveau.

Nationaal Dreigingsbeeld

Bron: http://www.openbaarministerie.nl/lp/documents/2004-19%20Nationaal%20dreigingsbeeld.pdf en http://www.ejure.nl/exturls/dossier_id=50/id=657/show.html

Het Nationaal Dreigingsbeeld zware of georganiseerde criminaliteit is in opdracht van de ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties opgesteld door de dienst Nationale Recherche Informatie bij het KLPD.

Dit dreigingsbeeld omvat een overzicht van de belangrijkste verschijnselen van zware georganiseerde criminaliteit voor de komende vijf jaar. Op basis van het Nationaal dreigingsbeeld en op basis van adviezen van het College van procureurs-generaal en de Raad van Hoofdcommissarissen, worden de speerpunten voor de opsporingsdiensten, waaronder de NR en de BR, bepaald.

In het dreigingsbeeld wordt aandacht besteed aan de volgende ICT-gerelateerde misdrijven:
- 3.2.6. ICT-piraterij (schending van auteursrechten);
- 3.2.7. Internetfraude, zoals Nigerian scam fraude, identiteitsdiefstal, creditcard fraude en phishing;
- 3.2.10. Afpersing door middel van een aanval op ICT-infrastructuren (dDOS-aanvallen);
- 3.2.14. Telecomfraude (PABX-fraude en 0900-fraude).

Ook de volgende hoofdstukken zijn interessant:
- 2.4 Het gebruik van informatie en communicatietechnologie;
- 3.3.12 Het gebruik van internet als marktplaats.

Nota 'Politie in ontwikkeling - Visie op de politiefunctie'

Bron: http://www.politie.nl/Nieuws/Images/32_143587.pdf

De nota Politie in ontwikkeling is bedoeld om richting te geven aan toekomstige ontwikkelingen van het politievak. Het document moet een duidelijke boodschap overbrengen aan de omgeving en aan de eigen organisatie. Hiermee worden de meest concrete en dringende problemen waar het gaat om de politiefunctie en de politieorganisatie hanteerbaar gemaakt voor de politie zelf en voor burgers, gezagsdragers, bestuurders, politiek en partners in veiligheid. Onderdeel daarvan is het aanbrengen van ordening in een veelheid aan ideeën en visies op deelterreinen van het politiewerk om op die manier samenhangen duidelijk te maken. On-

derdeel is ook het richting geven aan de bedrijfsarchitectuur die door de politie wordt ontwikkeld, in het bijzonder het processenmodel van de Nederlandse politie.

Signaleren en adviseren is een expliciete taak van de Nederlandse politie Met het oog op haar wettelijke taakopdracht vervult de Nederlandse politie verschillende functies. Ze wil deze in samenhang inhoud blijven geven ten gunste van maximale legitimiteit, doeltreffendheid en doelmatigheid. Binnen deze brede, samenhangende taakuitvoering kunnen de volgende taken worden onderscheiden: handhaving, opsporing, noodhulpverlening, signaleren en adviseren. De taak tot signaleren en adviseren vloeit voort uit de drie in de Politiewet 1993 genoemde taken van de politie: handhaving, opsporing en noodhulp. Signaleren en adviseren impliceert dat de politie aangeeft waar bestuur, OM en partners in haar optiek een bijdrage zouden kunnen en moeten leveren aan het reduceren van onveiligheid. De politie wil dan ook in haar relatie tot deze partijen geen passieve speler zijn, maar rekent het tot haar verantwoordelijkheid problemen op het gebied van onveiligheid te signaleren en daarover te adviseren, ook in internationaal verband.

Binnen het gebiedsgebonden werken vormt een nodale oriëntatie een noodzakelijke aanvulling op de lokale oriëntatie De Nederlandse politie is traditioneel sterk georiënteerd op plaatsen (gebieden, territoir). Sociale processen worden echter steeds meer bepaald door stromen van mensen, goederen, geld en vooral informatie. Dit geldt ook voor bijvoorbeeld criminaliteit en terreur. Dit stromenland wordt ook space of flows genoemd. Space of flows wint aan betekenis naast de zogenaamde space of places. Met space of flows wordt bedoeld de gebiedsgebonden, fysieke, leefomgeving met belangrijke plaatsen, zoals de wijk, de stad, de 'marktplaats' en andere ontmoetingsplaatsen. De wisselwerking tussen de leefruimte en stromenland is in toenemende mate bepalend voor het karakter van onveiligheid, en biedt tegelijkertijd aanknopingspunten voor de bestrijding daarvan.

Dit aanknopingspunt ziet de politie in de infrastructuur, waarover de stromen zich bewegen. Deze infrastructuur kan worden onderverdeeld in verschillende niveaus:
- intrastedelijke infrastructuur (bijvoorbeeld doorgaande routes in de stad);
- interstedelijke infrastructuur (weg-, water- en railverbindingen);
- internationale infrastructuur (het Europees verbindingennet, internationaal luchtverkeer, havens);
- virtuele infrastructuur (bijvoorbeeld computernetwerken).

Bijlage 2

Beschrijving organisaties in netwerkvisual

Organisatie	**Volledige naam**	**1. Korte beschrijving van de organisatie. 2. Soort relatie**
AIVD	Algemene Inlichtingen en VeiligheidsDienst	1. waarschuwen voor bedreigingen voor de veiligheid van Nederland en ondersteunen bij het nemen van beveiligingsmaatregelen 2. informatie-uitwisseling
AFM	Autoriteit Financiële Markten	1. heeft buitengewoon opsporingsambtenaren in dienst. Doen onderzoek naar aanleiding van het vermoeden dat (een poging tot) een strafbaar feit is gepleegd of gepleegd zal worden 2. informatie-uitwisseling
AHTCC	Australian High Tech Crime Center	1. geeft voorlichting over en biedt preventie ten aanzien van High Tech Crime door middel van samenwerking met wetsuitvoerders, overheidsinstellingen, bedrijven en private organisaties. Aangezien zij inzien dat High Tech Crime nooit volledig tegengegaan kan worden bieden zij ook hulp bij problemen. 2. kennisuitwisseling, omdat het AHTCC een vergelijkbare doelstelling heeft wordt veel kennis en ervaring uitgewisseld.
Bedrijfsleven	Bedrijfsleven	1. willen High Tech Crime tegengaan. Ze hebben daarvoor vaak specialisten in huis. Tevens schakelen zij het NHTCC in voor hulp in geval van High Tech Crime. 2. vertrouwensrelatie opbouwen zodat informatie kan worden uitgewisseld
BOTNET Taskforce	BOTNET Taskforce	1. is gespecialiseerd in het bestrijden van botnets. Een bot is een programma dat zelfstandig geautomatiseerd werk kan uitvoeren. Een persoon kan een botnet vanuit een centraal punt op het internet besturen. 2. kennisuitwisseling (o.a. bijwonen vergaderingen)
BUZA	Ministerie van buitenlandse zaken	1. draagt door middel van de Organisatie voor Veiligheid en Samenwerking in Europa bij aan de bestrijding van High Tech Crime (zie:OVSE) 2. relatie moet nog worden opgebouwd

Organisatie	**Volledige naam**	**1. Korte beschrijving van de organisatie. 2. Soort relatie**
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	1. draagt door middel van de Korps Landelijke Politie Diensten, Algemene Inlichtingen en Veiligheids-Dienst en GOVCERT.NL.nl, bij aan de bestrijding van High Tech Crime (zie KLPD, AIVD en GOVCERT.NL). 2. opdrachtgever
CERT's	Computer Emergency Response Teams (zowel in binnen- als buitenland)	1. houden zich bezig met preventie en afhandeling van ICT-gerelateerde veiligheidsincidenten. Zij vormen een belangrijke bron voor informatie-uitwisseling. 2. (inter)nationale informatie-uitwisseling met overheids- en private CERT's
DNB	De Nederlandse Bank	1. is betrokken bij overheidsinitiatieven rond High Tech Crime. Dit betreft o.a. activiteiten in het kader van het Nationaal Platform Criminaliteitsbeheersing en het project High Tech Crime (zie NPC). 2. informatie-uitwisseling
ECP.NL	E-commerce Platform	1. levert een bijdrage aan de ontwikkeling van eNederland, door een platform te bieden waar deelnemende bedrijven en instellingen worden gestimuleerd om kennis te delen op het gebied van de ontwikkeling en toepassing van ICT. 2. kennisuitwisseling over HTC en ICT-trends en ontwikkelingen
ENISA	Europees Agentschap voor netwerk- en infobeveiliging	1. helpt bij de totstandbrenging van een hoog niveau van netwerk- en informatiebeveiliging. Bevordert de ontwikkeling van een cultuur van netwerk- en informatiebeveiliging ten behoeve van de burgers, consumenten, bedrijven en organisaties uit de publieke sector in de Europese Unie. 2. relatie moet worden opgebouwd
EPN.NET	Platform voor de Informatiesamenleving	1. zet zich in voor het verbeteren van de kwaliteit van de samenleving met behulp van ICT. Daarbij probeert EPN altijd een paar jaar vooruit te denken. De stichting verricht onderzoek, publiceert, ondersteunt voorbeeldprojecten en initiatieven en organiseert bijeenkomsten over thema's rond ICT, toekomst en samenleving. 2. kennisuitwisseling
Europol	The European Police Office	1. hebben als doel straffen ten aanzien van aanvallen op informatiesystemen geproportioneerd, effectief en afwerend te laten zijn in alle lidstaten. 2. informatie-uitwisseling

Organisatie	**Volledige naam**	**1. Korte beschrijving van de organisatie. 2. Soort relatie**
EZ	Ministerie van Economische zaken	1. draagt bij - door middel van de Onafhankelijke Post en Telecommunicatie Autoriteit en E-commerce Platform - aan de bestrijding van High Tech Crime. Tevens levert het door middel van 'kwetsbaarheid op het internet (KWINT) een bijdrage aan de ontwikkeling van eNederland. 2. opdrachtgever
GOVCERT.NL	Governmental Computer Emergency Response Team	1. is het Computer Emergency Response Team van de Nederlandse overheid. GOVCERT.NL ondersteunt de overheid bij preventie en afhandeling van ICT-gerelateerde veiligheidsincidenten. GOVCERT.NL. is voor de overheid het centrale meldpunt voor veiligheidsincidenten met betrekking tot ICT, zoals computervirussen, hacking en fouten in applicaties en hardware, verstrekt informatie en ondersteunt bij preventie van en reactie op veiligheidsincidenten. 2. intensieve relatie met betrekking tot HTC informatie-uitwisseling. Programma managers hebben wekelijks contact
Interpol	International Criminal Police Organization	1. draagt bij aan de bestrijding van High Tech Crime door middel van The Financial & High Tech Crime afdeling. 2. informatie-uitwisseling
ISP's	Internet Service Providers	1. hebben een eigen verantwoordelijkheid bij de bestrijding van High Tech Crime op het internet. 2. informatie-uitwisseling
ISPO	Internet Service Provider Overleg	De ISPO kerngroep bestaat uit grote, kleine, zakelijke-, consumenten-, dsl-en kabel-isp's. De leden van de kerngroep zijn: BIT, Demon, Luna.nl, KPN Internet, UPC, Tiscali, Wanadoo Nederland, XS4ALL Internet BV. ISPO preten-deert niet namens alle ISP's van Nederland een standpunt uit te dragen. De activiteiten van ISPO worden gedragen door een groep ISP's van steeds wisselende samenstelling. Deze ISP's hebben gemeen dat zij zich zorgen maken over (overheids)plannen die het internet en daarmee internetproviders en hun klanten raken. 2. informatie-uitwisseling
JZ	Ministerie van Justitie	1. Onder de verantwoordelijkheid van dit ministerie vallen het Landelijk Parket en het Nederlands Forensisch Instituut (zie LP, NFI). 2. opdrachtgever en intensieve informatie-uitwisseling

Organisatie	**Volledige naam**	**1. Korte beschrijving van de organisatie.** **2. Soort relatie**
KLPD	Korps Landelijke Politie Diensten	1. is door het project HTC met de ministeries van Justitie, Binnenlandse Zaken en Koninkrijksrelaties, Economische Zaken gezamenlijk aan de slag gegaan om ICT misbruik tegen te gaan. Binnen de KLPD is ook de digitale recherche actief. 2. opdrachtgever, voorzitter van de Stuurgroep en intensieve informatie-uitwisseling
KMAR	Koninklijke Marechaussee	1. heeft het voornemen samen met het NHTCC in eerste instantie High Tech Crime op de luchthaven Schiphol aan te pakken. 2. relatie moet worden geïntensiveerd
LP	Landelijk Parket	1. houdt zich bezig met de aanpak van internationale vormen van georganiseerde misdaad. 2. intensieve informatie-uitwisseling
LPDO	Landelijk Project Digitaal Opsporen	1. is gestart door de Raad van Hoofdcommissarissen. Dit project moet verbetering in de situatie van het digitaal opsporen brengen. Uitgangspunt daarbij is een onderscheid tussen tactisch uitvoerend en technisch ondersteunend opsporingswerk. 2. werkrelatie
NCTB	Nationaal Coördinator Terrorismebestrijding	1. is verantwoordelijk voor de beleidsontwikkeling, de analyse van (inlichtingen-)informatie en de regie over te nemen beveiligingsmaatregelen bij de bestrijding van terrorisme. Informatie wordt doelmatig verzameld, geanalyseerd en gebruikt, er zijn voldoende instrumenten om tijdig in te grijpen en potentiële doelwitten worden adequaat beveiligd. 2. kennisuitwisseling
NFI	Nederlands Forensisch Instituut	1. verricht forensisch onderzoek op (overwegend) technisch, medisch-biologisch en natuurwetenschappelijk terrein. 2. kennisuitwisseling
NHTCU	National Hi-Tech Crime Unit	1. bestrijden georganiseerde High Tech Crime binnen de UK of die van invloed is op de UK d.m.v. wereldwijd erkende standaarden 2. kennisuitwisseling, omdat het NHTCU een vergelijkbare doelstelling heeft wordt veel kennis en ervaring uitgewisseld.

Organisatie	**Volledige naam**	**1. Korte beschrijving van de organisatie.** **2. Soort relatie**
NPC	Nationaal Platform Criminaliteitsbeheersing	1. werkt met vele publieke en private partijen uit het bedrijfsleven gezamenlijk aan: het verminderen van de kwetsbaarheid van de overheid en bedrijfsleven voor cybercrime het verhogen van het bewustzijn voor de gevolgen van cybercrime het organiseren van preventieve maatregelen het verbeteren van het collectieve reactievermogen 2. geven gezamenlijk invulling aan vormgeving bestrijding HTC
NVB	Nederlandse Vereniging van Banken	1. heeft een samenwerkingsverband met het project High Tech Crime (NHTCC) om high tech crime tegen financiële instellingen beter het hoofd te kunnen bieden 2. intentieverklaring moet nader bezien worden na besluitvorming
Onderwijs	Ministerie van Onderwijs en Wetenschappen	1. geeft de jeugd (en hun ouders) voorlichting op dit gebied door onder andere Surfnet en Kennisnet. Tevens vervult het onderwijs een preventieve rol 2. informatie-uitwisseling
OPTA	Onafhankelijke Post en Telecommunicatie Autoriteit	1. houdt toezicht op de naleving van de wet- en regelgeving op het gebied van post en telecommunicatie en het stimuleren van bestendige concurrentie in de telecommunicatie- en postmarkten. 2. kennisuitwisseling
OVSE	Organisatie voor Veiligheid en Samenwerking in Europa	1. voorkomt conflicten (preventieve diplomatie) of verleent bijstand na een conflict door bij te dragen aan de (weder)opbouw van de democratie en de rechtsstaat. 2. relatie moet worden opgebouwd voor het uitwisselen van kennis
PI	Platform Informatiebeveiliging	1. is een vereniging die zich beijvert voor de beveiliging van informatie en informatiesystemen. De belangrijkste pijler voor PI is het ontwikkelen en onderhouden van richtlijnen voor de praktische inrichting van informatiebeveiliging. Het organiseren van themabijeenkomsten is een tweede pijler voor de onderlinge samenwerking tussen de leden. 2. relatie moet worden opgebouwd voor het uitwisselen van kennis

Organisatie	**Volledige naam**	**1. Korte beschrijving van de organisatie.** **2. Soort relatie**
Politieke Partijen	Politieke Partijen	1. leveren hun aandeel door middel van de speciale ICT-woordvoerders. Vooral PvdA CDA, VVD en SP houden zich bezig met het onderwerp. 2. ervoor zorgen dat zij op de hoogte zijn van de wijze waarop HTC in NL bestreden kan worden
Private initiatie-ven algemeen	Private initiatieven alge-meen	1. zoals bijvoorbeeld IBM, Microsoft en Cisco leve-ren onder andere een bijdrage aan de bestrijding van High Tech Crime door met name de software-ware die zij ontwikkelen. 2. Zij zijn de zogenaamde ICT (toe)leveranciers – belangrijke bron voor informatie uitwisseling.
Regiokorpsen	Regiokorpsen	1. kunnen door een betere vastlegging van de aan-giftes van High Tech Crime een bijdrage gaan leve-ren aan de bestrijding van High Tech Crime. 2. er ligt een taak voor deze korpsen om hier (in samenwerking met KLPD) een protocol voor te ontwikkelen.
R ICT Politie	Regieraad ICT politie	1. heeft tot taak: ontwikkeling, implementatie, evaluatie en bijstelling van het ICT-beleid voor de Nederlandse politie; realisatie van een gelijkwaar-dig basisniveau van ICT-voorzieningen en een ho-mogene basisinformatievoorziening bij de politie-korpsen; ontwikkeling van standaarden voor net-werkvoorzieningen, hard- en software voor de poli-tiekorpsen onderling en voor de aansluiting tussen de korpsen en door de Regieraad aangewezen der-den. 2. werkrelatie
SIF	Safe Internet Foundation	1. is een stichting die de belangen behartigt voor de eindgebruiker van de elektronische snelweg. SIF verbetert de kwaliteit en veiligheid van het inter-net. De stichting neemt initiatieven om internet gebruikers voorlichting te geven over het veilig gebruik van internet. SIF maakt onderdeel uit van het EPN-netwerk (zie ook EPN). 2. kennisuitwisseling
Stuurgroep	Stuurgroep	1. te weten een afvaardiging van BZK, JZ, EZ en de KLPD. Zij zijn verantwoordelijk voor de inhoud en de totstandkoming van NHTCC (zie: BZK, JZ, EZ en KLPD) 2. gezamenlijke opdrachtgevers, geven sturing aan het project HTC
TDE	Team Digitale Expertise	1. is gespecialiseerd in digitale opsporing. Binnen dit team zijn diverse professionals werkzaam die

Organisatie	**Volledige naam**	**1. Korte beschrijving van de organisatie.** **2. Soort relatie**
		over voldoende kennis en ervaring beschikken om internetcriminaliteit (zijnde de verspreiding van computervirussen) op te sporen. 2. werkrelatie
TNO	Nederlandse Organisatie voor toegepast natuurwetenschappelijk onderzoek	1. helpt de sector Veiligheid met kennis en innovatieve oplossingen op het gebied van o.a.: Beveiliging van informatie; Optimale inzet en samenwerking van mobiele netwerken; Toekomstscenario ontwikkeling van High Tech Crime 2. kennisuitwisseling
VNO-NCW	Verbond van Nederlandse Ondernemingen (VNO) en het Nederlands Christelijk Werkgeversverbond (NCW).	1. geeft in samenwerking met de overheid een extra impuls aan de veiligheid van het bedrijfsleven. Daartoe ondertekende zij het Actieplan Veilig Ondernemen deel 2. 2. met deze belangrijke belangenbehartiger moet een vertrouwensrelatie verder worden uitgebouwd zodat nog frequenter informatie kan worden uitgewisseld

Bijlage 3

Publicaties project HTC

oktober 2004 - september 2005

Publicatiedatum	Medium	Titel
14 oktober 2004	Security online	Aanpak computercriminaliteit faalt
15 oktober 2004	Markvervaar.nl	Aanpak computercriminaliteit faalt
5 november 2004	Nieuwsbank.nl	Ministeries en KLPD pakken high-tech crime aan
5 november 2004	NRC Handelsblad	Ministeries tegen computercriminaliteit
5 november 2004	Webwereld.nl	Overheid en KLPD pakken ICT-misdaad aan
5 november 2004	VoorneNET business ISP	Overheid en KLPD pakken ICT-misdaad aan
5 november 2004	DMEurope	National High Tech Crime Centre launched in Netherlands
5 november 2004	Personal Computer Magazine	Ministeries en KLPD pakken high-tech crime aan
5 november 2004	Automatiseringgids	Ministeries en KLPD willen 'high-tech crime' aanpakken
5 november 2004	Niburu.nl	Centrum bestrijdt digitale misdaad
8 november 2004	Surfopsafe.nl	Ministeries en KLPD pakken high-tech crime aan
8 november 2004	Planet internet.nl	ICT-crimefighter en zwaardere Straffen
8 november 2004	Mediaplaza.nl	ICT-crimefighter en zwaardere Straffen
8 november 2004	Elsevier.nl	Harde aanpak van computercriminaliteit
9 november 2004	Het Parool	Front tegen computercriminelen
9 november 2004	Viruslist.com	Netherlands takes a stand against cyber-crime
9 november 2004	Recht.nl	Ministeries en KLPD pakken high-tech crime aan
9 november 2004	VNU.net	Overheid gaat ICT-criminaliteit hard aanpakken
10 november 2004	Radio Tros Online	Radio Interview Nienke van den Berg
12 november 2004	Computable.nl	Oogje op vitale infrastructuren
12 november 2004	Computable.nl	Criminaliteit met en tegen ICT
19 november 2004	Norea.nl	National High Tech Crime Center
19 november 2004	Computable.nl	Cybermisdaad breed te lijf
17 januari 2005	Nu.nl	Overheid reageerde waardeloos op computeraanval
17 januari 2005	Frontpage.fok.nl	Aanpak DDoS-attack regeringssites slecht
17 januari 2005	Jouwnieuws.nl	Aanpak DDoS-attack regeringssites slecht

Publicatiedatum	Medium	Titel
21 januari 2005	Automatiseringgids	Capaciteit digitale recherche moet fors worden uitgebreid
25 januari 2005	NHTCC.nl	Ministeries en KLPD pakken high-tech crime aan
1 februari 2005	Webwereld.nl	Leiding weg bij NHTCC
1 februari 2005	Computers.rekenmodules.nl	Projectleider N. van den Berg is na enkele maanden weggestuurd bij het NHTCC
11 maart 2005	Hccmagazine.nl	Cyberterrorisme: internet als massavernietigingswapen
22 maart 2005	Tweakzone.nl	Webshops bovenaan lijst van criminelen
08 april 2005	NHTCC.nl	National High Tech Crime Center heeft nieuwe projectleiding
02 juni 2005	CVIB.nl	Misbruik van internet?
07 juni 2005	Het Financieele Dagblad	Grootste Trojaanse paard kan tot in Nederland reiken
14 juni 2005	Planet.nl	Banken eisen cybercrimestrijd
15 juli 2005	Webwereld.nl	Banken willen betere aanpak digitale oplichting
15 juli 2005	Rtl.nl	Banken pakken computermisdrijven aan
15 juli 2005	NHTCC.nl	NVB en NHTCC werken samen in strijd tegen high-tech crime
15 juli 2005	NVB.nl	NVB en NHTCC werken samen in strijd tegen high-tech crime
15 juli 2005	Mcnews.nl	Banken gaan computermisdrijven aanpakken
15 juli 2005	Automatiseringgids	Banken en overheid trekken op tegen computercriminaliteit
16 juli 2005	NRC Handelsblad	Gezamenlijke actie in computerfraude
17 juli 2005	computer idee	NVB en NHTCC samen tegen high-tech crime
18 juli 2005	Ecp.nl	NVB en NHTCC werken samen in strijd tegen high-tech crime
18 juli 2005	Jouwnieuws.nl	NVB en NHTCC samen tegen high-tech crime
18 juli 2005	Surfopsafe.nl	Banken willen betere aanpak digitale oplichting
18 juli 2005	Vnunet.nl	NHTCC en NVB slaan handen ineen tegen high-tech crime
18 juli 2005	Emerce.nl	NHTCC en NVB slaan handen ineen tegen high-tech crime
18 juli 2005	Regionale dagbladen	NHTCC en NVB slaan handen ineen tegen high-tech crime
20 juli 2005	Solv.nl	Banken gaan samenwerken om computercriminaliteit tegen te gaan
23 juli 2005	Elsevier	Pasfraude via het web

Publicatiedatum	Medium	Titel
1 augustus 2005	Business News Radio	Interview Esther Schaddelee / Cisco
17 augustus 2005	Bitsoffreedom.nl	Oprichting Notice and Takedown systeem
18 augustus 2005	SIF.nl	Donner richt Notice and takedown systeem op
9 september 2005	Regionale dagbla-den/Radio 1	Lekken op Schiphol
7/8 oktober 2005	Regionale/landelijke dagbladen. NOS televi-sie	Botnets. Computerkrakers opgepakt
15 oktober 2005	Regionale/landelijke dagbladen	1,5 miljoen PC's door Botnets besmet
25 oktober 2005	Tros Radio Online	Radio interview met Hans Oude Alink over Botnets/oppakken hackers

Bijlage 4

Hoofdlijnen Wet Computercriminaliteit I en Wetsvoorstel Wet Computercriminaliteit II

Inleiding

De Wet computercriminaliteit I[9] heeft betrekking op de strafbaarstelling en bestrijding van misdrijven die met behulp van computertechnologie worden begaan, alsmede op misdrijven waarbij (computer) systemen het doelwit zijn. Naast de inhoudelijke strafbaarstelling (materiële bepalingen) omvat de Wet Computercriminaliteit I bepalingen die betrekking hebben op bevoegdheden die worden toegekend aan de met opsporing en vervolging belaste organen (formele bepalingen). Het wetsvoorstel Computercriminaliteit II van maart 2005 [10] is een combinatie van het wetsvoorstel Computercriminaliteit II uit 1999[11] en de aanpassingen die voortvloeien uit het Cyber Crime Verdrag.[12]

In deze bijlage wordt op hoofdlijnen de strafbaarstelling (materiele bepalingen) op grond van de Wet Computercriminaliteit I en van het wetsvoorstel Wet computercriminaliteit II beschreven.[13] Zowel ten aanzien van de Wet Computercriminaliteit I als het Wetsvoorstel computercriminaliteit II worden de formele bepalingen, alsmede de voorgestelde wijzigingen hiervan buiten beschouwing gelaten.

Wet computercriminaliteit I

De Wet Computercriminaliteit I onderscheidt in het Wetboek van Strafrecht op hoofdlijnen de strafbaarstelling van de volgende categorieën computercriminaliteit:

- Het binnendringen in een geautomatiseerd werk (hierna: computer(systeem) (artikel 138a Wetboek van Strafrecht);
- Stoornis in de gang of werking van een computer(systeem) veroorzaken (artikelen 161sexies en 161septies Wetboek van Strafrecht);
- Het onbruikbaar maken en veranderen van gegevens (artikelen 350a en 350b Wetboek van Strafrecht), en
- Het afluisteren en /of aftappen (artikelen 139c, 139d en 139e Wetboek van Strafrecht).

[9] Staatsblad 1993, 33.
[10] Tweede Kamer, vergaderjaar 2004 - 2005, 26 671, nr 7 -17.
[11] TK 1999 – 2001, 26 671, nrs 1 - 6.
[12] Goedkeuring van het op 23 november 2001 te Boedapest totstandgekomen Verdrag inzake de bestrijding van stafbare feiten verbonden met elektronische netwerken (Trb. 2002 nr.18), TK 2004 – 2005, 30 036 (R 1784), nr. 3 - 5.
[13] In deze paragraaf is een vereenvoudigde weergave opgenomen van de strafbaarstelling van computercriminaliteit. Voor een nauwkeurige weergave van de strafbaarstelling wordt te allen tijde verwezen naar de desbetreffende artikelen in het Wetboek van Strafrecht.

Computervredebreuk (artikel 138a Wetboek van Strafrecht)
Voor de strafbaarstelling van computervredebreuk (hacken) zal tenminste sprake moeten zijn van het binnendringen in het (computer)systeem waarbij *enige* beveiliging wordt doorbroken, of door het verwerven van toegang door een technische ingreep, met behulp van valse signalen of een valse sleutel of het aannemen van een valse hoedanigheid wordt binnengedrongen.

Stoornis in de werking (artikelen 161sexies en 161septies Wetboek van Strafrecht)

Bij het veroorzaken van stoornis in de werking van een (computer)systeem gaat het om:
- het beschadigen of onbruikbaar maken van het (computer)systeem, of
- het vernielen van het (computer)systeem, of
- het buiten werking stellen van een veiligheidsmaatregel die ten opzichte van het (computer)systeem is genomen.

Een belangrijke voorwaarde voor de strafbaarstelling van het veroorzaken van de stoornis is, dat één van de volgende gevolgen intreedt:
- De opslag of verwerking van gegevens ten algemene nutte wordt verhinderd of bemoeilijkt, er ontstaat stoornis in een openbaar telecommunicatienetwerk of er ontstaat stoornis in de uitvoering van een openbare telecommunicatiedienst;
- Er bestaat ernstig gevaar voor goederen of voor de verlening van diensten;
- Er bestaat levensgevaar voor een ander;
- Er bestaat levensgevaar voor een ander en het feit heeft iemands dood ten gevolge.

Het onbruikbaar maken en veranderen / wijzigen van gegevens (artikelen 350a en 350b Wetboek van Strafrecht)

De strafbaarstelling van het veranderen van gegevens heeft betrekking op de bescherming van een ongestoorde gebruik van computergegevens tegen onder meer onbevoegde verandering of het ontoegankelijk maken van die gegevens.
Voor de strafbaarstelling is het noodzakelijk dat er sprake is van:
- Het vernielen en veranderen van gegevens, en
- Het ter beschikking stellen en verspreiden van gegevens die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een (computer)systeem.

Afluisteren / aftappen (artikelen 139c, 139d en 139e Wetboek van Strafrecht)

Het aftappen en /of opnemen van gegevens van een openbaar telecommunicatienetwerk is strafbaar in de volgende gevallen:
- het opzettelijk met een technisch hulpmiddel aftappen of opnemen van gegevens die niet voor iemand, mede voor iemand of voor degene in wiens opdracht wordt gehandeld, zijn bestemd, of
- het zonder toestemming plaatsen van een technisch hulpmiddel met de bedoeling om een gesprek, telecommunicatie of andere gegevensoverdracht af te luisteren, af te tappen of op te nemen, of

- het voorhanden hebben en gebruiken van gegevens waarvan iemand weet of redelijkerwijs kan vermoeden dat die gegevens door onrechtmatig afluisteren, aftappen en/of opnemen zijn verkregen.

Wetsvoorstel Computercriminaliteit II (Wetboek van Strafrecht)

Evenals de Wet Computercriminaliteit I onderscheidt het Wetsvoorstel Computercriminaliteit II op hoofdlijnen de strafbaarstelling van de volgende categorieën computercriminaliteit:

- Het binnendringen in een (computer)systeem (artikel 138a Wetboek van Strafrecht);
- Stoornis in de gang of werking van een (computer)systeem (artikelen 161sexies en 161septies Wetboek van Strafrecht) veroorzaken;
- Het onbruikbaar maken en veranderen van gegevens (artikelen 350a en 350b Wetboek van Strafrecht), en
- Het afluisteren en /of aftappen (artikelen 139c, 139d en 139e Wetboek van Strafrecht).

Hieronder wordt per categorie de belangrijkste voorgestelde wijzigingen ten opzichte van het huidige Wetboek van Strafrecht beschreven.

Computervredebreuk (wijziging van artikel 138a, eerste lid van het Wetboek van Strafrecht)

Een belangrijke wijziging die voortvloeit uit het Wetsvoorstel Computercriminaliteit II voor de strafbaarstelling van hacken, is het vervallen van *de eis* in het huidige Wetboek van Strafrecht dat er sprake moet zijn van doorbreking van *enige* beveiliging, of dat door middel van een technische ingreep, met behulp van valse signalen, een valse sleutel of het aannemen van een valse hoedanigheid wordt binnengedrongen in een computersysteem. Voornoemde *voorwaarden voor strafbaarheid* zijn in het wetsvoorstel opgenomen als *voorbeelden* van gevallen waarin er sprake *kan* zijn van het opzettelijk en wederrechtelijk binnendringen in een computersysteem. Dit betekent dat *ook andere methoden of technieken* op basis waarvan wordt binnendrongen in een computersysteem strafbaar worden. In het geval wordt binnengedrongen door middel van het doorbreken van de beveiliging, wordt benadrukt dat in het wetsvoorstel niet meer wordt gesproken over *"het doorbreken van enige beveiliging"*, maar over *"het doorbreken van een beveiliging"*. Dit betekent dat niet meer hoeft te worden gediscussieerd over of de vraag of de mate waarin beveiligingsmaatregelen zijn genomen voldoet aan de eis van het doorbreken van "enige beveiliging" in het huidige artikel 138a Wetboek van Strafrecht.

Stoornis in de werking (invoering van artikel 138b Wetboek van Strafrecht)

Op basis van het wetsvoorstel Wet Computercriminaliteit II wordt de strafbaarstelling voor het belemmeren van de functie van een (computer)systeem makkelijker.

De belangrijkste wijziging in dit artikel heeft betrekking op het feit dat ook het veroorzaken van stoornis in de werking van (computer)systemen die niet ten al-

gemene nutte worden gebruikt (zoals thans in de artikelen 161sexies en septies van het Wetboek van Strafrecht is opgenomen) eveneens strafbaar wordt.

Dit betekent dat ook de belemmering van of het veroorzaken van een stoornis in een privé-computer of het platleggen van computersystemen ((d)Dos aanval) die niet het openbaar belang dienen, strafbaar wordt gesteld. Een voorwaarde voor strafbaarheid is wel dat er sprake is van *ernstige hinder.*

Ten aanzien van het veroorzaken van stoornis in de werking van een (computer)systeem wordt in de voorstellen tot wijziging van de artikelen 161sexies en 161septies van het Wetboek van Strafrecht in het wetsvoorstel Wet Computercriminaliteit II ook de *voorbereidende handelingen* ten aanzien van het veroorzaken van een stoornis een (computer)systeem strafbaar gesteld. Er is sprake van een voorbereidende handeling in het geval:

- iemand een technisch hulpmiddel dat hoofdzakelijk geschikt is gemaakt of is ontworpen voor het veroorzaken van de stoornis ter beschikking stelt of voorhanden heeft door bijvoorbeeld het vervaardigen, verkopen, verwerven, invoeren of het verspreiden, of
- iemand een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden verkregen tot het (computer)systeem of een deel daarvan, verkoopt, verwerft, verspreidt of anderszins ter beschikking stelt of voorhanden heeft.

Het onbruikbaar maken en veranderen/wijzigen van gegevens (wijziging van de artikelen 350a en 350b Wetboek van Strafrecht)

De kern van de voorgestelde wijzigingen tot de strafbaarstelling van het onbruikbaar maken en veranderen en/of wijzigen van gegevens is dat de strafbaarstelling ook betrekking heeft op het onbruikbaar maken en veranderen en/of wijzigen van gegevens bij de overdracht van gegevens tussen computer(systemen). Daarnaast wordt ook het schade aanrichten door het ter beschikking stellen of verspreiden van gegevens die zichzelf technisch gezien *niet* vermenigvuldigen strafbaar gesteld. In het huidige strafrecht is voor de strafbaarstelling bepalend of de schade is veroorzaakt door gegevens die zichzelf technisch gezien vermenigvuldigen.

Afluisteren/aftappen (wijziging van de artikelen 139c en 139d van het Wetboek van Strafrecht)

De kern van de voorgestelde wijzigingen tot strafbaarstelling van het aftappen en/of opnemen van gegevens is enerzijds dat wordt verduidelijkt dat degene die in opdracht van een gerechtigde gegevens opneemt of aftapt, niet strafbaar is. Anderzijds worden een aantal voorbereidingshandelingen zoals het vervaardigen, verkopen, verwerven, invoeren, verspreiden of anderszins ter beschikking stellen of voorhanden hebben van een technisch hulpmiddel en/of toegangscodes die hoofdzakelijk geschikt is gemaakt of ontworpen is tot het plegen van bepaalde strafbare feiten, strafbaar gesteld.